



# UNIVERSITY OF STRATHCLYDE

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCES

## An End-User Centred Framework for Data Access Management and Security in the Enterprise Public Cloud

EYA NWANNEKA GETHRUDE

This dissertation was submitted in partial fulfilment of the requirements  
for the degree of Doctor of Philosophy in Computer and Information  
Science.

April 2024.



---

## Dedication

---

*"Dedicated to the memory of my father, Mr Felix Chidi Eya, who always believed in my ability to be successful in the academic arena. You are gone but your belief in me has made this journey possible."*

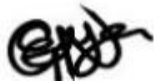


# Declaration

This thesis is the result of the author's original research. It has been composed by the author and has not been previously submitted for examination which has led to the award of a degree.

The copyright of this thesis belongs to the author under the terms of the United Kingdom Copyrights Acts as qualified by the University of Strathclyde Regulation 3.50. Therefore, Due acknowledgement must always be made of the use of any material contained in or derived from this thesis.

Signature:

A handwritten signature in black ink, appearing to be 'E. J. ...', written over a faint circular stamp or watermark.

Date: 22/04/2024

# Publications

June 2019, Abstract and Poster Presentation, Title: “The impact of Cloud Computing on Enterprise System Security.” SISCA PhD Conference 18th June,2019, University of Stirling Scotland, United Kingdom.

February 2020, Paper Presentation, Title: “A Report Evaluating the Factors that supports and inhibits the creation of an Information Security Culture within Organization-SMEs.”,723rd International Conference on Management and Information Technology (ICMIT), 16th – 17th February 2020, New York, United States of America. Published in “International Journal of Advances in Electronics and Computer Science”, Paper ID: AW-ICMITNY-160220-11044.

March 2021, Paper Presentation, Eya, Nwanneka, and George RS Weir. "End-User Authentication Control in Cloud-based ERP Systems." 2021 National Computing Colleges Conference (NCCC). IEEE, 2021.

The dataset used in this project can be found on Strathclyde pure using the temporal DIO: 10.15129/bb286941-d772-49dc-b43b-e70a00922e00.



# Abstract

Cloud Computing, an emerging internet technology that provides on-demand services to end-users with high scalability in an efficient way over the internet. Enterprises in recent years have been keen on cloud-based Enterprise Resource Planning software as it is more affordable than traditional on-premises Enterprise Resource Planning software. An interesting pattern emerges when enterprises, although keen on cloud-based Enterprise Resource Planning software, are concerned about their data security in the cloud, which is the major concern hindering the adoption of cloud-based Enterprise Resource Planning software applications within enterprises. In this context, this research reviewed various cloud computing security models and proposed an implementation framework which uses '*Enterprise Access Directory, Cloud Service Provider Access Directory, Enterprise Database Fragmentation, and End-user Access Queries*' to encourage more enterprise end-user involvement in the security of enterprise data in the cloud. A sequential exploratory mixed method approach was designed in four stages namely: 'Project Initiation', 'Project Prioritization', 'Project Analysis Phase' and 'Project evaluation'. This was used to evaluate the attributes of the proposed framework. The analysis of the research data showed that the proposed framework was asked in the right direction. The proposed framework encourages end-user participation in enterprise cloud data security while also reducing the impact of malicious insiders on the data stored in enterprise public cloud. This research contributes to existing knowledge of cloud computing security models by augmenting the research area of end-user roles and responsibilities within the enterprise to determine the level of access to data in the cloud-based Enterprise Resource Planning system. Policies for data management security and incentive programmes for enterprises, in the initial study for this research revealed that communication methods predict how well end-users follow policies. The initial study for this research confirmed the value of communication in this domain.



# Acknowledgements

I am especially indebted to Dr George Weir, my PhD Supervisor at the Computer and Information Science Department, University of Strathclyde. Who has been supportive of my research goals and who worked actively to provide me with the protected academic time to pursue those goals. Thank you.

I am particularly grateful to Dr Karen Renaud, my PhD Supervisor, for taking time to review my thesis and provided helpful feedback. Thank you.

This work would not have been possible without the financial support of the Faculty of Science Elite Scholarship Programme Award. As a self-funded researcher, this scholarship made a huge difference in my finances and helped me to actualize my PhD research goals. I am grateful.

I am grateful to all of those with whom I have had the pleasure to work with during this research and other related projects. Each of the members of my examination team and my research group (The security research group) has provided me with extensive personal and professional guidance and taught me a great deal about both scientific research and life in general. The constant feedback they were willing to provide always made a difference.

My gratitude, appreciation, and heartfelt thanks go out to each interview and questionnaire respondent, who was kind with their time and provided detailed discussion and thoughtful insight, for sharing their valuable experiences.

Nobody has been more important to me in the pursuit of this project than the members of my family. They are the ultimate role models. I would like to thank my brother Felix and my mum Eucharika; whose love and guidance are with me in whatever I pursue. Most importantly, I wish to thank my loving and supportive husband Francis, who provides unending inspiration. Thank you, baby Ezinne, for coming into our lives, you are such a joy. I want to also acknowledge my late father Felix Chidi Eya, who was my main inspiration to fulfil the promises I made to him.

# Contents

Declaration .....	i
Publications .....	ii
Abstract .....	iv
Acknowledgements.....	v
Contents.....	vi
List of Tables.....	ix
List of Figures.....	xi
List of Abbreviations .....	xiv
Chapter 1. Introduction .....	1
1.1 Introducing the Views / Overview .....	1
1.2 Problem Domain.....	7
1.3 Research Motivation and Novelty .....	15
1.4 Research Aim and Objectives. ....	17
1.5 Research Questions .....	18
1.6 An Understanding of Our Research Assumptions .....	20
1.7 Research Contributions and Limitations.....	29
1.8 Research Methodology Summary .....	30
1.9 Thesis Outline .....	31
1.10 Summary of Chapter 1 .....	33
Chapter 2. Related Work and Relevant Theories .....	35
2.1 The Enterprise .....	37
2.2 Data.....	45
2.3 The Fundamentals of Information Security .....	50
2.4 Cloud Computing .....	57
2.5 Cloud Computing Security Models .....	67
2.6 Understanding the Concepts of Human Factors.....	73
2.7 A Systematic Literature Review on the Adoption of ERP Systems within Enterprises .....	98
2.8 A Narrative Literature Review on the Adopting End-User Security Responsibility in Ensuring Enterprise Data Security in Public Cloud.....	122

2.9 Summary of Chapter 2.....	131
Chapter 3. Research Methodology .....	133
3.1 Research Questions and Research Assumptions .....	139
3.2 Research Design and Strategy.....	151
3.3 Data Collection Techniques .....	170
3.3.1 Quantitative Techniques .....	171
3.3.2 Qualitative Techniques .....	184
3.4 Validity, Reliability, Repeatability.....	197
3.5 Ethical Consideration .....	198
3.6 Summary of Chapter 3.....	198
Chapter 4. End-user Centric Access Control Framework.....	200
4.1 Parametric Comparison of the various Cloud Security Models.....	201
4.2 Strengths and Weaknesses of the Cloud Security Models.....	208
4.3 End-user Data Access Management Implementation Framework for Enterprise ERP Software based in the Public Cloud. ....	211
4.4 Summary of Chapter 4.....	216
Chapter 5. Quantitative Data Analysis.....	218
5.1 Quantitative Data Visualization Using Tables and Bar Charts.....	218
5.2 Statistical Analysis of our Research Assumptions .....	238
5.3 Summary of Chapter 5.....	268
Chapter 6. Evaluation and Discussion .....	270
6.1 Information and Trends about Research Participants.....	273
6.2 Response Rate .....	274
6.3 Research Question Assessment.....	276
6.4 The EAD and CSP AD Directories .....	287
6.5 Discussion on the Study of the Role of Human Factors on Enterprise System Security in Public Cloud.....	289
6.6 Summary of Research Findings with Emphasis on Research Questions .....	311
6.7 Summary of Chapter 6.....	318
Chapter 7. Conclusion and Recommendations.....	320
7.1 Summary of Main Research Contribution .....	320
7.2 Project Strengths.....	331
7.3 Project Limitation.....	332
7.4 Further Research Recommendation .....	332

7.5 Summary of Chapter 7.....	333
Reference.....	335
Appendix .....	395
8.1. Appendix 1. Research Ethics documentation.....	395
8.2. Appendix 2. Initial Study Interviews Questions and Initial Study Transcripts. .....	405
8.3. Appendix 3. Main Study Survey Questions Draft and Main Study Transcript generated from Qualtrics software. ....	412
8.4. Appendix 4. Research Communications.....	455
8.5. Appendix 5. Initial Study Participating Enterprise Profile. ....	461

# List of Tables

Table 2.1: Enterprise classification using the number of employees in the enterprise. By (Raczyńska, 2019); (OECD, 2022)-----	39
Table 3.1: An Overview of Paradigm. By Salma Patel (2015)-----	137
Table 3.2: Initial Research Assumptions (Eya, 2023) -----	150
Table 3.3: Mixed Method Designs. By Creswell et. al., 2009-----	161
Table 3.4: Mixed Method Designs Comparison -----	162
Table 3.5: Research survey questions and the research assumption it is addressing, and the type of data response collected-----	175
Table 3.6: Interview Sample for participating enterprises -----	193
Table 4.1: Summary of Framework Attributes Definitions-----	201
Table 4.2: Summary of Parameters Definitions-----	202
Table 4.3: Table representation of the cloud security model and its analysing features -----	208
Table 4.4: Summary of the strength and weakness of the different CSM-----	210
Table 5.1: Data representation of SQ1 -----	218
Table 5.2: Data representation of SQ2 -----	220
Table 5.3: Data representation of SQ3 -----	221
Table 5.4: Data representation of SQ4 -----	223
Table 5.5: Data representation of SQ5 -----	225
Table 5.6: Data representation of SQ6 -----	226
Table 5.7: Data representation of SQ7 -----	227
Table 5.8: Data representation of SQ8 -----	229
Table 5.9: Data representation of SQ9 -----	230
Table 5.10: Data representation of SQ10 -----	231
Table 5.11: Data representation of SQ11 -----	233
Table 5.12: Data representation of SQ12 -----	234
Table 5.13: Data representation of SQ13 -----	235
Table 5.14: Data representation of SQ14 -----	236

Table 5.15: Data representation of SQ15 -----	237
Table 5.16: The Assumption variables and the SQs Variables-----	238
Table 5.17: The Agreement Scale (Eya, 2023) -----	239
Table 5.18: Test of Normality of our Assumption Variables-----	242
Table 5.19: Case Processing Summary for “Test of Normality ”-----	243
Table 5.20: The Descriptive Statistics of the each of the Assumption Variables---	244
Table 5.21: Test of Normality of the Log10 A1, A3 and A4-----	249
Table 5.22: Case Processing Summary for log_A1, log_A3 and log_A4-----	250
Table 5.23: The Descriptive Statistics of the each of the Assumption Variables for log_A1, log_A3 and log_A4 -----	250
Table 5.24: Ordinal Regression Case Processing Summary-----	253
Table 5.25: Model Fitting Information -----	254
Table 5.26: Goodness of fit-----	255
Table 5.27: Pseudo R-Square -----	255
Table 5.28: Test of Parallel Lines -----	256
Table 5.29: Ordinal Regression Parametric Estimates of the Lower Bound-----	257
Table 5.30: Ordinal Regression Parametric Estimates of the Upper Bound -----	259
Table 5.31: Correlations Analysis I -----	260
Table 5.32: Correlations Analysis II -----	261
Table 6.1: Difference between the CSP AD and EAD (Eya, 2023)-----	288
Table 6.2: Initial Study Coding Themes (Eya, 2023)-----	290
Table 6.3: Summary of the Research Assumption Validation Results.-----	313

# List of Figures

Figure 2.1: The overview of what this Chapter stands to achieve. (Eya 2023) -----	35
Figure 2.2: Infrastructure of an e-commerce website (Nednur, 2018 ;Eya, 2023).---	60
Figure 2.3: Three levels of the Default Gateway Platform (Eya, 2023). -----	72
Figure 2.4: Summary of the categories of human factors (Mortazavi-Alavi, 2016) ;(Eya, 2023).-----	77
Figure 2.5: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews (MJ, et.al; 2021).-----	104
Figure 2.6: The history of ERP systems in enterprises -----	106
Figure 2.7: The history of adoption of cloud-based ERP systems in Nigerian enterprises -----	112
Figure 2.8: Chart showing the research article distribution by number of years. ---	114
Figure 2.9: Chart showing the research articles and the number of citations-----	115
Figure 2.10: Chart showing the research article and the type of theory of the research -----	116
Figure 2.11: Chart showing the research article and the sample size of the research participants -----	116
Figure 2.12: Chart showing the research article and the research methodology ----	117
Figure 2.13: Chart showing the research articles and the type of enterprises the research carried out in -----	117
Figure 2.14: Chart showing the research articles narrowed focus area -----	118
Figure 3.1: Visualization of Research Overall Process -----	158
Figure 3.2: Components of Mixed Method -----	160
Figure 3.3: Data Collected Technique for Mixed Method Approach. (Eya, 2023)-	170
Figure 3.4: Phases of the Initial study research activities (Eya, 2023) -----	192
Figure 4.1: Classification of the Different Security Responsibilities between the End- Users and the CSP in the various Cloud Security Models (Eya, 2023)-----	206
Figure 4.2: Separation of responsibility between the end-user and CSP using different cloud deployment models (Chou ,2010)-----	207
-----	215
Figure 4.4: End-user Data Access Management Implementation Framework for Enterprise ERP software based in the Public Cloud (Eya, 2023)-----	215
Figure 5.1: Bar Chart representation of collected data for SQ1 -----	219

Figure 5.2: Bar Chart representation of collected data for SQ2-----	220
Figure 5.3: Bar Chart representation of collected data for SQ3-----	222
Figure 5.4: Bar Chart representation of collected data for SQ4-----	223
Figure 5.5: Bar Chart representation of collected data for SQ5-----	225
Figure 5.6: Bar Chart representation of collected data for SQ6-----	226
Figure 5.7: Bar Chart representation of collected data for SQ7-----	228
Figure 5.8: Bar Chart representation of collected data for SQ8-----	229
Figure 5.9: Bar Chart representation of collected data for SQ9-----	230
Figure 5.10: Bar Chart representation of collected data for SQ10-----	231
Figure 5.11: Bar Chart representation of collected data for SQ11-----	233
Figure 5.12: Bar Chart representation of collected data for SQ12-----	234
Figure 5.13: Bar Chart representation of collected data for SQ13-----	235
Figure 5.14: Bar Chart representation of collected data for SQ14-----	236
Figure.5.15: Bar Chart representation of collected data for SQ15-----	237
Figure 6.1: Summary of SQ1 and SQ2 that shows the IT and Cloud based ERP experience of our research participants (Eya, 2023) -----	274
Figure 6.2: Summary of the responses to all the SQs showing the number of responses in each response category -----	277
Figure 6.3: Summary of the SQs that addressed research question "RQ1" -----	279
Figure 6.4: Summary of the SQs that addressed research question "RQ2" -----	281
Figure 6.5: Summary of the SQ11 that addressed research question "RQ3" -----	283
Figure 6.6: Summary of the SQ12 that addressed research question "RQ4" -----	284
Figure 6.7: Summary of the SQ12 that addressed research question "RQ5" (Eya, 2023)-----	286
Figure 6.8: Word cloud for Cloud-based ERP system impact on enterprise data security -----	291
Figure 6.9: Word cloud for Data Management Security Policy (Eya, 2023) -----	295
Figure 6.10: Word cloud for End-user skills and end-user roles-----	299
Figure 6.11: Word cloud for the Number of staff in your enterprise-----	302
Figure 6.12: Word cloud for Organization data security culture -----	303
Figure 6.13: Word cloud for Training programs and organization EIS regulations	305





# List of Abbreviations

AaaS: Anything as a Service

AX: Axapta

AWS: Amazon Web Services

CAD: Computer-Aided Design

CCS: Cloud Computing Security

CEO: Chief Executive Officer

CCSM: Cloud Computing Security Model

CIC: Community Interest Company

CIM: Computer Integrated Manufacturing

CLG: Company Limited by Guarantee

CMM: Capacity Maturity Model

CPU: Central Processing Unit

CRAM: Cloud Risk Accumulation Model

CS: Cloud Service

CSA: Cloud Security Alliance

CSP: Cloud Service Providers

CSP AD: CSP Access Directory

DaaS: Database as a Service.

DBMS: Database Management System

DGPM: Default Gateway Platform Model

DM: Design Management

DMS: Data Management System

DooS: Denial of Service Attack

EAD: Enterprise Access Directory

EAQ: End-user Access Quires

EDF: Enterprise Database Fragmentation

EDS: Electronic Data Systems

EIS: Enterprise Information Systems

ES: Enterprise Systems

ERP: Enterprise Resource Planning

EUCS: End-User Computing Satisfaction

GOST: Government Standard

IaaS: Infrastructure as a Service

ICT: Information Communication Technology

ILO: International Labour Organization

IoT: Internet of Things

ISO/IEC 27001: International Organization for Standardization/International Electrotechnical Commission 27001

ISS: Information Security System

IT: Information Technology

JCCM: Jericho Forum's Cloud Cube Model

Log: Logarithms

LTD: Company Limited by Shares

MCDM: Multiple Cloud Database Model

ML: Machine Learning

MRP: Material Requirement Planning

MTM: Multiple Tenancy Model

NIST: National Institute of Standard and Technology

OECD: Organization for Economic Co-operation and Development.

OSHA: Occupational Safety and Health Administration

OTP: One Time Password

PaaS: Platform as a Service

PAP: Project Analysis Phase

PIP: Project Initiation Phase

PLC: Programmable Logic Controller

PLC: Public Limited Company

PPP: Project Prioritization Phase

RC: Royal Charter

RMQ: Research Main Question

RPA: Robotic Process Automation

ROI: Return on Investment

RTPO: Real-Time Process Optimization

SaaS: Software as a Service

SCM: Supply Chain Management

SFDC: Shop Floor Data Collection

SIEM: Security Information and Event Management

Sig: Significance

SLA: Service Level Agreement

SME: Small Medium Enterprises

SNC: Secure Network Communications

SPC: Statistical Process Control

SPSS: Statistical Package for Social Science

SSF: Security Strength Factor

SSL: Secured Socket Layer

SWOT: Strength Weakness Opportunity Treats

TLS: Transport Layer Security

TPM: Technology Acceptance Model

TVDs: Trusted Virtual Data Centre

UNDP: United Nations Development Program

UNESCO: United Nations Educational, Scientific and Cultural Organization

Unltd: Unlimited Company

URIs: Uniform Resource Identifiers

VAT: Value Added Tax

VLANs: Virtual Land Area Networks

VM: Virtual Machines

VPC: Virtual Private Cloud

VPN: Virtual Private Network

2FA: Two Factor Authentication



# Chapter 1. Introduction

This first Chapter will introduce the whole concept of research. Section 1.1 introduces the overview, section 1.2 talks about the problem domain, section 1.3 talks about the research motivation and novelty, section 1.4 talks about research aims and objectives and gave a summary of research methods, research contribution, limitation and the research questions. Section 1.5 talks about the research questions, section 1.6 talks about the understanding of our research assumptions. Conclusively this Chapter is where the overview of the research is discussed. The problem domain is established, and the rationale behind the research discussed. This Chapter talks about the novelty of the research, its aims and objectives, and the research questions. It also reviews the research contributions and limitations in section 1.7. A summary of the research methodology is also provided in section 1.8. This Chapter concludes by providing an outline of the thesis to guide the reader through the thesis in section 1.9.

## **1.1 Introducing the Views / Overview**

In the modern era, or what many will call the “information age” (Kline, 2015; Solove, 2004), enterprises have an increased need to maximize productivity across all functional areas to remain competitive in their market niche. Because of the necessity to respond to changing market trends, the average business can become overly reliant on technologies that enable them to do so. The history of Enterprise Resource Planning (ERP) systems dates to the 1960s and 1970s (She, 2007; Monk, 2012; Katuu, 2020). During this period, the concept of integrating diverse business processes and functions into a single system emerged. The modern ERP as it exists today, however, began to take shape in the 1990s. ERP systems were initially developed primarily to manage manufacturing processes and materials requirements planning (MRP) (Bahssas, 2015). Large organisations and enterprises utilised these systems to expedite their production and inventory management.

As technology progressed and business requirements changed, ERP systems expanded to include a wider variety of functions, such as finance, human resources, sales, and procurement, among others (Mabert, 2001). In the late 1990s and early 2000s, as businesses realised the benefits of integrating their core business processes into a unified software platform, ERP adoption gained significant traction across industries (Evans, 2002). Providing a centralised platform for data management, collaboration, and decision-making, ERP systems are now indispensable to businesses of all sizes and in a variety of industries, as they facilitate data management, collaboration, and decision-making (Su, 2010). As technology continues to advance, ERP systems will likely undergo additional developments and enhancements to satisfy the changing requirements of modern businesses.

ERP applications are unique software applications developed to integrate all functional areas of an enterprise; for instance, finance, project management, sales, inventory management, etc., which encourages a transparent flow of information within the enterprise and therefore boosts its effectiveness. Jacobs (2007) mentioned that ERP software application adoption rate over the next decade will be impressive as many enterprises will adopt the ERP application and will have an absolute dependency on these software's to provide them with information to make major business decisions. In Chapter Two, section 2.7, we carried out a systematic literature review on the adoption of ERP systems where we discussed this context in more detail using current literature.

The major challenges that enterprises face when implementing an ERP software application are the associated infrastructure and maintenance costs (Seethamraju, 2015; Elmonem, 2016), which make such applications unaffordable for small-and medium-sized businesses (SMEs) (Al-Johani, 2013). Although many ERP software applications target SMEs (Bezemer, 2010), when the return on investment (ROI) is measured against the cost of the ERP software application implementation cost, the result is mostly lean (Haddara, 2011). Rashid et al, (2002) stated that, as of 1998, a large sum of US \$17 billion was the annual estimated expenses associated with the



implementation of ERP software applications in United States enterprises. It was argued that this was a direct result of the 30% to 50% growth rate experienced by ERP vendors in the US in 1998. By the end of the year 2000, the figure had gone up to the US \$21.5 billion, representing a growth rate of 13.1%. This figure continues to grow as each year passes with more enterprises' adopting ERP software applications.

Computing technology has experienced a major shift with the introduction of the internet. The statement "Computing technology has undergone a significant transformation since the advent of the internet" refers to the internet's transformative effect on the field of computing. Prior to the Internet's widespread adoption, computing predominantly consisted of isolated systems and local networks (Mailland, 2017). The internet revolutionised this landscape by interconnecting computers and networks around the world, thereby facilitating the interchange of information and communication on a scale never before seen (Aceto, 2018). Here are a few of the most significant aspects of the Internet's revolutionary impact:

*Connectivity on a Global Scale:* The internet created a global network that linked computers and devices from all over the world (Coetzee, 2011). This enabled worldwide communication and information sharing between individuals, enterprises, and organisations. It removed the restrictions of physical distance and enabled collaboration and data exchange in real time (Coetzee, 2011). *Access to Information:* The internet made enormous quantities of information accessible to anyone with an internet connection (Mahmoud, 2015). Prior to its introduction, gaining access to information typically required a visit to a library, the use of physical media, or reliance on limited local resources. With the advent of the Internet, people acquired access to a wealth of information, research, educational materials, and multimedia content, vastly expanding the opportunities for exploration and learning (Hsieh, 2017). *E-commerce and Online Services:* By introducing e-commerce platforms, the internet revolutionised commerce (Casaló, 2011). By removing geographical barriers and allowing businesses to reach a global customer base, online shopping has become a convenient and effective method of purchasing products and services

(Niranjanamurthy, 2013). In addition, various online services, such as online banking, entertainment streaming, social media, and others, have emerged, transforming how people interact, ingest media, and go about their daily lives (Matrix, 2014).

*Communication and Social Networking:* The Internet enabled new forms of communication, such as email, instant messaging, and voice over IP (VoIP) services (Herring, 2010; Houmansadr, 2013). It provided social networking platforms that enabled people to connect, share ideas, and collaborate in virtual communities. Platforms for social media have emerged as potent instruments for disseminating information, nurturing online communities, and facilitating social interactions (Hajli, 2017). *Cloud Computing and Storage:* The internet was instrumental in the development of cloud computing, which enables remote data storage, processing, and application access (Qi et al, 2018). Cloud services provide scalability, adaptability, and cost-effectiveness (Mohabbattalab, 2014), allowing businesses and individuals to leverage potent computing resources and storage without making substantial up-front investments. *Internet of Things:* The Internet enabled the development of the Internet of Things (Rose, 2015), a network of interconnected physical devices embedded with sensors, software, and connectivity. IoT devices can collect and exchange data, allowing for the automation, remote monitoring, and control of a wide range of systems, from smart homes and cities to industrial operations (Zeinab and Elmustafa, 2017).

These are just a few examples of how the advent of the internet has revolutionised computer technology. Influence of the internet continues to evolve, spurring innovations in fields such as artificial intelligence, data analytics, and cybersecurity, among others. It has had a profound and pervasive effect on how we live, work, communicate, and interact with technology in the contemporary world. This has changed the way individuals access information, and enterprises are not left out. Enterprises are experiencing a move from traditional computing, which involves a lot of expensive infrastructures, to more responsive internet-based computing technology

that can handle the rapid demand for real-time information to make business decisions and help them remain competitive in the market.

The enterprises have encountered various emerging computing technologies, but cloud computing appears to be more promising as it delivers economic gain. Emerging computing technologies refer to innovative approaches, tools, and paradigms that are gaining prominence in the technology landscape (Shawish and Salama, 2013). These technologies often offer novel solutions to existing problems and have the potential to transform various industries. However, when compared to other emerging technologies, cloud computing stands out as a particularly promising option due to its ability to deliver economic gains to enterprises. Cloud computing can be defined as the computing technology that allows enterprise access to a set of networked servers using the internet (Mell and Grance, 2009; Avram, 2014; Computing and Creeger, 2009). Cloud computing enables seamless collaboration and information sharing across geographically dispersed teams, resulting in enhanced productivity and efficiency (Wu et al; 2015). It is designed to scale resources on-demand, ensuring businesses have the computing power and storage capacity they need when they need it. It also provides robust backup and disaster recovery capabilities, allowing businesses to quickly recover their data and resume operations in the event of a disaster or system failure (Mell and Grance,2009). Cloud computing providers often provide a vast array of advanced technologies and services, such as artificial intelligence, machine learning, big data analytics, and IoT platforms, which enable organisations to leverage data-driven insights, automate processes, and drive innovation without substantial up-front investments (Tambare et al; 2021). Cloud computing provides businesses with a scalable, flexible, and cost-effective computing infrastructure, allowing them to concentrate on their core competencies while benefiting from dependable and efficient internet technology resources (Carroll, et al; 2011).

This simply means that, with cloud computing, an enterprise does not require a physical server to be located on its premises. Any internet technology service provided by a cloud service provider to an enterprise over the cloud is known as a “cloud service”

(Zhou, et al; 2010). Various types of cloud services are currently available, namely software as a service, platform as a service, infrastructure as a service, security as a service, analytics as a service, storage as a service, desktop as a service, monitoring as a service, and basically any internet technology service provided by a cloud service provided over the cloud (Simmon, 2018).

The deployment of a cloud service can take different models, but the one thing that determines what model an enterprise should use is the nature of the enterprise and the type of service the enterprise will need (Patel and Kansara, 2021). There are five cloud deployment models, which are: public cloud, private cloud, community cloud, hybrid cloud, and virtual private cloud (Patel and Kansara, 2021). A deployment model is considered a public cloud when the cloud can be used by any type of organization or individual, but the cloud is wholly owned by the cloud service provider, and the services provided are billed on a pay-as-go basis, although there may be some free applications on this type of cloud (Saritha, et al; 2020). On the other hand, the private cloud is the opposite of the public cloud; it is a cloud solely owned by an enterprise for its use, and the enterprise with a private cloud enjoys absolute control of the data in the cloud (Smith, et al; 2014). The Virtual Private Cloud (VPC) is another type of cloud deployment that is a fraction of the public cloud but gives users more detailed control over their resources in the cloud considering their security needs. It is like being on a public cloud where you are given preferential access due to your specific security needs to enable your enterprise to have better control (Nick, et al; 2010; Wood, et al; 2009).

The community cloud is a shared cloud deployment model, but the sharing is only between enterprises of similar operations or niches; for instance, university institutions in the UK may have a cloud solely for their use, or construction companies in the US may have a cloud solely for them (Goyal, 2014). The advantage of this type of deployment is that it puts into consideration the specific requirements of the sector or group that are critical to them. The hybrid cloud, which is normally the most recommended deployment model for an enterprise, encourages the enterprise to keep

most of its critical data within the enterprise's private cloud or server while still leveraging the cost benefits of the public cloud. This hybrid cloud allows the enterprise to combine two or more deployment models for their best interest while addressing concerns about security, loss of control, and compliance (Patel and Kansara, 2021).

The next sections present a brief of the problem domain.

## **1.2 Problem Domain**

Cloud Computing is an emerging internet technology that provides on-demand services to end-users with high scalability in an efficient way over the internet (Gajbhiye, 2014). Enterprises in recent years have been keen on cloud-based ERP software as it is more affordable than traditional on-premises ERP software (Saeed, 2012). The benefits of ERP software cannot be overemphasized, as this is evident in the rate of adoption of these systems by enterprises (Seethamraju and Sundar, 2013). This is because enterprises need to maximize productivity across all functional areas to remain competitive and rely on their market niche. An interesting pattern emerges when enterprises, although keen on cloud-based ERP software, are curious about their data security in the cloud (Pasquale and Ragone, 2013). In June, 2012, LinkedIn experienced a cyber-attack where its database containing 6.5 million usernames and passwords was compromised. A downloadable file containing data believed to have been scraped from LinkedIn and comprising information on more than 700 million users was leaked online in September 2021 after hackers attempted to sell it in June 2021 (Wikipedia, 2012). This exposure impacted LinkedIn user base. The data was dumped in two waves, initially exposing 500 million users. On November 24, 2014, a hacker organisation known as "Guardians of Peace" disclosed sensitive data belonging to Sony Pictures Entertainment (SPE). The data included confidential information about Sony Pictures employees and their families, emails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, future Sony film plans, scripts for some films, and other information were published publicly by hackers (Wikipedia, 2014). iCloud, which is an add-on service from Apple, also experienced a cyber-attack where images from their database were made public (Abi, 2022). These instances of cyber-attacks make it well evident that

the concerns enterprises have about a cloud-based ERP system are founded, and there is thus a need to look at a more user-centred cloud data security model that improves the data security of a cloud-based ERP system of organizations.

Raza, et al. (2015) argued that the adoption rate of cloud computing ERP software applications is rather slow-paced because of the many challenges associated with cloud computing, identifying the key challenges as the lack of awareness of cloud computing and fear of job loss among the information technology workforces. Modi, Patel, et al. (2013) stated that the major concern hindering the adoption of cloud-based ERP software applications is concerns about data security. The authors argued that lack of trust in cloud service providers and feelings of vulnerability that the enterprise's sensitive data will be lost are major issues that research has yet to extensively address to boost the enterprise's confidence in adopting a cloud-based ERP software application. According to Mell and Grance (2011), the rate of sharing and outsourcing associated with cloud computing presents unique data security challenges to the enterprise. Stavrou, Kandias et al. (2014) used the term "Malicious Insider" to describe an employee of a cloud service provider who may use their privileged position to take undue advantage of treasured data of an enterprise using their services. The authors concluded that among the threats to data security in the cloud, a malicious insider from the cloud service provider poses a concrete risk to data security, but it was not clear how the employee of the client enterprise is eliminated from being a great risk to cloud data. Moreover, the client enterprise employees have on-demand access to this data as they perform their various duties daily at work. Sen, (2014) affirms that social engineering attacks are a major concern for data security in the cloud. It takes into consideration the various educational and professional levels of employees within an enterprise and argues that the role of humans in cloud computing data security cannot be neglected. The nature of humans cannot be controlled by security technologies like firewalls, it is concluded that human behaviour is an important context in protecting or bridging data security in the cloud.

Fan, et al. (2015) think that a lot of times cloud data security is looked at from the cloud service provider's perspective. It is argued that when cloud data security is viewed from the "consumer point of view," many trends that lead to data security breaches will be uncovered. There are many data management security models that enterprises deploy to manage data security within the enterprise, but it is not clear how these data management security models will function in the face of a cloud-based enterprise system considering the enormous sharing that cloud computing presents (Anciaux, et al. (2019). Various data management security frameworks are implemented by enterprises to ensure data security within organisations. Here are some frequently used models:

*Access Control Models:* These models determine who within an enterprise has access to what data (Yu et al; 2010). Role-Based Access Control (RBAC), in which access is granted based on job roles, and Attribute-Based Access Control (ABAC), in which access is granted based on the attributes or characteristics of the user, are examples of access control models (Coyne and Weil, 2013). *Encryption:* This is the process of encoding data in a manner that renders it unintelligible without the corresponding decryption key (Thitme and Verma, 2016). Encryption techniques, such as Advanced Encryption Standard (AES) or RSA, are frequently employed by businesses to secure sensitive data at rest and in transit (Ananya et al; 2023). *Data Loss Prevention (DLP):* Data Loss Prevention (DLP) solutions are intended to prevent unauthorised data leakage (Tahboub and Saleh, 2014). They monitor and control data in motion, at rest, and in use, and enforce policies to prevent sensitive data from exiting the organisation via multiple channels.

*Data Masking:* This involves substituting sensitive data with fictitious but plausible data. It ensures that sensitive data is not disclosed to unauthorised parties while preserving the data's utility for development, testing, and analytics (Varshney, Munjal et al. 2020). *Tokenization:* Tokenization replaces sensitive data with unique identifiers or references that have no external significance or value (Ahmad, Paul et al. 2016). Tokenization can be used to protect sensitive information such as credit card numbers,

Social Security numbers, and personally identifiable information (PII) (Rozenberg 2012). *Classification and Labelling of Data*: Businesses use classification and labelling models to categorise data based on its sensitivity and to implement the appropriate security controls (Cherdantseva and Hilton 2013). This enables organisations to prioritise their security efforts and safeguard sensitive data accordingly. *Auditing and Logging*: Comprehensive mechanisms for logging and auditing are required for data security (Sundareswaran, Squicciarini et al. 2012). They record and monitor user activities, access attempts, and data modifications, thereby providing an audit trail for forensic analysis, compliance, and detecting security incidents (Weir, Aßmuth et al. 2017).

*Secure Development Lifecycle (SDL)*: The Secure Development Lifecycle (SDL) model assures that security is integrated throughout the software development process (de Vicente Mohino, Bermejo Higuera et al. 2019). It incorporates security practises at every stage, from design and coding to testing and deployment, thereby reducing the risk of application vulnerabilities and security defects (Farhan and Mostafa 2018). *Identity and Access Management (IAM)*: This refers to the management of user identities, authentication, and authorization to access enterprise resources by IAM systems (Nuss, Puchta et al. 2018). They enforce robust password policies, multi-factor authentication, and centralised provisioning and deprovisioning of users. *Security Information and Event Management (SIEM)*: SIEM systems aggregate and analyse security event logs from diverse enterprise network and application sources. By correlating events and identifying potential security vulnerabilities, they enable real-time monitoring, threat detection, and incident response (Gnatyuk, Berdibayev et al. 2021).

Individually or in combination, these models can be used to construct a comprehensive data management security framework tailored to an enterprise's particular needs and requirements. Looking at how these data management security models function in a cloud-based enterprise system considering the enormous sharing that cloud computing presents, it is possible to adapt and implement data management security models



within a cloud-based enterprise system to address the unique challenges and requirements of cloud computing and data sharing. How these models function in a cloud environment is as follows:

*Access Control Models:* Cloud service providers (CSPs) provide robust access control mechanisms to manage user access to cloud-stored data (Höfer and Karagiannis 2011, Albulayhi, Abuhusseini et al. 2020). Before being uploaded to the cloud, data can be encrypted and decrypted when accessed by authorised users. Additionally, enterprises can use encryption techniques like envelope encryption or client-side encryption to retain control over encryption keys. *Data Loss Prevention (DLP):* DLP solutions can be extended to the cloud to monitor and control the passage of data into and out of the cloud. This includes scanning for sensitive information, implementing policies to prevent unauthorised sharing, and identifying potential data breaches (Purohit and Singh, 2013).

*Data Masking and Tokenization:* Cloud-based data masking and tokenization techniques can be used to safeguard cloud-stored sensitive data (Domingo-Ferrer, Farras et al. 2019). Using these techniques, the cloud environment can operate with anonymized or tokenized data, thereby minimising the risk of divulging sensitive information (Domingo-Ferrer, Farras et al. 2019). *Classification and Labelling of Data:* Businesses can classify and label their data in the cloud environment, ensuring that the appropriate security controls are implemented based on the sensitivity of the data (Younis, Kifayat et al. 2014). This helps maintain consistent security practises and enforce data classification-based access controls (Shaikh and Sasikumar 2015). *Auditing and Logging:* Cloud service providers provide auditing and logging capabilities, enabling enterprises to monitor and analyse user activities, access attempts, and modifications made to cloud-based data (Ko, Jagadpramana et al. 2011); Rasheed 2014). These records provide visibility into security events and support compliance investigations. *Secure Development Lifecycle (SDL):* Enterprises can incorporate secure coding practises, vulnerability assessments, and security testing when developing cloud-based applications or services (Kumar and Goyal 2020);

(Kritikos, Magoutis et al. 2019). This ensures that cloud-based systems are designed from the beginning with security in mind.

*Identity and Access Management (IAM)*: Cloud providers offer Identity and Access Management (IAM) solutions that facilitate centralised management of user identities, authentication, and authorization (Sharma, Dhote et al., 2016). These capabilities enable enterprises to enforce strong authentication methods, implement least privilege access, and administer user provisioning and deprovisioning in the cloud. *Security Information and Event Management (SIEM)*: Cloud-based SIEM solutions can aggregate and analyse security records from cloud-based resources and applications (Van Niekerk and Jacobs, 2013). This enables enterprises to detect and respond to security incidents in real time, even in the cloud.

When employing cloud computing, it is essential for businesses to evaluate the security and compliance capabilities of the cloud service provider. By combining these cloud-specific security measures with the previously mentioned data management security models, enterprises can mitigate risks and safeguard their data in a cloud-based enterprise system. It can be argued that identity and access management can provide the solution to data security in the cloud, but this model is still largely dependent on human factors (Indu, et al., 2018). Things like credential theft (Esparza, 2019), strong password authentication, duplicate passwords, and unauthorized app usage within the enterprise are still some of the hot solutions and issues that mostly surround the human factor. (Lacey, 2009; Brown, 2018).

The set of policies, procedures, technologies, and controls that function jointly to safeguard cloud-based systems, infrastructures, and data is known as the Cloud Computing Security Model (CCSM) (Eya and Weir 2021; Chen and Zhao, 2012). A study of various identified cloud computing security models with a close look at the model that addresses the data security challenges of a cloud-based ERP system showed that all CCSM have the similar objective of safeguarding the cloud system, but the Multi-Cloud Database Model (MCDM) is more focused on protecting data in the cloud

(Che et al., 2011; Eya and Weir, 2021). The MCDM was studied to find a way to ensure end-user experience is accommodated in the design and development stage. This dissertation proposes a cloud computing security framework that uses Enterprise Access Directory (EAD), Enterprise Data Fragmentation (EDF) in the cloud, and End-user Access Quires (EAQ). The new framework will consider the end-user role and responsibility within the enterprise to determine the level of access and the set of data to be accessed in the cloud. Securing the enterprise data is achieved by ensuring no single end-user can access the whole enterprise cloud database in one instance (Mather et al.,2009).

The significance of research in Nigeria cannot be overstated, since its significance varies from presenting new ideas to facilitating greater perception, obtaining the best information, extending one's knowledge base, addressing problems, and enhancing one's general talents. Our research on the role of human factors on enterprise system data security in Nigeria's public cloud is essential for Nigerian enterprise operations, digital transformation of the Nigerian enterprises, and the growing utilization of cloud-based ERP systems within the Nigerian enterprises. Our research addresses data security concerns from the adopting end-user perspective, compliance and regulations, employee training and awareness, challenges associated with cloud adoption, and have academic and professional contributions, and policy recommendations. Understanding the role human factors in cloud security and end-user security responsibility can assist enterprises in aligning their practises with legal requirements, enhancing employee training and awareness, and facilitating the migration of Nigerian enterprises to the cloud. In addition to contributing to academic knowledge and policy recommendations, this research can shape the direction of Nigerian national cybersecurity strategies. Understanding the impact of human factors on enterprise system data security and the role of an adopting end-user in their enterprise data security in the public cloud in Nigeria is crucial for improving data security practises, fostering informed decision-making, and contributing to digital transformation and cybersecurity resilience. Cyberspace and the Internet have an effect on almost every part of a person's life. Today, computers and the Internet help run financial institutions in Nigeria, the justice system, oil and gas firms, airlines, hospitals, the communication industry,

transportation, government, education, and other important parts of a country's economic life (Ogunsola and Aboyade, 2005). We believe that behind this progress in technology, however, the use of the cloud-based ERP systems can and does pose a threat to data security and growth of those establishments. Foreign intelligence agencies, hackers, and other groups of online criminals can put a country's security at risk and hurt its economy, government, and society (Rudner, 2013).

As a result, cyber threats, cyber-attacks, and cyber-crime are at an alarming level in Nigeria right now. Oni, Berepubo et al., (2019) stated that statistics from around the world show that Nigeria ranks very high in the area of cybercrime. In addition, due to the frequency with which individuals and organizations store and transmit information electronically in Nigeria, the demand for information security cultures within the enterprises has increased significantly (Ayof and Irwin, 2010 ; Adebola, 2014). Information security risk management in the context of an adopting enterprise in Nigeria entails preventing unwanted access to information, electronic data at rest or in transit, software applications, and hardware (Derenyiello and Joseph, 2018). According to Lundgren and Moller (2019); Carroll, (1990), the primary objectives of information security are to secure the confidentiality, integrity, and accessibility of data.

This investigation was driven by the fact that public outrage about cyberattacks in the Nigerian oil and gas sector has increased (Mohammed, Reinecke et al., 2022; Achunike and Egbuna, 2016). According to a 2022 report by Sophos, 71% of Nigerian organizations were hit by ransomware in the past year, yet some of Nigeria's worst cybersecurity incidents are still not reported. A report from Guardian Nigerian newspapers titled "Cyber-attack on Nigerian SMEs up by 89 per cent in 2022" on 31 May 2022 written by Adeyemi Adepotun started that "researchers from Kaspersky who looked at how attacks on small and medium-sized businesses (SMEs) in Nigeria changed between January and April 2022 and the same time period in 2021 warned that these threats pose a growing risk to entrepreneurs. When compared to the same time period in 2021, there were more than twice as many Trojan-Password Stealing Ware (PSW) detections in Nigeria in 2022 as there were in 2021. In 2022, there were

2654 detections compared to 1076 in 2021. Trojan-PSW is malware that steals passwords and other account information. This lets attackers get into the corporate network and steal sensitive information. The cyber security company said that another common way to attack small businesses is through the Internet, especially through web pages. Even though there were less of these attacks in Nigeria in the first four months of 2022 than in the first four months of 2021 (56,836 infections in 2022 compared to 99,146 infections in 2021), the report said that Internet attacks are still a problem that needs to be guarded against. In the first four months of 2021, Kaspersky found and stopped 161,000 RDP attacks in the country”. This demonstrates shortcomings in the Nigerian SME's management of information security of their ERP systems. To identify and resolve these issues, it is necessary to investigate the factors impacting the implementation of information security risk management in the SME business, particularly in Nigerian oil and gas; hence, this proposal for research.

Empirical studies such as: (Ali, Usman et al., 2021; Ukwandu, Okafor et al.,2023; Yeboah-Boateng, 2013) and (Ifinedo, Mengesha, et al., 2019) have been undertaken thus far in an effort to identify the factors that influence information security threats in developing nations such as Nigeria, where the threat posed by organization insiders continues to be one of the primary difficulties facing SMEs, there are numerous unresolved issues related with inefficient information security policies and culture within Nigerian enterprises. Our research examines the key direct and indirect human factors that influence the development and adoption of a cloud-based ERP systems in the context of enterprise information security culture and staff security responsibility and cloud-based ERP implementation best practices in SMEs organizations in Nigeria.

### **1.3 Research Motivation and Novelty**

Digital transformation is still fairly new to the Oil and Gas industry in Nigeria (Inuwa, 2022). From the upstream to the downstream, the industry has been under constant pressure to join the digital revolution (Akintokunbo and Arimie, 2021). Only recently have they started to accept new technologies like Artificial Intelligence (AI), the use of drones, Robotic Process Automation (RPA), Machine Learning (ML), and the

Internet of Things (IoT) (Wanasinghe et al., 2020). We believe that both parts of the industry will be able to do better with the help of cutting-edge technology. After the pandemic and the oil price crash, organizations have had to rely on their digital assets to stay afloat (Ozili, 2021). In the Oil and Gas industry, there is a growing push to improve sustainability (Okeke, 2021). When you add in the desire to make more money, make better decisions, and get the most out of your employees, you have to have a strong digital framework that includes Robotic Process Automation (RPA), Internet of Things (IoT), and Machine Learning (ML), and you have to use drones (Wanasinghe et al., 2021; Inuwa, 2022).

To their credit, the majority of businesses across oil and gas industries in Nigeria are shifting to the cloud at now (Bello, 2021). Maximizing asset production and revolutionizing data – making data universally accessible and facilitating a well-structured management of business processes – are among the numerous advantages of migrating to the cloud-based ERP systems, all of which we believe stem from the complete digitization of the organization on the cloud (Nguyen, 2020; Johansson et al., 2015). However, we believe the Nigerian Oil and Gas industry is far from perfect on the route to complete digitization. Although the Nigerian Oil and Gas industry has gotten off to a poor start, now is the time to act. This research was inspired by a challenge the researcher and colleagues had to deal with when implementing Microsoft Dynamics AX for an oil service firm in Nigeria. The management refused all pleas from the team to host their software application on the cloud, even when that meant reducing the cost of implementation by 38%. The reason the management gave was that their employees were not ready for such a cloud computing technology transition. They had serious concerns about their data security and how their employees would handle data losses.

It left the team and the researcher with the question, "Is there a relationship between enterprise data security in the cloud and the adopting enterprise employee?". There was a gap as most research focused on cloud service providers and not on the adopter's enterprise end-users. This curiosity led to this research which will answer this question

and reassure enterprises to embrace cloud computing. They need to know that they can adopt cloud computing while still maximizing data security in the cloud.

This research presents an *end-user centric access control framework for enterprise systems running on public cloud infrastructure*. The proposed framework will define what the best approaches for implementation of a cloud-based ERP systems within an enterprise. The proposed framework has two separate phases: the first security phase is handled by the adopting enterprise end-users, and the second phase is handled by the CSP enterprise. The first security responsibility phase is when the adopting enterprise classifies its data sets according to their security importance and prepares its Enterprise Cloud Directory using its distinctive enterprise roles and responsibilities against the already classified dataset. The security responsibility of this first phase is managed by the adopting enterprise end-users. The second phase starts when a classified adopters end-user uses the correct username and password to have access to a fragment of the enterprise database in the cloud. The second phase has three features: the *CSP Access Directory*, the *Enterprise Database Fragmentation*, and *End-user Access Queries* (Eya and Weir, 2021). The three features are managed by the Cloud Service Provider (CSP) and their security responsibilities are solely the CSP's to ensure. The proposed framework, when compared with other exciting models, will encourage more adopter's end-user participation in their enterprise data security in the cloud. The model also mitigates the impact a malicious insider will have on the enterprise cloud data set in the cloud since no single user can gain access to the whole enterprise database in the cloud at the same time.

#### **1.4 Research Aim and Objectives.**

The main objective of this research is to propose a framework for choosing the best approach for the implementation of a cloud-based enterprise resource planning (ERP) systems within an enterprise, putting into consideration the security responsibility of the adopting enterprise end-users. The following small aims put together will achieve the main objective of the research.

- A thorough review of the academic literature on cloud computing security models and enterprise resource planning systems.
- To propose a new cloud-based ERP implementation approach: the end-user centric access control framework for enterprise resource planning systems running on public cloud infrastructure.
- To evaluate the proposed framework with IT professional of the industry, in order to seek for evidence in attributes of the proposed framework being ok.
- The primary data collected from the study was used to review the proposed framework attributes. Both the secondary data from the literature review and the primary data collected were utilized in analysing and evaluating the critical attributes of the end-user centric access control framework for enterprise resource planning systems running on public cloud infrastructure that can be widely adopted in the design and implementation of a cloud-based ERP system.

### **1.5 Research Questions**

The major goal of this research is to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. This study goal is accomplished by analysing the present status of cloud computing security models. It also examines the essential human factor elements that influence the adoption of a cloud-based ERP systems in such organisations. This research main objective is to propose a framework for choosing the best approach for the implementation of a cloud-based enterprise resource planning (ERP) systems within an enterprise, putting into consideration the security responsibility of the adopting enterprise end-users.

A narrative review of our research questions is presented in the Section 3.1 of the Chapter 3 of this thesis. The following questions were posed to address the research problem, and achieve its aim and objectives: (RMQ= Research Main Question, RQ= Research Question):



**RQ1:** How important is end-user access control in ensuring enterprise data security in the cloud?

**RQ2:** How important is shared security responsibility between a CSP and an enterprise end-user in ensuring enterprise dataset security in a cloud-based ERP system?

**RQ3:** To what extent should enterprise dataset classification form part of a cloud-based ERP implementation to promote enterprise data security in the cloud?

**RQ4:** To what extent can enterprise database fragmentation in the cloud improve the enterprise data security of a cloud-based ERP software system?

**RQ5:** To what extent can cloud computing have an impact on enterprise system data security?

The research question was examined using the following relating research assumptions which a detailed explanation of the concepts behind the eight research assumptions with citations can be found in Section 1.6 in Chapter 1 of this thesis.

**A1:** Participants who have worked with a cloud-based ERP system are more likely to provide a valid response to our research survey.

**A2:** Ideally, any upgrade in technology should have an impact on the previous technology, although this impact can either be positive or negative. Therefore, Cloud computing would have an impact on Enterprise system data security in Cloud.

**A3:** When the Cloud Service Provider and the Cloud Service End-users share the security responsibility of the cloud system, it will result in more secured enterprise data in the cloud.

**A4:** A proper Access Management within the Cloud Service End-user enterprise would positively improve their enterprise data security in Cloud.

**A5:** The proposed CSP Access Directory when implemented, would improve Access Control Management in the Cloud.

**A6:** Enterprise data set classification when carried out as an integral process of moving enterprise data set to the Cloud would help in creating the Enterprise Access Directory and improve Enterprise data security in Cloud, since only classified data are moved.

**A7:** System notification to the Enterprise System Administrator when there is an unsuccessful login attempt is more likely to promote Enterprise data security in the Cloud.

**A8:** Enterprise Database Fragmentation in the Cloud would improve Enterprise data security of a Cloud-based ERP system.

## **1.6 An Understanding of Our Research Assumptions**

As a starting point for conducting research, a research assumption is a proposition or statement that the researcher assumes to be true (Chigbu, 2019). As foundational beliefs or premises that guide the research process and influence the formulation of research questions, hypotheses, and the overall methodology, assumptions serve as the basis for research (Chigbu, 2019). Because research cannot be conducted in a vacuum due to limitations of time, resources, and practicality, these assumptions are often necessary. Existing knowledge, prior research findings, common sense, expert opinion, or theoretical frameworks may inform assumptions (Chigbu, 2019). Chigbu, (2019) states that research assumptions aid in defining the scope and limits of an investigation and provide context for interpreting the results. In order for readers to comprehend the underlying beliefs and premises upon which the study is based, it is crucial for researchers to state their assumptions explicitly in their research papers. In addition, acknowledging assumptions helps maintain the research process's transparency and credibility (Pratt et al., 2020). For our research we have eight research assumptions, which will be discussed in detail in the following paragraphs below, these assumptions formed the foundation that guided our research activities, for example, creating our research questions, choosing our targeted research participants and focusing on the best research methodology in conducting our research.

Participants with prior experience working with cloud-based enterprise resource planning (ERP) systems are more likely to provide relevant and valuable responses to research surveys. This is due to their familiarity with technology, contextual understanding, detailed insights, user perspective, ability to address challenges and benefits, informed responses, and potential subject matter expertise. Familiarity with

technology is crucial for participants to understand the impact of cloud-based ERP systems on enterprise operations (Das and Dayal, 2016). They have firsthand knowledge of how these technologies affect day-to-day operations, decision-making, and overall efficiency, allowing them to provide nuanced and educated responses.

Cloud-based ERP systems typically come with unique features and functionalities, making them unique from traditional ERP systems (Akin et al., 2014). Users with experience with cloud-based ERP systems can provide a user-centric perspective, providing insights into the user interface, ease of use, training required, and user satisfaction. This perspective is essential for understanding the practical implications of implementing these systems and identifying areas for change. Participants who have used cloud-based ERP systems in the past are likely to have experienced both obstacles and benefits, providing insights on issues such as data migration, system unavailability, user adoption, and ongoing maintenance. They may also emphasize benefits such as enhanced data accessibility, real-time reporting capabilities, and collaboration more effectively. Informed responses are less likely to be general or ambiguous, as respondents with prior experience can provide specific, examples, and in-depth explanations. This breadth and calibre of responses improve the quality of the research data collected.

In conclusion, we assumed that participants with prior experience with cloud-based ERP systems are more likely to provide valid responses to our research surveys due to their familiarity with the technology, contextual understanding, specific insights, user perspective, ability to address challenges and benefits, informed responses, and potential subject matter expertise. Their contributions can improve the overall quality and applicability of research findings. Hence our first research assumption is that **“A1: Participants who have worked with a cloud-based ERP system are more likely to provide a valid response to our research survey.”**

The principle that any technology upgrade should impact previous technologies emphasizes the interconnected nature of technological advancements (Perez, 2004).

The introduction of cloud computing has a significant impact on enterprise system data security, with positive outcomes such as enhanced security practices, access to expert expertise, and innovation adoption (Elragal and Haddara, 2013). However, negative impacts include dependency on third parties, data exposure risk, integration challenges, and lack of control. Cloud service providers often invest heavily in security infrastructure, such as advanced encryption, intrusion detection, and regular security audits, which can positively influence security standards and practices within enterprise systems (Sharma et al., 2016).

Integration challenges can arise from compatibility issues not being addressed immediately, leaving potential entry points for cyberattacks (Akin et al., 2014). Additionally, enterprises may have less direct control over their data security in the public cloud environment compared to their on-premises systems, leading to concerns about compliance, data governance, and regulatory requirements (Mallo and Ogwueleka, 2019). In conclusion, the impact of cloud computing on enterprise system data security depends on how well security measures are integrated and managed within both cloud and on-premises systems. Therefore, it is safe to assume that **“ideally, any upgrade in technology should have an impact on the previous technology, although this impact can either be positive or negative. Therefore, Cloud computing would have an impact on Enterprise system data security in Cloud.”** This assumption is what we took as our research assumption A2.

The shared responsibility model is a collaborative security method that divides the responsibility for maintaining the safety of a cloud computing environment between the Cloud Service Providers (CSPs) and the Cloud Service End-users (CSEUs) (Hwang et al., 2011). This concept improves the overall safety of enterprise data stored in the cloud by drawing on the capabilities that both parties bring to the table. The concept includes a distinct separation of responsibilities, with CSPs controlling the safety of the cloud infrastructure itself, while CSEUs are responsible for the protection of their own cloud-based applications, data, and configurations (Eya and Weir, 2021). Therefore shared responsibility model is a collaborative security method.

CSPs have substantial expertise in managing and securing cloud infrastructure, having invested in the most cutting-edge security tools, technologies, and best practises available (Mell and Grance, 2009). By drawing on the knowledge and experience of CSP, CSEUs have the opportunity to attain a greater level of security than they would be able to on their own. CSPs are able to invest in more advanced security measures thanks to the economies of scale and automation that enable them to do so. These measures include intrusion detection systems, powerful firewalls, and security information and event management (SIEM) technologies (Sundareswaran et al., 2012). CSEUs retain control over their applications and data, giving them the ability to personalise their security procedures in accordance with the requirements that are unique to them (Eya and Weir, 2021). This degree of control makes certain that the safety precautions taken are commensurate with the sensitive nature of the data that is being processed.

Both the CSPs and the CSEUs continually monitor the environment to look for potential security threats and vulnerabilities. This makes shared vigilance a vital component of the shared responsibility paradigm. CSPs offer CSEUs the tools and dashboards necessary to monitor the security posture of their resources, hence enhancing the likelihood that security events will be discovered and remedied in a timely manner. In a model of shared responsibility, in which each party is responsible for regularly assessing and improving security measures, continuous improvement is an absolute necessity (Eya and Weir, 2021). CSPs are required to continually update their security architecture in order to keep one step ahead of new threats, whereas CSEUs are required to be knowledgeable regarding best practises, security updates, and any vulnerabilities in their applications.

Due to the fact that many different sectors have their own industry-specific regulatory standards that regulate data handling and security, compliance and regulations are also a crucial component of the shared responsibility model. The entire security posture of the cloud environment is improved as a result of the provision of educational resources, guidelines, and training materials by CSPs to CSEUs for the purpose of facilitating the

CSEUs' comprehension of and compliance with security best practises within their respective cloud installations (Jaatun et al., 2020). Finally, the shared responsibility model encourages a cooperative approach to cloud security. In this model, cloud service providers (CSPs) are responsible for providing robust infrastructure and security measures, while cloud service end users (CSEUs) are responsible for safeguarding their own applications and data within the cloud (Jaatun et al., 2020) (Eya and Weir, 2021). However, in order to ensure the successful execution of security measures, it is essential for all parties to have a good understanding of the duties and responsibilities that are assigned to them. Hence our research assumption **A3** states that **“when the Cloud Service Provider and the Cloud Service End-users share the security responsibility of the cloud system, it will result in more secured enterprise data in the cloud”**.

Proper Access Management is essential for preserving the security and integrity of a enterprise's sensitive data and digital assets in the cloud (Wang et al., 2010). Controlling data access, adhering to the principle of least privilege, employing robust authentication methods such as multi-factor authentication (MFA), assigning specific roles to users based on their responsibilities, and providing audit trails and monitoring capabilities are all components of data security (Iluore et al., 2020). Managing user accounts, permissions, and access policies across multiple cloud services from a single dashboard requires centralised management (Iluore et al., 2020).. This facilitates administration simplification and assures uniformity of security measures. When users change roles, depart the enterprise, or no longer require access to certain resources, access can be revoked promptly.

Compliance and regulations are essential for numerous industries, and proper Access Management enables enterprises to adhere to these regulations by preserving granular control over data access (Wang et al., 2010).. To enhance security, cloud service providers offer various access management tools and features, such as Amazon Web Services' (AWS) Identity and Access Management (IAM) services and Microsoft Azure's Azure Active Directory (Boneder, 2023). It is also essential to cultivate a

culture of security awareness among adopting enterprise end users, encouraging them to consider security implications and best practises when accessing cloud resources (Eya and Weir, 2021). Through the implementation of controlled access, effective authentication, and role-based controls, organisations can significantly improve their cloud data security posture. Hence our research assumption **A4** which states that **“A proper Access Management within the Cloud Service End-user enterprise would positively improve their enterprise data security in Cloud.”**

Implementing a Cloud Service Provider's (CSP) Access Directory in the public cloud can significantly enhance access control management by providing centralised Identity and Access Management (IAM), efficient Role-Based Access Control (RBAC), simplified user onboarding and offboarding, multi-cloud management, enhanced security with Multi-Factor Authentication (MFA), audit trail and compliance, and enhanced access monitoring and threat detection (Eya and Weir, 2021). A well-implemented CSP Access Directory can provide a single point of control for managing user identities, roles, and permissions across multiple cloud services and resources, thereby reducing complexity and preventing inconsistent or erroneous permission assignments (Hrishev, 2020). Additionally, it facilitates user onboarding and offboarding, thereby reducing the risk of lingering access rights for users who no longer need them (Eya and Weir, 2021).

In addition, a CSP Access Directory can enforce additional layers of authentication, making it more difficult for unauthorised users to gain access, even if their credentials have been compromised (Kumari and Nath, 2018). It also maintains comprehensive logs of access attempts, permission changes, and other activities, ensuring regulatory compliance and monitoring potentially malicious activities (Kumari and Nath, 2018). With a centralised directory, improved access monitoring and threat detection are also possible (Eya and Weir, 2021). Finally, a properly implemented CSP Access Directory can substantially improve access control management in the public cloud by enhancing security, operational efficiency, and administrative simplicity (Eya and Weir, 2021). However, the actual benefits depend on implementation specifics, integration with

existing systems, and alignment with an enterprise's particular security and compliance requirements. Therefore, one of our research assumptions **A5**, is that **“The proposed CSP Access Directory when implemented, would improve Access Control Management in the Cloud.”**

Classifying enterprise data sets prior to migrating them to the Public Cloud has numerous advantages, including data understanding and categorization, access control, minimised exposure, data protection compliance, encryption and data loss prevention (DLP), intrusion detection and monitoring, resource optimisation, incident response, data lifecycle management, and cost efficiency (Andrikopoulos et al., 2013). By classifying data according to its nature, sensitivity, and purpose, enterprises can better manage and safeguard their data assets while maximising the benefits of cloud computing.

Data classification enables enterprises to comprehend the nature, sensitivity, and purpose of their data by classifying it into various classes or levels based on its sensitivity, regulatory requirements, and access controls (Ben-David et al., 2010). This enables more effective access control mechanisms in the public cloud, ensuring that only authorised users and applications have access to sensitive data. Moving only classified data to the cloud reduces the attack surface by minimising the exposure of sensitive information (Eya and Weir, 2021). Moreover, classification ensures compliance with data protection regulations by managing sensitive data and employing the appropriate security controls. Encryption and data loss prevention (DLP) are also improved by categorising data based on its sensitivity, thereby enhancing protection against accidental or intentional data breaches (Hauer, 2015). The classification of data access patterns simplifies intrusion detection and monitoring. Resource optimisation is accomplished by optimising resource allocation for critical or frequently accessed data and prioritising response and recovery efforts in the event of security incidents or breaches. Data classification also contributes to data lifecycle management by facilitating the establishment of data retention and disposal policies (Ben-David et al., 2010).



Furthermore, the classification of enterprise data sets prior to migration to the Public Cloud is a strategic method for augmenting data security, regulatory compliance, and resource efficiency (Hauer, 2015). By transferring only classified data, enterprises can potentially reduce the volume of data transmitted and stored in the cloud, thereby saving money. We therefore assumed in our research assumption **A6** that **“Enterprise data set classification when carried out as an integral process of moving enterprise data set to the Cloud would help in creating the Enterprise Access Directory and improve Enterprise data security in Cloud, since only classified data are moved.”**

When an unsuccessful login attempt occurs in a cloud-based enterprise environment, notifying Enterprise System Administrators with a system notification can substantially improve data security (Eya and Weir, 2021). This strategy includes immediate awareness, proactive threat detection, rapid incident response, user behaviour analysis, policy and configuration adjustments, documentation and compliance, educational opportunities, early warning for compromised accounts, incident analysis and learning, and an all-encompassing security strategy. Notifications in real-time enable administrators to respond quickly to potential security violations, investigate the attempt, evaluate its severity, and take the necessary steps to prevent unauthorised access (Eya and Weir, 2021). Continuous monitoring of failed login attempts provides administrators with insights into prospective brute-force attacks or unauthorised access attempts, enabling them to identify patterns and trends prior to the occurrence of actual security breaches (Al-Mohannadi e al., 2020).

According to Boriky, et.al; (2019), receiving recent notifications about failed logon attempts enables administrators to fine-tune security policies and configurations, thereby enhancing the cloud environment's overall security posture. Rodrigues, et al; (2013) in their paper titled “Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records System” stated that documentation and compliance are essential for monitoring and maintaining security, while educational

opportunities provide opportunities for educating users on password management best practises, phishing assaults, and security hygiene. We believed that early warnings for compromised accounts can aid in the identification of compromised accounts and the implementation of corrective measures, such as mandating password resets. Therefore, sending notifications for failed login attempts is advantageous, but it should be part of a comprehensive security strategy that also includes multi-factor authentication, strong password policies, network monitoring, intrusion detection systems, routine security audits, and user education. Additionally, sensitive data, such as the content of notifications, should be handled with care to prevent further security vulnerabilities. We assumed in A7 that **“System notification to the Enterprise System Administrator when there is an unsuccessful login attempt is more likely to promote Enterprise data security in the Cloud.”** This we hoped would improve the overall outlook of the cloud environment.

Enterprise database fragmentation is the division of a database into smaller sections or fragments, typically in distributed databases (Özsu and Valduriez, 1999). Ashish, (2014) mentioned that there are various fragmentation varieties, such as horizontal, vertical, hybrid, location, and replication. These fragments can improve query performance and contribute to fault tolerance. Noraziah, Fauzi, et al. (2021) believed that to ensure data consistency and integrity, managing fragmented databases requires careful consideration of data distribution, synchronization, and maintenance. We believe that fragmentation of enterprise databases can improve query performance, scalability and security. However, it complicates data distribution, synchronization, consistency, and administration. Therefore, fragmentation would require a well-designed strategy to maximize benefits without jeopardizing data integrity or efficacy.

We believe that fragmentation can enhance data security in cloud-based ERP systems by isolating data, reducing attack surface, assigning role-based access control, encrypting data independently, mitigating insider threats, minimising data exposure, ensuring compliance, enhancing disaster recovery and masking data. Although according to Otuonye, (2021), the goal of enterprise database fragmentation in a

Cloud-based ERP system is to improve data security by mitigating the effects of potential intrusions and unauthorised access. This strategy we believe entails slicing data into smaller, isolated fragments that are dispersed across multiple locations or servers in a cloud infrastructure. Sarathy et al., (2010) stated that distributing fragments across multiple virtual servers enables dynamic scaling and more efficient resource allocation. While fragmentation increases security, it complicates data distribution, synchronisation, and administration. Regardless, we assumed in our assumption A8 that “**Enterprise Database Fragmentation in the Cloud would improve Enterprise data security of a Cloud-based ERP system.**” Although some authors like (Otuonye, 2021; Eya and Weir, 2021; Mezgár and Rauschecker, 2014) already suggested this idea, but we are also hoping to get the views of our research participants in this regard, as fragmentation also forms a critical part of our proposed framework.

### **1.7 Research Contributions and Limitations**

Our study provided an insight into the impact of Cloud Computing on Enterprise System Security and the need for end-users to have a greater security responsibility within their enterprise (Eya, 2023). Our research contributed to the current knowledge of the cloud security model by demonstrating using the proposed framework the importance of enterprise dataset classification, cloud enterprise database fragmentation, and enterprise access directory as a tool for enhancing enterprise data security in the cloud (Eya and Weir, 2021). Furthermore, our research improves the understanding of the role of human factors in cloud computing security especially the Nigeria oil and gas and SMEs perspectives.

It is expected that the main outcome of our research will help academic scholars do further research on the cloud computing architecture as an emerging IT technology, and where possible, develop a cloud architecture that can encourage more end-user security responsibility, thereby limiting the risk that enterprise employees can pose to the data security in the cloud. This will give insight to company executives on the importance of their employees’ involvement in securing their enterprise data in the

cloud. Company executives will also know the part they can play as an enterprise in ensuring data security in the cloud; for instance, preparing a detailed dataset classification before moving data to the cloud, ensuring that employees only have access to a fragment of the enterprise data they require to work with, and finally, making sure that the CSP performs a database fragmentation of their enterprise database in the cloud. Finally, ensure that no single end-user within their enterprise has access to the whole company database in the cloud.

An IT professional within an enterprise with this insight can develop or modify security models to suit cloud computing technology, having in mind the implications of the actions of the employees who use this system. This will mean that cloud service providers can be persuaded through Nigerian government influence to include in their service level agreement some of the issues the research noted, like the enterprise preparing a detailed dataset classification and having their Enterprise Access Directory before moving their enterprise data to the cloud. This is to ensure the enterprise plays its role in ensuring its data is safe in the cloud.

The limitation of the research can be attributed to the number of participants. Although there are many cloud computing professionals around the globe, we could only get responses from forty-four people, which we used to form the basis of our research findings. We were unable to secure a participating enterprise due to time and financial constraints, even though we have a few enterprises in our initial study who declined to be used as case studies. It is thought that case study research may have given the proposed model different facts to back it up.

### **1.8 Research Methodology Summary**

For this research, we used a four-stage approach, which are the research initiation phase, the research execution phase, the research analysis phase, and the research finalization phase. The research initiation phase involved the initial study, the investigation and prioritization of the various cloud computing security models, A

literature review of the various cloud computing models was carried out, and an end-user authentication control model was proposed. The second phase involved surveying to determine if the views we are proposing in the model are supported or opposed. The third phase involved the review of both our quantitative and qualitative data to understand the opinion of our research participants on the proposed model. The last step was to write down our findings and look over our model.

## **1.9 Thesis Outline**

**Chapter 1: Introduction.** This Chapter 1 reveals the inspiration for the research and the novelty of this research by outlining the research overview, problem domain, research methodology, research aims, research objectives, research contribution, and research limitations. This Chapter 1 introduces the whole concept of research. This is where the overview of the research was discussed. The problem domain was established, and the rationale behind the research was also discussed. This chapter talks about the novelty of the research, the aims and objectives of the research, and the research questions. It also briefly talked about the research contributions and limitations. A summary of the research methodology was also given in this chapter. This chapter concludes by giving the thesis outline to guide the reader through the rest of the thesis.

**Chapter 2: Related Work and Relevant Theories.** This Chapter 2 focuses on the review of literature relating to cloud computing. This chapter of the thesis gives an overview of the literature that is relevant to the research topic. It provides a general understanding of the various concepts that formed the basis of the research, such as enterprise, data, the fundamentals of information security, cloud computing, cloud computing security models, and understanding of the concept of the human factor. The understanding of the reviewed concepts or topics, and the topics discussed in this chapter help the reader with the general knowledge and understanding that propels our research.

**Chapter 3: Research Methodology.** This Chapter 3 discusses in detail the research methodology. The mechanism for collecting data was discussed, as well as the development of the data collection tool. On this chapter, we will discuss the qualitative analysis of the initial interviews. The chosen research method's validity, reliability, and repeatability were established. It was stated that the ethical consideration was made. This chapter also discussed the analysis method chosen, the research approach, and the research implementation. Additionally, the four stages of our research were discussed in detail. This chapter also discusses and illustrates the results of each stage of our research. As this is our methodology chapter, we will summarise our activities by evaluating the perspectives in our proposed model. This chapter discussed the data collection tools we used in detail, as well as the rationale for the various questions included in our research survey. Additionally, this chapter discussed in detail how we collected data, and the data cleaning exercises we conducted before beginning to analyse the collected data.

**Chapter 4: End-user Centric Access Control Framework.** The Chapter 4 of this thesis introduces the novel end-user authentication control model for enterprise systems in the public cloud. This proposed model discussed in this chapter is a major contribution of our research to knowledge. This chapter also contains a comparison of the various cloud security models and our proposed model. The strength and weaknesses of the cloud security models were also discussed in this chapter.

**Chapter 5: Framework Attribute Validation.** This Chapter 5 discusses our data analysis in detail to understand how the views in our proposed model are justified based on the responses of our research participants. This chapter is divided into two parts. The first part is the quantitative research data understanding, where we give a summary of each of the research questions and the data collected. Here we used a bar chart to virtualize the responses gotten for each research question. The second part of this chapter is the statistical data analysis of our research assumptions. The focus of this part is to use SPSS to review the data we collected to uphold or not uphold the views of our proposed model. The following tests were performed and are represented

here by tables and charts: normality test, ordinal regression, parallel line test, and non-parametric correlations.

**Chapter 6: Evaluation and Discussion.** The Chapter 6 is the evaluation and research results discussion chapter. In this chapter, we discuss the information and trends about our research participants and the response rate we got. This is where our research findings are discussed along the lines of our initial research questions, aims, and objectives. The subsections of this chapter are directly an evaluation of our research findings along the lines of the impact of cloud computing on data security systems, end-user security responsibility in ensuring data security in the cloud, the concept of fragmentation of databases, and the concerns regarding the implementation of ERP systems. The sections 6.4 and 6.5 of this chapter discuss the initial interview results and the EAD and CSP AD directories in detail. Section 6.6 summarizes research findings.

**Chapter 7: Conclusion and Recommendations.** In Chapter 7 which is the last chapter of our thesis, we gave a critical evaluation of our research activities by discussing the strength and weaknesses of the research exercise, we discuss the conclusions of our research findings and gave recommendations for future research interests. This is the last chapter of our thesis is followed by the Reference session and the Appendix session.

### **1.10 Summary of Chapter 1**

The adoption of enterprise resource planning (ERP) solutions by enterprises can be dated back to 1970s (Bjelland and Haddara, 2018; Zmud, 1980; Van der Molen, 1970). The major challenges that enterprises face are the associated infrastructure and maintenance costs. Cloud computing allows enterprise access to a set of networked servers using the internet (Van der Molen, 1970). Hybrid cloud allows the enterprise to combine two or more deployment models for their best interest. Cloud computing is an emerging IT technology that provides on-demand services to end-users over the

internet. Enterprises have been keen on cloud-based ERP software as it is more affordable than traditional on-premises ERP systems. Human behaviour is the main context in protecting or bridging data security in the cloud. Credential theft, strong password authentication, duplicate passwords, and unauthorized app usage are still some of the hot solutions and issues that mostly surround the human factor.

The main objective of this research is to propose a framework for choosing the best approach for the implementation of a cloud-based enterprise resource planning (ERP) systems within an enterprise, putting into consideration the security responsibility of the adopting enterprise end-users. The research outcome will help academic scholars do further research on cloud computing architecture. This is to ensure the enterprise plays its role in ensuring its data is safe in the cloud. The limitation of the research can be attributed to the number of participants. We were able to secure a participating enterprise for the initial study and used a mixed method approach for the data collection for the main study. A literature review of the various cloud computing models was done, and an end-user centric access control framework for enterprise systems running on public cloud infrastructure was proposed. The thesis gives a general understanding of the various concepts that formed the basis of our research. The tools we used in the collection of data were discussed, as well as the different research questions and research assumptions.



## Chapter 2. Related Work and Relevant Theories

This chapter of the thesis gives an overview of the literature that is relevant to the research topic. Chapter 2 serves as an introduction to the overarching research framework, delineating key components and concepts. Section 2.1 provides an overview of enterprises, setting the foundation for subsequent discussions. Section 2.2 delves into the intricacies of data, elucidating its significance within the research context. In Section 2.3, fundamental principles of information security are expounded upon, laying the groundwork for understanding security dynamics. Following this, Section 2.4 delves into the realm of cloud computing, exploring its implications within enterprise settings. Transitioning into more specialized domains, Section 2.5 dissects cloud computing security models, offering insights into various frameworks and approaches. Section 2.6 deepens the discourse by examining human factors and their influence on security paradigms. Section 2.7 provides a systematic literature review on the adoption of ERP systems, synthesizing existing research in this domain. Meanwhile, Section 2.8 offers a narrative review on the pivotal role of end-user security responsibility in safeguarding enterprise data within cloud environments. Concluding the chapter, Section 2.9 offers a comprehensive summary of the diverse topics covered throughout Chapter 2, encapsulating key findings and insights gleaned from the literature review process.

Our research gap was identified from the understanding of the reviewed concepts or topics, and the topics discussed in this chapter help the reader with the general knowledge and understanding that propels our research. The Figure 2.1 below shows the overview of the review outcome. As argued by Bryman (2008), a literature review is the opportunity a researcher or an author will have to identify, analyse, and compare all other existing literature relating to their research in a way that gives rise to logical arguments or conclusions. There are various methods that can be used to carry out a literature review, such as: traditional or narrative literature reviews, scoping reviews, systematic literature reviews and annotated bibliography. For the majority of our

review, we utilized the narrative literature review method because narrative literature reviews provide a comprehensive summary of existing research on a particular subject, enabling readers to comprehend the current state of knowledge without the need for complex statistical analyses or meta-analyses. They identify research gaps and develop theoretical frameworks, investigate various perspectives, provide historical context, inform policy and practice; and serve as preliminary or exploratory research in emerging or understudied fields. However, narrative reviews differ in methodology and rigor from systematic reviews and meta-analyses.

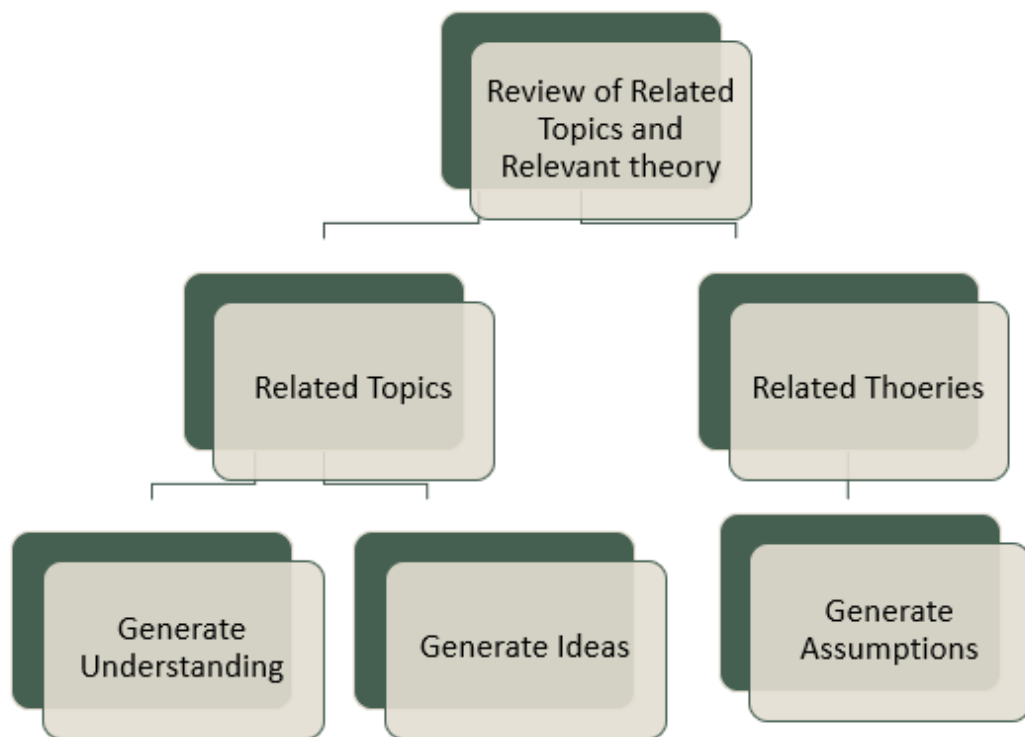


Figure 2.1: The overview of what this Chapter stands to achieve. (Eya 2023)

For the section 2.7 where we conducted a systematic literature review on the adoption of ERP systems within enterprises, we adopted a systematic literature review method here because this reviews are a rigorous and thorough method for synthesizing existing research, providing evidence-based decision-making, minimizing bias, identifying gaps, pooling and synthesizing data, resolving conflicting evidence, assessing study quality, enhancing generalizability and external validity, supporting research synthesis, and ensuring transparency and reproducibility. In addition, they assist in resolving conflicts, evaluating the quality of studies, and ensuring the generalizability of findings beyond individual studies. Systematic reviews also contribute to research

synthesis by providing an exhaustive overview of previous work and ensuring its reproducibility and transparency. Overall, systematic literature evaluations are essential for evidence-based research, policy development, and decision-making, advancing knowledge and enhancing practices in a variety of academic disciplines. We took into consideration the nature of our research purpose and objectives of our study when deciding to adopt both narrative and systematic literature review methods.

## **2.1 The Enterprise**

Companies, institutions, firms, and corporations that are set up to help society are called enterprises (Utting, 2005). They can be for-profit or not for profit (Dees and Anderson, 2017). Another perspective defines an enterprise as an entrepreneurial venture that is strictly a profit-making company (Choi and Gray, 2008). It is believed that any entity set up to do business can be referred to as an enterprise (Dobrin, 2015). In many cases, an enterprise is a legal entity that is duly registered with the government of the state where the enterprise is located. When you think of a business as a legal entity, you can group it into different types, like a sole proprietorship, a partnership, a limited liability company, a public limited company, and a professional limited liability company (Raczyńska, 2019).

A "sole proprietorship" is a business that is owned and run by one person for his or her own gain (Crusto, 2001). It is usually responsible for any problems that could happen because of the business. This means that the person will be responsible for anything that goes wrong in the business (Crusto, 2001). On the other hand, a business is called a partnership when two or more people own it together (Waddock, 1988). This type of business is where most family businesses can be found. Also, a corporation is a type of business where the owners are protected from anything unexpected that might happen because of how the business is run (Winter Jr, 1977). Shares in these businesses have limited liability. For example, there are limited liability enterprises, public limited liability enterprises, and professional limited liability enterprises (Carney, 1994). Moreover, the enterprise can be classified using different criteria like the number of

employees, type of legal entity, nature of their judicial subject, type of operation, and place of operation (Fay, 1998); (Raczyńska, 2019).

Looking at an enterprise by its *type of operation*, an enterprise can either be profit-oriented or non-profitmaking (Ng'ethe, 1989). For non-profit making, we have NGOs, community organizations, fundraising, etc. as examples of such enterprises. Profit-oriented enterprises are every other enterprise that is created for profit-making. For instance, we have manufacturing enterprises, sales enterprises, etc. When classifying an enterprise according to the *nature of its judicial subject*, it can either be a state-owned enterprise or a privately owned enterprise (Kowalski et al., 2013). Private-owned enterprises are enterprises where the running of the enterprise's activities is carried out by the owners. As an example of a business that is owned by its owners, a sole proprietor is a business that has its owners as managers, administrators, organizers, and so on. A state-owned enterprise is an enterprise where the running of the enterprise's activities is carried out by a public body representing the state, and its activities are normally in the common interest of everyone. For example, the different government commissions, etc., are examples of state-owned enterprises. The ownership of religious organization is different from one country to the other, but in many instances religious bodies can be classified as state own enterprises (Princewell, 2017).

An enterprise can either be local or international when classified by *place of operation* (Castellani, 2022). It is "local" when the enterprise is located and operates within the same country where it is legally registered. An enterprise is international when it carries out its operations on a global level. It could have branches in different countries, not just the country where it was legally registered. When classifying an enterprise by the *type of legal entity*, one can have various forms, such as sole proprietorship, partnership, limited liability company, public limited company, and professional limited liability company (Halpern, 1980). Finally, when distinguishing enterprises by the *number of their employees*, there can be four categories, such as micro-enterprise, small enterprise, medium enterprise, and large enterprise (OECD, 2022). A micro-

enterprise is an enterprise whose staff strength is between one and nine. Many of the sole proprietors fall under this category. A small enterprise would normally have a staff strength of ten to forty-nine, and many of the enterprises globally will fall under this category (OECD, 2022). Medium enterprises are those enterprises whose staff strength is between fifty and two hundred and forty-nine (OECD, 2022). Many international enterprises that have global operations would normally fall under this category. Lastly, a large enterprise is any enterprise whose staff strength is over two hundred and fifty, but just a very small number of enterprises fall under this category (OECD, 2022). As a result, the various categories of an enterprise and the various criteria used to classify an enterprise are clear. Therefore, for this research, we will be classifying an enterprise by the size of its employees as seen in Table 2.1 below, since we are interested in the role of end-users and enterprise data security in the cloud.

*Table 2.1: Enterprise classification using the number of employees in the enterprise. By (Raczyńska, 2019); (OECD, 2022)*

<b>Microenterprise</b>	<b>1-9 Staff strength</b>
<b>Small enterprise</b>	<b>10 - 49 Staff strength</b>
<b>Medium enterprise</b>	<b>50 - 249 Staff strength</b>
<b>Large enterprise</b>	<b>250 and Above Staff strength</b>

Furthermore, looking at the classification of enterprises within the United Kingdom, although a lot similar to what is already discussed in the presiding paragraphs but there are some noteworthy classification that emerges when you look at how an enterprise is classified in the UK. Each enterprise type in the United Kingdom has its own legal ownership, organisational structure, and tax implications. As of March 2021, the primary categories of businesses are sole proprietorships, partnerships, limited liability partnerships, and corporations (Cowling et al., 2023). A *sole proprietorship* is the easiest business entity to register, as it is operated by a single individual and must be registered with HMRC (Moussetis and Cavenagh, 2021). They may retain all profits as income, but they must pay tax and national insurance.

*Partnerships* involve two or more individuals who agree to share in the profits or losses of the business (Moussetis and Cavenagh, 2021). They are personally responsible for the losses or debts and are also liable for other partners' negligence or misconduct. The profits or losses from a partnership will be shared between the partners, with each partner paying tax on their share of the profits. Subsequently, *limited liability companies* are privately held, shareholder-managed businesses (Moussetis and Cavenagh, 2021). They are distinct legal entities from their proprietors and directors, allowing them to own assets, enter into contracts, and file lawsuits in their own names. In 2021, 74.3% of all British enterprises were limited liability companies (Shaw, 2021). However, there is also the *liability of limited liability partnerships* (LLP) which is limited to the quantity of capital invested in the business (Keatinge et al., 1995). Annually, they must register with Companies House and HMRC, prepare and submit annual accounts, and file a personal Self-Assessment Tax Return. Members must also pay income tax and National Insurance to HMRC on their share of the partnership's profits (Freedman, 2000). Other business types in the United Kingdom include the public limited company (PLC), the company limited by shares (LTD), the company limited by guarantee (CLG), the unlimited company (Unltd), the community interest company (CIC), the royal charter (RC), the multinational corporation, and the franchise (Aiken et al., 2006). Depending on the nature, scale, and objectives of the business, each type possesses unique perks and disadvantages.

The UK's classification of enterprises is based on factors such as the size of the enterprise, its industry, and its legal status (Kumar, 1985). The Office for National Statistics (ONS) categorizes businesses into three main types on the Inter-Departmental Business Register (IDBR): enterprises, local units, and enterprise groups (Shaw, 2021). The ONS publishes annual statistics on UK business activity, size, and location using the IDBR data. The main business sizes are small and medium-sized enterprises (SMEs), mid-sized enterprises, and large enterprises (Shaw, 2021). SMEs have less than 250 employees and a turnover of less than £25 million, mid-sized enterprises have between 50 and 249 employees and a turnover of between £10 million

and £50 million, and large enterprises have 250 or more employees and a turnover of more than £50 million (Shaw, 2021; Raczyńska, 2019; OECD, 2022). The ONS also categorizes enterprises by turnover size bands, ranging from less than £100,000 to more than £500 million (Chittenden et al., 2003). Turnover is the total value of sales made by an enterprise in a given period, excluding value added tax (VAT).

### **2.1.1. The Enterprise System**

The enterprise system is a commercial software application and IT infrastructure that is used by organisations to establish harmony in information flow between all their business processes. It can handle a large volume of data, which makes it possible for enterprises to coordinate and integrate all the different units within the organization (Kristiansen, 2013). Markus and Tanis, (2000) believed that an enterprise system is any software application that automates enterprise business processes by efficiently organising and analysing the enterprise data. Authors stated that an enterprise system is transaction-oriented data application software that could harmonise all business processes within the organization (Markus and Tanis, 2000). This definition shows a limit on how the enterprise system can harmonise the business process since the software is data-oriented and can only work with the set of inputted data to carry out its integration. It could be said that data integration or storage isn't the most important part of an enterprise system. Instead, the flow of information between the different parts of the organisation is the most important part.

An enterprise system is a large-scale software application designed to automate core business functions and processes within an organization (Da Xu, 2011). Key characteristics include integration, centralization of data, standardization, scalability, modules, security, reporting and analytics, and user access control (Zissis and Lekkas, 2012). These systems are used by large and complex organizations to manage operations efficiently and effectively (Da Xu, 2011). Examples of well-known enterprise systems include ERP systems like SAP, Oracle, and Microsoft Dynamics, and CRM systems like Salesforce (Lee et al., 2009). These systems are used across various industries to manage various business functions, such as finance, human

resources, procurement, inventory management, sales, and marketing. Implementing an enterprise system can result in increased efficiency, improved decision-making, and better overall management of an organization's resources and operations (Da Xu, 2011).

On the other hand, an Enterprise Information System (EIS) is a software platform that manages and disseminates information within an organization (Romero and Vernadat, 2016). It focuses on data management, document management, knowledge management, communication and collaboration, business intelligence and reporting, content management, security and access control, integration with other systems, workflow automation, and search and retrieval (Firestone, 2007; Romero and Vernadat, 2016). EIS centralizes and manages structured and unstructured data, provides tools for data storage, retrieval, and manipulation, and helps organizations capture, organize, and share knowledge among employees (Power, 2002). It facilitates communication and collaboration through features like email, instant messaging, video conferencing, and collaborative workspaces (Romero and Vernadat, 2016). EIS can also integrate with other systems for seamless data flow and information sharing (Balfour, 2014). Its search capabilities enable users to quickly find information within vast repositories of data and documents (Millet and Mawhinney, 1992).

Therefore, to establish the difference between an enterprise system and an enterprise information system, we note that Enterprise Systems (ES) and Enterprise Information Systems (EIS) are related concepts, but they have distinct differences. ES refers to integrated software applications that automate core functions and processes within an organization, such as ERP, CRM, and SCM systems (Da Xu, 2011). It includes functionalities beyond information management, such as finance, human resources, and manufacturing (Da Xu, 2011). EIS, on the other hand, focuses on managing and disseminating information within an organization, focusing on document management, knowledge sharing, communication, and data analytics (Romero and Vernadat, 2016). ES aims to streamline and automate business processes, improving operational efficiency, resource management, and customer relations (Shang and Seddon, 2002).



EIS focuses on information management and sharing within an organization, ensuring information is readily available, accessible, and effectively utilized by employees (Leidner and Elam, 1995). ES may include modules or applications addressing different business functions, while EIS typically includes components related to data and document management, knowledge sharing, communication, and analytics (Romero and Vernadat, 2016). The terminology and distinctions between ES and EIS can vary across different industries and organizations, with the specific functionalities and features of these systems often overlap (Arif et al., 2005). Summarily, an enterprise system, also known as an enterprise resource planning (ERP) system, is a cross-functional information system that coordinates and integrates key business processes, including finance, accounting, human resources, supply chain management, and customer relationship management. It typically includes modules for finance, accounting, human resources, and supply chain management (Da Xu, 2011). An enterprise information system (EIS) is an information system that improves the functions of enterprise business processes by integrating large volumes of data and supporting complex organizations (Romero and Vernadat, 2016). EIS is more informational and analytical, while an enterprise system is transactional and operational. It may be part of an EIS, but not vice versa. However, enterprise systems can eliminate the hardware component by using the new and emerging technology known as cloud computing. With cloud computing, the enterprise system does not need to have a physical server as this is provided by the cloud service providers. It's safe to say that both terms are used to refer to any systems that make it easier for an organisation to work more quickly (Shang and Seddon, 2002).

### **2.1.2. Stages of Development of Enterprise Information System in an Enterprise.**

According to Eya (2015), enterprise information system adoption has progressed through numerous stages since it began many years ago. The most up-to-date information systems include e-commerce applications, digital marketing, and the usage of communication protocols by various businesses. According to Eya (2015), many businesses in Nigeria may not have used a platform-independent programming

language, virtual enterprise, or supply chain management system that integrates not only internal departments but also external organisations in the supply chain. Using manufacturing enterprises as an example, the sequential evolution of enterprise information systems in manufacturing follows the trend from Material Resource Planning (MRP) systems to Shop Floor Data Collection (SFDC) systems to Design Management (DM) systems (Cecelja, 2002), demonstrating how information systems at various stages assist businesses in improving operations. However, businesses continue to use enterprise information systems that were implemented from the outset, which may be ascribed to their business environment and maturity model degree of capabilities (CMM) (Paulk et al., 1991; Gökalp and Martinez, 2021). These various information systems can assist an average business in optimising its operations: Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Material Resource Planning (MRP), Computer Integrated Manufacturing (CIM), Statistical Process Control (SPC), Computer-Aided Design (CAD), Shop Floor Data Collection (SFDC), and Date Management via Programmable Logic Controllers (PLC), to name a few (Jun et al., 2010). Shoniwa (2021) believes that in recent years, as IT gear has become more inexpensive and Personal Computers have become more user-pleasant, the rising interest of businesses in implementing corporate information systems has grown.

There are several ways to classify an enterprise information system, particularly in the contemporary company; it may be classified according to the impact that the enterprise information system's deployment will have on the enterprise's strategic and operational goals (Annamalai and Ramayah, 2012). According to Kearns and Sabherwal (2007), strategic enterprise information systems have a direct influence on an organization's strategic objectives, such as the goal of opening a new manufacturing line or increasing sales percentage. However, operational enterprise information systems will influence the company's day-to-day management and operational operations. The development of an Enterprise Information System (EIS) involves several stages, varying in complexity and duration depending on the enterprise's size and requirements (Zacharewicz et al., 2017). These stages include planning and analysis, system design, software development, database implementation, integration, testing, deployment,

monitoring and maintenance, optimization and improvement, scalability, documentation and knowledge transfer, compliance and governance, continuous evaluation, and adaptation and innovation (Niu et al., 2013).

The EIS development process within an enterprise begins with a needs assessment, feasibility study, requirements gathering, system design, software development, database implementation, integration, testing, and deployment (Peppers et al., 2007). Zacharewicz et al., (2017) recommended that regular updates and user support are provided to ensure the EIS remains up-to-date and meets the evolving needs of the enterprise. The EIS must also comply with relevant laws and regulations, establish governance policies, and continuously evaluate its performance and return on investment (ROI) (Wei, 2008). Embracing technological advancements and innovation is crucial for staying competitive and adapting to changing needs within enterprises (Eya, 2015).

The development process of EIS involves several stages, depending on the chosen software development methodology. The systems development life cycle (SDLC) is a common methodology, consisting of six phases: preliminary analysis, requirements analysis, design, implementation, testing, and change and maintenance (Ruparelia, 2010). Agile methodologies, such as Scrum, Kanban, Extreme Programming (XP), and Lean Software Development, involve frequent collaboration and feedback from stakeholders throughout the development process (Alqudah and Razali, 2016; Ciampa and Nagel, 2020). The evolution of information technology in a business enterprise is also a significant aspect of the development process.

## **2.2 Data**

Data is seen as a set of variables, either quantitative or qualitative, that can be processed into a piece of information in any given circumstance using various data processing techniques (Luna-Reyes and Andersen, 2003). Data can be generated from any source by anyone, mostly to analyse the data into useful information. The

enterprise generates a lot of data during the business processes, including sales data, revenue data, profit margin data, personal data, market research data (Berry and Linoff (2004). Enterprise data needs to be classified since it will enable the data to be easily retrievable and encourage prompt data security response depending on the class of data that has been breached (Ahmad et al., 2021). The process of determining what value a piece of data holds, how it can be accessed and by whom within the enterprise can be called enterprise data classification (Panetto, 2007). A piece of information can make the difference between the success or failure of an enterprise. It is worthy of note that in the cause of data protection within the enterprise, there are three key areas: *data confidentiality*, *data integrity*, and *data availability* (Boruch, 1971; Griesser, 1978; Denning and Denning, 1979; Kumar and Bhatia, 2020; Aldossary and Allen, 2016). Finally, any enterprise data that is of great value to the enterprise should be easily accessible to the authorised personnel, and data's confidentiality, integrity and availability is maintained. It should also remain confidential and not get into the wrong hands.

For many reasons, the average enterprise collects a lot of data during its operations. Data collected can be critical, sensitive, or personal information (Kambatla et al, 2014). When data is critical to an enterprise's survival, it is considered critical. For example, transaction data of a sales enterprise is considered so critical that the enterprise would be unable to carry out its operations without it. Sensitive data, as the name implies, is data whose confidentiality is of utmost importance because of the nature of the information it contains (Jansen and Grance, 2011). For instance, the yearly budget of an enterprise that contains major financial plans of the enterprise is sensitive data that if it gets into the wrong hands, the outcome may be harmful to the enterprise. Finally, the protected personal data includes information about the employee's situation, such as their health or financial situation, which could lead to discrimination or harm if it was leaked and fines in the EU and UK.

### **2.2.1. Data Security**

...

The concept of data security is everything about ensuring that digital data retains its

acceptable data confidentiality, data integrity, and data availability. Every activity carried out to ensure the security of data can be referred to as data security. Saigushev et al., (2018) stated that enterprise data security in any enterprise network is a big issue in modern-day information technology because of the threats posed by data theft and malware effects. According to the authors, the design of a protected corporate network, whose security will be ensured through the use of VLAN technology, an AAA server, and an access list, could provide a solution to enterprise data security. An AAA server is a server application that manages user requests for computer resource access and offers authentication, authorisation, and accounting (AAA) services for a business. Authentication is the process of determining the identity of a user, often using a username and password (Glass et al., 2000).

Wang, (2018) stated that among the many concerns enterprises may have about data security, these concerns are aggravated when enterprises upload or store their data on public cloud servers. However, the paper believed that a secured data sharing scheme to ensure the privacy of the data owner and the security of the outsourced cloud data could solve the data security challenges, especially for an enterprise in the health sector that holds mostly sensitive personal data. This paper proposed a data-sharing scheme that was developed using binary paring, which will increase the confidentiality of data and the anonymity of the data owner. In their paper, Iureva, Andreev et al., (2018) showed concerns about the integrity of information resulting from analytical platforms that are designed to collect, store, and process data; this, he argued, was largely because of data security concerns. The paper showed that smart factories have a general dependency on the Internet of Things (IoT) technologies and went on to highlight the data security challenges that IoT technologies will pose to a modern-day smart enterprise.

It is believed that information derived from data is the most valuable asset of a business in the 21st century (Stepanov et al., 2018). According to Freeman et al., (2017), human error is the leading cause of enterprise data loss. Despite this, Stepanov, Parinov, et al., (2018) emphasized the importance of data in a contemporary enterprise. It was unclear

what the role human factors would play in the data security of enterprises, especially considering that human carelessness, which is a component of human factors, was identified as a major cause of data loss within enterprises.

Many researchers believe that the enterprise has concerns about data security, but these concerns are even greater with the introduction of cloud computing. Although Saigushev et al., (2018); Wang, (2018); Iureva et al., (2018) all offered a data security model that could be deployed in the enterprise to achieve effective enterprise data security, none explained how the end-user is engaged within the enterprise to achieve maximum enterprise data security in the cloud. Despite this, Stepanov et al., (2018) emphasised the importance of data in a modern-day enterprise, but it was not clear what role end-users would play in the enterprise's data security, especially when human carelessness, which is an accepted human factor, was identified as a major source of data loss.

### **2.2.2. Types of Data in Cloud Computing and Various Types of Actions Performed on Data in Cloud Computing.**

Three main types of data have been identified in cloud computing. It is normally described based on the current action happening with the data. Therefore, we have *transmission data*, *processing data*, and *storage data* (Sen, 2013). The transmission data is a set of cloud data that is in transit between the cloud service provider and the service users. The processing data is a set of data that is currently being processed to execute a request command that is received from the service users. An example of processing data is the data that is processed to answer a query in the database of an enterprise. The last type of cloud data, stored data, is the set of data at rest (Sen, 2013). It is important to note that the majority of the cloud service providers do carry out some level of data encryption for the transmission of data and processing of data. But many of the encryption methods do not extend to storage data (Vouk, 2008). This leaves a security gap and explains the concerns service users may have about their data security (Vouk, 2008). Data security in the cloud is a major concern and, as such, it was important to clarify the type of data category in cloud computing that has the least

protective features using the current security models. It has been suggested by some data management security models for cloud computing to use things like strong authentication or encryption to keep your data safe (Kaur and Sharma, 2014).

Cloud computing is a system that processes, stores, and manages various types of data, including structured, unstructured, semi-structured, log files, time-series, geospatial, metadata, big data, and user-generated content (Grover and Kar, 2017). Cloud computing platforms offer services and tools to handle these data types efficiently, such as storage solutions, databases, data analytics, and machine learning services (Rao et al., 2019). Cloud computing offers various actions on data, depending on the cloud service model used (Birk and Wegener, 2011). Infrastructure as a service (IaaS) provides basic computing resources, allowing users to create, delete, modify, and access data (Moreno-Vozmediano et al., 2012). Platform as a service (PaaS) provides the development and deployment environment for cloud-based applications, allowing users to create, test, deploy, manage, and update applications using data from various sources (Rani and Ranjan, 2014). Software as a service (SaaS) provides access to cloud-based applications hosted and managed by the service provider, allowing users to use, configure, and integrate applications with other services (Rani and Ranjan, 2014). Furthermore, serverless computing allows the execution of code without requiring the user to manage underlying infrastructure or servers, allowing users to write, deploy, and invoke functions triggered by events or requests (Baldini et al., 2017).

Cloud computing allows organizations to store, process, and secure data in a scalable and cost-effective manner (Birk and Wegener, 2011). Common actions include data ingestion, data archive, backup and recovery, and replication. Data transformation is performed using services like AWS Glue, Azure Data Factory, and Google Dataflow (Sreemathy et al., 2021). Data analytics is provided by platforms like AWS Redshift, Azure Synapse Analytics, and Google Big-Query (Orešćanin and Hlupić, 2021). Janiesch et al., 2021 noted that machine learning services are available for training models and predictions in cloud computing. Real-time processing is enabled by stream

processing frameworks like Apache Kafka and cloud-native services like AWS Kinesis and Azure Stream Analytics (Shahraki et al., 2022). Security measures in cloud computing data include data encryption, access control, data masking and redaction, and auditing and logging (Mather et al., 2009).

## **2.3 The Fundamentals of Information Security**

Information security is the prevention of unauthorised access, modification, destruction, or use of information. There are basic properties of a piece of information that could be used to measure when that information has been fully secured; this brings us to the discussion of attributes of information security. The attributes of information security are similar to the same attributes mentioned earlier for data security; they are information confidentiality, information integrity, information availability (CIA) and a further two new attributes by Mortazavi-Alavi 2016, information auditability, and information accountabilities (Mortazavi-Alavi 2016).

### **2.3.1. Information Confidentiality**

Informational confidentiality is simply making sure that information is viewed by only the authorised people with the right system permission. Information confidentiality has become a major concern in many organisations over the last decade as a result of major breaches and the General Data Protection Regulation (GDPR) (Vorakulpipat et al., 2017). For example, in 2005, LinkedIn experienced a cyber-attack in which its database containing 6.5 million usernames and passwords was published on public sites. Sony experienced a similar cyber-attack which, where its movie projects, financial data, and personal data were published publicly by hackers (Abi, 2022). iCloud, which is an add-on service from Apple, also experienced a cyber-attack where images from their database were made public (Abi 2022). Enterprises are concerned with keeping their data and information confidential.

The ethical responsibility of confidentiality refers to an individual's or enterprise's commitment to protect confided information. The ethical imperative of confidentiality



entails safeguarding information from unauthorized access, use, disclosure, alteration, loss, or theft (Fisher, 2008). Confidentiality is about privacy and honouring another person's preferences. It indicates that employees of an enterprise should not reveal a person's personal information with others unless the individual has given permission, or it is essential, for example: when it is required by the law. A breach of confidentiality happens when sensitive information is released to a third party without permission. Most breaches of confidentiality occur unintentionally. Regardless, individuals impacted may still incur monetary losses and reputational harm.

Kong and Zhanchuan, (2022) is of the opinion that a new embedding technique can improve data confidentiality during transmission, addressing several security issues on the Internet of Things. The results of their experiments demonstrate that the suggested method performs better than several multi-pass embedding methods. Their research focused on data confidentiality during transmission which the authors believed is the time when confidentiality of information is easily compromised. The most common breaches of confidentiality mostly happen in public places when enterprise employees use their own devices to access sensitive information about the enterprise and this information is viewed by shoulder surfing by unauthorised people. Encryption and secure system finite automata were identified by Xiaochao et al., (2006) as techniques that can be used to tackle the information confidentiality challenges within enterprises. These attacks can put the confidentiality of information at risk, including catching network traffic, port scanning and listening in on eavesdropping. Hackers can also steal password files by sniffing and listening in on conversations (Ahmed, Munir, et al., 2012). Multi-authentication methods, for example, can be used by businesses to make sure that only people who are supposed to have access to the data do (Ahmed, Munir, et al., 2012).

### **2.3.2. Information Integrity**

Information Integrity is assured when an information system preserves the authenticity of the information in its database and only authorised modifications of the information are made by the authorised users (Flowerday and Von Solms, 2007). This is to say that

all the information that is going back and forward through the system cannot be modified without detection. Information security, when fully achieved, gives confidence to the system because an enterprise can trust the stored information to inform major business decisions without fearing that the information may have been modified. Sokol and Hogan, (2013) argued information integrity may not be as obvious as information availability. To ensure good information integrity, some techniques can be used, for example: data access control, intrusion detection, and encrypting the information on both ends. Encryption and hashes play a role in information security systems where they are used to ensure that transmitted information has not been modified. The sender generates a hash of the information to be sent, encrypts it, and sends it along with the information itself. The recipient then decrypts both the information and the hash, produces another hash from the received information, and compares the two hashes. If they are the same, there is a very high probability that the message was transmitted intact (Aggarwal and Kumar, 2021).

There may also be problems with the user that impact the integrity of the system's information. For example, a user may modify a file, or there may be an input error in which incorrect data is entered into the system. These human errors can occur very often because of oversight, incompetence, fatigue, stress, lack of communication, inadequate training, etc. and can have a major impact on the information integrity of the system (Metalidou et al., 2014). Therefore, it is important for enterprises to implement the least privileges principle on their systems, ensuring that users do not have more access than they should so that if they make a mistake, it will have very little effect on the entire system. It is also recommended that enterprises have application data input checks, which could be manual or automated, to ensure that input data is complete, accurate, and valid. Another technique that enterprises can use is security event logging and monitoring. Security event logging and monitoring is a process that organizations perform by examining electronic audit logs for indications that unauthorized security-related activities have been attempted or performed on a system or application that processes, transmits or stores confidential information. Logging and monitoring will help to identify patterns of activity on enterprise networks, which in turn provide indicators of compromise. In the event of incidents,

logging data can help to identify the source and the extent of compromise more effectively. Failure to sufficiently log, monitor, or report security events, such as login attempts, makes suspicious behaviour difficult to detect and significantly raises the likelihood that an attacker can successfully exploit your application (Posthumus, 2007; Chung and Hung, 2020).

### **2.3.3. Information Availability**

This is simply defined as when an information system is up and running and when the information is available to the authorised person at the time of need. It simply means systems, networks, and people will be up and running to ensure the right information is available to the right people at the right time. This is a major objective of information security. It is one of the information security attributes that form part of the information security triangle. It is not possible to say that we have a fully secured information system within an organisation where information is not available to the right people when needed. Information availability affirms the continuous access to required information even in the face of attacks like DoS (Denial of Service). It's important to note that having good control over who has access to information and making sure they follow all the security rules or policies, will make the enterprise better able to deal with things like information interruption, information redundancy, information destruction, and information loss (Qadir and Quadri, 2016). McLeod and Dolezel (2022) mentioned that End user compliance is necessary for information security rules to secure computer resources. End-users may be giving up on security compliance because they think breaches are unavoidable especially when information availability is delayed due to information security protocols, according to their theory. The capitulation theory looks at self-efficacy, vulnerability, dangers, loss of privacy, and scepticism of information security.

According to Qadir et al., (2016) one of the crucial pillars of information security is information availability, presented in this paper. It gives the current CIA triad security model a good review and the report also classifies the different kinds of availability

that a system may have. Ometov et al., (2022) implied that research interest is currently high around information privacy and information availability. The paper believed a distinctive ecosystem is already being formed by various computer paradigms, from cloud to edge computing. Our examination of the literature seeks to pinpoint commonalities, discrepancies, primary assaults, and defenses in the various paradigms described and how information security is shaping the dynamics. Backups are also a huge part of the information available within an enterprise. For instance, if someone deleted information in error, we must be sure we can retrieve the current information from the backup, thus maintaining availability. When looking at the information available from the point of view of capacity and performance of the systems and networks, we must consider the ability to detect any threats to the system in time and manage them in time to avoid interruptions to information availability. This is achieved by ensuring an adequate access control mechanism is in place (Rai et al., 2013). Information availability can also be affected by hardware and software failures. When there is an error with the backup systems, information will not be readily available. In ensuring information availability, we need to ensure that the enterprise has trained technicians who can take care of any system security.

We also must consider the environment of the data centre when considering information availability; we want to ensure that the data centre has the right temperature and humidity to keep the systems up and running. According to Saritha et al., (2020), both enterprises and individual end-users can now organize their data more easily thanks to cloud storage and backups. Old file systems with extensive native disk-based storage backend optimizations are unable to fully take advantage of the cloud's affordability. The study offers a survey of various cloud-backups and their cost-effective file systems.

Furthermore, among the many threats faced by the enterprise information system within an organization, some of the threats are directed at disrupting information availability (Bisong et al., 2011). For instance, denial of service (DoS) attacks, information deletion, data disruption, and communication interruption attacks are

common (Bisong et al., 2011). Since these systems are mainly used by humans, it will not be out of place to say that some of the attributes of humans also have an impact on the availability of information. For example, the alteration of a very important piece of information due to human error, oversight, incompetency, tiredness, etc. may result in the information not being accessible when needed (Mortazavi-Alavi, 2016). Information availability issues can happen because of the actions of employees, a mistake in the security strategy, or the wrong configuration of security controls (Bisong et al., 2011).

### **2.3.4 Information Accountability**

Information accountability as a fundamental of information security is the process of accounting for events and actions of end-users using a dataset in a system, which means the usage of information is transparent and actions or omissions can be traced back to the individual or events (Weitzner et al., 2008). Information accountability holds end-users responsible for actions or inactions that lead to data loss within an enterprise. This is because every action in an accountable system can be traced back to the individual using various system auditing techniques. According to Williams, (2007), information accountability challenges can be managed within the organisation by using organisational information governance. She proposed a tactical approach model aimed at addressing information accountability challenges. Olt, (2022) states the digital world presents both end-users and enterprises with a variety of information security and privacy-related concerns. The upkeep of information security is a constant struggle for end-users, enterprises, and IT specialists. The author identifies the various difficulties that end-users encounter when carrying out the actions required to keep this enterprise information safe.

When using ERP software or an online service, enterprise end-users should think about how their actions will affect their personal goals of maintaining information security. Therefore, encouraging end-users to take more care of the enterprise information. The author went further to explain end users' security fatigue and creates a mechanism for empirically examining people's capacity for cognitive explanation of security

suggestions and policies. Gajanayake et al., (2011) in their paper titled “sharing with care” stated that E-health technologies, a type of an ERP software offers quick and easy ways to exchange medical data. However, they also bring up difficulties related to patients and healthcare providers having no control. The sharing of sensitive data like health information is hampered by concerns about information security and patient privacy. The authors provide a method for information accountability that combines social networks and the interoperability standard to encourage more information accountability by end-users of these system. The authors said that giving patients control over their information could be very helpful for future health care needs. Sharing health information through social networks can help both patients and doctors get better care. Because of the Internet and the fact that people want to be more involved in their own care, the word "patient" is being replaced with "consumer." The author thought that putting his proposed “HL 7” framework into the structure of a social network would make it easier for patients to share health information (Gajanayake et al., 2011).

### **2.3.5 Information Auditability**

Information auditability is a crucial aspect of cloud computing security, enabling tracking, monitoring, and auditing of all data and information activities within a cloud environment where both cloud service providers (CSPs) and adopting enterprise end-users can verify and account for their actions and data in the cloud environment (Ko et al., 2011). It helps in compliance requirements, maintaining data accountability, tracing security incidents, ensuring access control and authorization, monitoring anomalies, forensic analysis, change management, data integrity, continuous improvement, and third-party assessment (Gul et al., 2011).

Information auditability provides a trail of data access and changes, allowing auditors to present evidence of compliance (Pasquier et al., 2018). It also helps in identifying security weaknesses, patterns of misuse, and areas for improvement, enabling policy changes and better security strategies (Wang et al., 2010). It also enables third-party assessments of cloud providers’ security practices. To achieve information

auditability, CSPs and cloud customers need to implement appropriate controls and mechanisms, such as logging and auditing, transparency and accountability, certification and attestation, and auditability by design. Implementing information auditability through logging and monitoring systems, access control policies, and security information and event management (SIEM) tools is essential for ensuring transparency, accountability, and compliance in a complex and dynamic computing environment (Jaatun et al., 2020).

CSPs should maintain comprehensive and accurate logs of all cloud activities and transactions, securely stored and protected from tampering (Gul et al., 2011). They should also disclose policies, procedures, standards, and practices governing cloud services, provide clear communication, and be accountable for any breaches or failures (Gul et al., 2011). CSPs should obtain independent certification or attestation from a reputable third-party auditor, based on widely accepted standards or frameworks (Ismail and Islam, 2020). We believe that CSP should provide the adopting enterprise end-users with evidence of their certification or attestation and allow them to review it. Auditability by design means that cloud services should have built-in features and functions for logging, auditing, transparency, accountability, certification, and attestation (Jin et al., 2018). It is okay for the SLA between the CSP and adopting enterprise end-users to specify the scope, frequency, methods, standards, and outcomes of information audits in the cloud.

## **2.4 Cloud Computing**

Cloud Computing is an emerging IT technology that provides on-demand services to end-user with high scalability in an efficient way over the internet ((Bhardwaj, Jain et al., 2010). Kumari and Nath, (2018) defined cloud computing as mainly outsourcing of computing resources over the internet. Computing resources here can mean any feature of traditional computing like servers, networks, data etc. Janulevičius, Marozas et al., (2017) stated that computing cost is greatly reduced by enterprises who adopt cloud computing, while noting that data security is a major concern. According to Mell and Grance, (2011) cloud computing is a model for empowering pervasive,

advantageous, on-demand network access to a common pool of configurable computing assets (e.g., systems, servers, storage, applications, and services) that can be quickly provisioned and discharged with insignificant administrative exertion or specialist service provider interaction. In a nutshell, cloud computing is the provision of computer services—such as networking, servers, storage, databases, software, analytics, and intelligence—through the internet, or "the cloud," in order to provide economies of scale, flexible resource allocation, and quicker innovation.

#### **2.4.1 The Adoption of Cloud Computing Technology in the Modern-Day Enterprise.**

In its development since the mid-1970s, computing has gone through a few phases, from centralised server personal computers (PCs) to minicomputers to PCs to network computing, client-server computing, and distributed computing. Presently, computing is moving outward to the clouds, to distant computing assets enabled through the Internet. Various scholars and organisations have attempted to define cloud computing depending on how they view it. Saa, et al., (2017) describe cloud computing as a method of computing where adaptable and elastic IT-enabled capacities are provided as a service to various clients using internet technologies. Rowsell-Jones and Gomolski, (2011) predict that 80% of Fortune 1000 enterprises will be using some level of cloud-computing services by 2012. Cloud computing is a new IT technology that involves the use of internet resources to carry out activities at a personal or enterprise level. These activities include software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), and anything as a service (AaaS), which represent the various service deployment models of cloud service providers. SMEs have become the main adopters of cloud computing because cloud computing is the most cost-effective when compared to traditional computing. (Johansson, et al., 2014).

#### **2.4.2 Attributes of Cloud Computing**

It is believed that there are characteristics of cloud computing that make it distinct from traditional computing; these features are what is referred to as the attributes of



cloud computing. Scholars have identified five attributes of cloud computing as follows: on-demand self-service, measured service, resource pooling, broadband network access, and rapid elasticity (Furht, 2010; Gong, Liu et al., 2010; Mell and Grance 2011; Zissis and Lekkias, 2012). Although their names suggest a meaning to what each attribute could stand for, we go further to explain each of the attributes in the following paragraphs.

#### **2.4.2.1 On-demand Self-service**

On-demand self-service simply means that end users of cloud services should be able to create a service whenever they want. End-users can select the resource they want and can access the resource at any time and from anywhere they want (Surbiryala and Rong, 2019). More importantly, end-users can upgrade and downgrade service any time they want.

#### **2.4.2.2 Rapid Elasticity**

Rapid elasticity is considered the most attractive feature of cloud computing for enterprises (Mell and Grance, 2011). As the name itself suggest, cloud computing is elastic. That means when there is a certain load on the server and it exceeds its threshold, it can increase its capacity automatically. For example, let's say that the infrastructure they have is something that looks like the image below in Figure 2.2. The white coloured box is the *load balancer* and the *VMs* are the web servers. So, when the traffic hits the web servers, it will hit through the load balancer. For enterprises, rapid elasticity is highly attractive because it offers unparalleled flexibility and agility in managing their IT infrastructure. It enables organizations to efficiently handle sudden spikes in demand, such as during peak periods or unexpected surges in user activity, without experiencing performance degradation or downtime. This ability to seamlessly scale resources up or down in real-time aligns well with the dynamic nature of modern business operations, allowing enterprises to optimize resource utilization and cost-effectively meet their evolving needs. Furthermore, rapid elasticity empowers enterprises to innovate and experiment more freely, as they can quickly provision and de-provision resources as needed without being constrained by traditional

infrastructure limitations. This agility fosters a culture of experimentation and enables organizations to rapidly deploy and iterate on new services and applications, accelerating time-to-market and gaining a competitive edge in today's fast-paced digital landscape. Overall, rapid elasticity stands out as a key enabler of agility, efficiency, and innovation for enterprises adopting cloud computing, offering unparalleled scalability and responsiveness to changing business requirements.

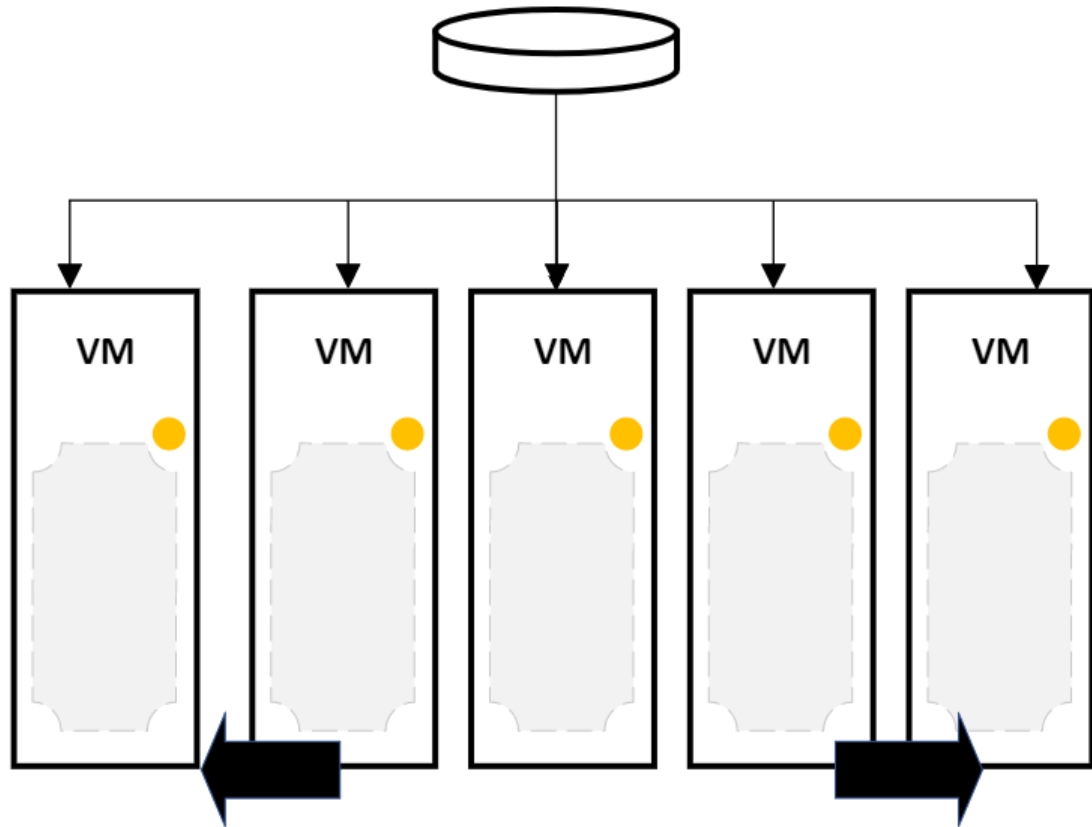


Figure 2.2: Infrastructure of an e-commerce website (Nednur, 2018 ;Eya, 2023).

During regular times, when there is no sales period, the traffic will be regular, which means the CPU utilisation on these servers will be normal, the network utilisation on these servers will also be normal, and even the disc utilisation will also be normal, and this is in a fair situation. If Amazon.com announces that there will be sales from 7 a.m. to 12 p.m., there is a high possibility that people like you and me who want to cut costs while shopping will be doing our shopping at the sales time. This means that thousands of people will be connected to Amazon.com sales right around that sales time. What will happen to the servers is that the CPU utilisation goes up above a certain threshold, the network utilisation also goes up, and the disc utilisation increases beyond its

capacity. It will mean that these servers that were running at 30% to 33% utilisation before are now close to 80% utilization. When that happens, the website's services will be denied to users. Users will notice delays in website access. This is due to the server's inability to handle the millions of loads that have been thrown at them. (Marston, Li et al., 2011).

With cloud computing's rapid elasticity attribute, the whole set-up of servers can detect a threshold that when the CPU goes above a certain load and new servers can automatically be deployed. For instance, if the CPU goes above 80%, developers can write code instructing that when that happens, it should create a new server. So, instead of the five servers we have in the image above in Figure 2.2, we will now have six servers behind the load balancer and the load will be distributed among six servers instead of between five servers. It is also possible to have a step scaling code written so that if the CPU usage goes above 90%, it creates two servers, or if the CPU goes above 95%, it creates three servers. This is called scaling-out. Which simply means creating new servers based on demand (*Nednur, 2018*).

However, when the sales are over, it is necessary to scale down. All the servers that were created to handle heavy traffic will be decommissioned to save costs. The process of terminating servers not needed anymore is referred to as "scaling-in," while "scaling-out" is the process of creating servers based on demand. The process of scaling in and scaling-out servers based on demand is what is called "horizontal scaling." There is also something called vertical scaling, which is the process of shutting down the servers, then increasing the memory size, say from 4GB to 8GB or 10GB, increasing the number of CPUs from 4CPUs to 6CPUs, and then powering on the machine. Therefore, vertical scaling can be defined as the process of increasing the computing power of the machine, whereas providing new servers in that load set is referred to as horizontal scaling. This contributes towards "elasticity." (*Nednur 2018*).

#### **2.4.2.3 Measure Service**

.....

Measure service as the name implies, is an attribute of cloud computing that suggests

that the services the cloud service users use during a period can be measured and billed accordingly. This could mean that, as a cloud service user, you will receive a bill or invoice with a description of all the items used. For instance: how many servers used or how much storage space. This means that enterprises are only billed for what they use, and they can see what they are paying for. In some cases, even the geographical location of the servers can be included in the invoice (Nednur 2018).

#### **2.4.2.4 Resource Pooling**

Resource pooling is an attribute of cloud computing that encourages the sharing of cloud resources by different entities (Grobauer, et al., 2011). For example, if someone needs to take transport to the airport, they can decide to board a cab that is shared with other travellers going to the airport, or they may decide to take a cab alone. Sharing the cab with other travellers, reduces the cost, but boarding the cab alone, creates more privacy. This is the same in cloud computing. When an enterprise decides to use the public cloud, they get to share all the cloud resources with other enterprises by creating virtual machines that give the users CPUs and memories. This will be more affordable but may expose the enterprise to a greater security risk as there will be other virtual machines on the same server that are owned by other enterprises, as compared to when the same enterprise decides to use a private cloud.

It is important to note that although these virtual machines are on the same server, they are completely distinctive. That means it is not possible to switch from one virtual machine to the other, but this still does not guarantee total data security, especially when human factors like error, low skills, etc., could have an impact. For instance, remember that one of the main goals and benefits of virtualization is making the best use of resources. Richings, (2022) says that server sprawl is one of the side effects of virtualization that was not expected. "Once administrators learn how easy it is to set up new servers, they start making them for everything. Soon, you find that you are in charge of 11 to 25 servers instead of just 5 to 10. The private cloud will, of course, be more expensive, but will provide a more secure option for the enterprise. Resource pooling is also described as multi-tenancy (Dillon, Wu et al., 2010).

#### **2.4.2.5 Broad Network Access**

Broad Network Access is an attribute of cloud computing that enables the cloud service user to have access to the cloud resources using the internet from any location and at any time. This simply means that the cloud services should be available twenty-four hours a day, all year round (Spring, 2011; Zissis and Lekkas, 2012). Although this is the ideal situation, it has been reported by some scholars that inevitable downtime is experienced by cloud service users. (Undheim, et al., 2011 ; Cérin, et al., 2013; Marinos and Briscoe, 2009). The adopting enterprise end-user must have two things to access cloud computing resources: an internet connection and a device with a compatible browser.

#### **2.4.3. Cloud Computing Service Models and their Security Challenges**

According to Jangjou and Mohammad (2022), the advent of cloud computing has caused cloud computing services to become more and more popular. Numerous security issues are brought on by data transfer and apps outside of end-users' control. The security issues, threats, and weaknesses in various network layers are examined by Jangjou and Mohammad (2022) in their paper and they also offered a cutting-edge remedies and preventive measures that can lessen vulnerabilities across most of the cloud delivery model. Also, Harfoushi, et al., (2014) stated that a collection of IT services known as "cloud computing" are made available to consumers via the internet on a subscription basis. The authors believe that cloud computing allows enterprises to scale up or down their internal foundations. It gives enterprises a cutting-edge virtual environment in which to deploy their apps or do business.

Despite the potential advantages, enterprises are hesitant to use them mostly because of security concerns. It is expected that data security is the main security concern of a cloud computing service, but it can be argued that the different service deployments of cloud computing have unique security challenges since some of the deployment models give a level of privilege to the service user to manage their own security

(Harfoushi, et al., (2014). This section classifies the various security challenges of cloud computing concerning the service deployment model they largely affect. There are three major service deployment models in cloud computing: Software as a Service (SaaS) Model, Infrastructure as a Service (IaaS) Model, and Platform as a Service (PaaS) Model.

#### **2.4.3.1 Software as a Service (SaaS) Model**

In the SaaS model of deployment, the service user makes use of the software application that he/she accesses via the internet to carry out business activities. In this model, the service user only has access via the user interface that is provided by the cloud service providers. The service user is not responsible for data security because all security responsibilities are borne by the cloud service providers. As stated in the earlier sections, data security within an enterprise context is looked at on three levels, which are data integrity, data confidentiality, and data availability. Therefore, the data security of the software as a service model is the sole responsibility of the cloud service providers, which means the service user loses control over their data (Di Costanzo, et al., 2009). The main security problem with a SaaS model is that the service provider is in charge of making sure data is confidential, available, and that it is safe. The enterprise must trust them to do this.

#### **2.4.3.2 Platform as a Service (PaaS) Model.**

A Platform as a Service (PaaS) model allows a service user to develop their application on the platform provided by the cloud service provider. This deployment model is mainly used by developers to build their applications completely on the internet using the resources and the different programming languages that are made available on the PaaS. The PaaS model is considered a very convenient way for developers to build their apps without worrying about the cost of the underlying infrastructure or even the cost of maintenance of such infrastructure (Hoffa, et al., 2008). However, in this deployment model, the data security responsibility is shared between the service users and the cloud service providers, where the service user has the responsibility of ensuring the data confidentiality of the application with the required data

authentication, encryption, etc. On the other hand, the cloud service providers are responsible for the data availability and data integrity (Ajoudanian and Ahmadi, 2012). It is important to note that due to business models, applications developed on a specific cloud service provider's platform cannot easily be moved to another cloud service provider. Where this is possible, it usually comes at a premium cost.

#### **2.4.3.3 Infrastructure as a Service (IaaS) Model**

IaaS is a type of cloud service delivery model that allows the cloud service users the privilege to run and deploy programmes, these can be software applications using the cloud service provider's computing hardware, processors, virtual servers, network storage, memory, and data centres. (Modi, et al., 2013). The IaaS model allows the service users to pay on a per-user basis, one of the greatest advantages a cloud-based ERP system has over a traditional ERP system. According to Bhardwaj et al., (2010), an increasingly common paradigm for gaining access to computational resources is cloud computing. In reality, cloud service providers often offer three types of services: infrastructure as a service, platform as a service, and software as a service. The paper suggested that because the infrastructure needed to supply compute power, storage, and networking is not required to be purchased or maintained by the end-user, an IaaS offers significant cost advantages. Enterprises are charged for only what is used. IaaS is a flexible service that frequently appeals to infrastructure builders because it offers a method for offloading workloads to the cloud that is based on architecture.

#### **2.4.4 Challenges of Cloud Computing Adoption in an Enterprise**

Beliefs about cloud computing can be positive. The opinion has been that the benefits of cloud computing adoption within an enterprise outweigh its challenges, especially implementation challenges. Pekane and Tanner, (2017) believe that cloud computing technology is the solution to the challenges faced by small and medium enterprises (SMEs) in Africa who normally shy away from traditional ERP (enterprise resource planning) software applications because of the associated cost of implementation. A critical review was conducted in his paper on why SMEs in developing countries should embrace cloud computing technologies, but it was not clear what the readiness

analysis of the SMEs would suggest. He suggested future research to determine if the SMEs and the employees would be able to handle such a transition giving their IT skills and resources. Subsequently, it could be argued that SMEs in Africa, although financially and technologically ready for cloud computing technology adoption, may not pass the readiness analysis if the employees lack the required IT knowledge and have a negative attitude towards data protection and security in the cloud. Cost-benefit analysis and risk analysis models could be used to figure out how far a SME can push their luck. Balachandran and Prasad, (2017) acknowledged that cloud computing is one of the most important emerging technologies in recent years. The authors think that cloud computing enhances the storage possibilities of an ERP software application, such as big data analytics. It offers the various benefits of cloud computing and big data analytics within an enterprise, where the greatest benefits are cost reduction and on-demand self-service.

Furthermore, the authors enumerated the challenges of cloud computing technologies in an enterprise as data quality, security and privacy, hacking and attacks, billing and service delivery, interoperability and portability business, reliability and availability, performance, and bandwidth cost. The authors suggested that enterprises would need to set up policies that are geared towards preserving data security while making use of trust relationships and promoting information sharing within the enterprise. An enterprise data security policy that took into consideration trust relationships could be considered to have understood the impact of their employees on their data security and to be able to establish who needs to be trusted and at what level of trust. Furthermore, according to Duncan et al., (2016), cloud security adoption is a difficult task. For it to be successful, strong cloud security measures must be agreed and implemented. The very nature of cloud computing can complicate security issues. The authors discuss why this is so and consider what desirable characteristics should be pursued, as well as a creative strategy for achieving these quickly and effectively. The authors proposed the use of systems based on the unikernel architecture which will enable an easy forensic trace in the cloud and enforcing good cloud security controls. The most intriguing feature of unikernels from a security standpoint is their ability to act as a minimum execution environment (Duncan et al., 2016).



According to Vasiljeva, et al., (2017), cloud computing, specifically backup and storage, web-based emails, and online office software, is widely used by SMEs in Latvia. The authors investigated how much employees of small businesses in Latvia know about cloud computing via a survey that had 86 businesses. Cloud computing is a term that most people in the business world know, but they don't know how it could affect their data or how their actions could affect the security of their data in the cloud, the study found. Finally, it can be keenly argued that although cloud computing technology offers benefits to an enterprise, it is not without its challenges.

Many of these challenges have been extensively reviewed by scholars, it suggests that providing adopting enterprise end-users more security responsibility and awareness could make the cloud safer for their business data (Ion, et al., 2011). It could be observed that the following: IT skills, IT knowledge, attitude to work, trusted or untrusted employee, little knowledge of cloud computing concepts, and lack of awareness of the impact of one's actions on the enterprise data security in the cloud, Error, Apathy, Negligence, Stress, Culture, Communication, etc., are all the cloud computing adoption challenges surrounding the employees of an enterprise (Cetindamar, et al., 2021; Pearson, 2013; Lansing and Sunyaev, 2016). A research activity to identify the extent to which these identified employee challenges would influence the adoption of cloud computing technology in an enterprise will be needed to add a novel insight to this field of knowledge.

## **2.5 Cloud Computing Security Models**

Cloud security is the use of the latest technology and security techniques to safeguard data, applications, and infrastructure associated with cloud computing. The set of policies, procedures, technologies, and controls that function jointly to safeguard cloud-based systems, infrastructures, and data is known as the Cloud Computing Security Model (CCSM). Examining the many cloud computing security models identified, with a focus on the model that handles the data security challenges of a cloud-based ERP system. It is observed that all CCSMs have a similar objective of

safeguarding the cloud system, but the Multi-Cloud Database Model (MCDM) is more focused on protecting data in the cloud. The MCDM was looked at to see if there was a way to make sure the adopting enterprise end-user experience is taken into account during the design and development stages.

### **2.5.1. Multiple Tenancy Model (MTM).**

As the name implies, a multiple tenancy model is a cloud feature that allows multiple customers to access the same application or cloud resources from the same physical server without compromising security and privacy (Tang et al., 2015). In a multiple-tenancy architecture, virtualization is used to differentiate and process each customer's demand; this is possible because virtualization can isolate and share the different computing resources such as processors and memory (Tsai et al., 2010), etc. Furthermore, the multiple tenancy model has some identified technological difficulties that place different demands on architectural design. For instance, the multiple tenancy model will require a cloud computing architecture that is highly scalable, flexible, and able to support different customers' demands without their data intertwining (Takabi et al., 2010). Multi-Tenancy security vulnerabilities are associated with integrity and confidentiality risks in cloud computing resource sharing. When several users share the same resources, a malicious user can gain access to all other users' resources by employing certain techniques (Shokrollahi, 2019). There are features that the multiple tenancy model has that enable it to withstand the presented technological difficulties. These features include its ability to prevent customer data interferences (data isolation), its ability to easily scale up or down as the customer requires (architecture extension), its ability to allow each customer to customise their system's service requirements (configuration self-definition), and finally, its ability to guarantee that each customer task will be attended to by customising performance using different workloads. (Zhang et al., 2010).

### **2.5.2. Cloud Risk Accumulation Model (CRAM)**

The Cloud Risk Accumulation Model (CSA) is a cloud security model that defines the boundaries of each service model and the relationships between them in terms of cloud

security (Che et al., 2011). IaaS is the fundamental service model from which all subsequent service models inherit their capabilities and security concerns. For example, if IaaS is the fundamental service model, the PaaS will inherit the IaaS's security capabilities and concerns while adding its own security capabilities and concerns. Additionally, the SaaS will incorporate the IaaS and PaaS's security capabilities into its own security capabilities and concerns. This risk accumulation model implies that it is critical to understand the layer dependency of various cloud service models to properly assess the security risks associated with cloud computing (Kaur and Sharma, 2014). It is critical to keep in mind that in a cloud risk accumulation model, the adopting enterprise end user's security responsibilities vary according to the service level. For example, at the IaaS level, the end-user is responsible for meeting the monitoring, compliance, and security requirements of the cloud system, whereas, at the SaaS level, the cloud service provider is responsible for monitoring and security of the cloud system (Che et al., 2011).

### **2.5.3. Jericho Forum's Cloud Cube Model (JCCM).**

As the name implies, Jericho Forum's cloud cube model is a cloud cube model that was created by Jericho Forum to categorise cloud networks based on four distinct characteristics: Internal/External, Proprietary/Open, De-perimeterized/Perimeterized, and Insourced/Outsourced (Chaturvedi and Zarger, 2015). The purpose of a cloud cube model is to facilitate the selection of cloud formations for secure collaboration. According to scholars (Chaturvedi and Zarger. 2015; Shahid and Sharif 2015), data classification is a critical step that any enterprise intending to move its data to the cloud should take. This is because data classification enables decision-makers to identify which data and processes to migrate to the cloud. The Jericho Forum's Cloud Cube Model offers a structured approach to understanding the different dimensions of cloud computing, encompassing concerns like trust, legal, and operational considerations. It provides a framework for organizations to evaluate and navigate the complexities of cloud adoption, ensuring security and compliance while maximizing benefits. Additionally, it determines which cloud formations meet their requirements. It assists in determining the cloud service level at which the end-user wishes to operate; this

could be IaaS, PaaS, or SaaS. The following four attributes are used to categorise cloud formation in the cloud cube model:

### **2.5.3.1 Internal/External**

This is a cloud cube model attribute that simply refers to the data's storage location. A set of data is considered "internal" if it resides within the data owner's data centre; for example, when data is stored in a private cloud, it is considered "internal." A set of data is considered "external" if it is stored in a data centre that is not within the data owner's boundaries, for example, any data stored in the public cloud (Shahid and Sharift, 2015).

### **2.5.3.2 Proprietary/Open**

This attribute of the cloud cube model describes the ownership structure of the cloud technology and its interfaces. When a cloud service provider owns the cloud technology infrastructure, this is referred to as the "proprietary dimension," which means they are responsible for safeguarding the data and cloud infrastructure they own and thus will be unable to allow end-users to easily migrate their applications to another cloud service provider (Shahid and Sharif, 2015). However, in an "open dimension," end users can transfer applications, share data, and collaborate with other cloud service providers through the use of open technology. This is possible in a public cloud with a large number of cloud service providers.

### **2.5.3.3 Perimeterized/De-perimeterized**

This is a simple cloud formation that indicates whether an end-user is operating within or outside of traditional IT security boundaries. Perimeterization refers to the fact that the end-user application is contained within the traditional IT security perimeter. The concept of "perimeterization" in the context of IT security refers to the traditional approach of securing networks by establishing a well-defined perimeter around an organization's internal network. In this model, security measures are primarily focused on protecting the boundary or perimeter of the network from external threats. This can

be accomplished using network firewalls. Additionally, de-perimeterization implies that end-user applications operate outside the confines of traditional IT security; this implies that end-user data is exposed. This data exposure is controlled through the use of metadata and the Jericho Forum's mechanism, which prohibits the unauthorised use of enterprise data (Chaturvedi and Zarger, 2015).

#### **2.5.3.4 Insourced and Outsourced**

This is a feature of the Jericho Forum's cloud cube model, which refers to the entity responsible for managing the cloud in an enterprise. Insourced cloud computing refers to cloud computing that is managed by an enterprise employee over whom the enterprise has control over his work activities, whereas outsourced cloud computing refers to cloud computing that is managed by a third party. This feature does not require technical or structural changes; rather, it is a business decision that will affect cloud data security (Che, Duan et al., 2011).

The Jericho Forum, an international organization focused on IT security and the challenges of de-perimeterization of networks and emerging technologies, officially disbanded in 2013. The forum made significant contributions to the field by promoting the concept of "de-perimeterization," which acknowledged the need for a more adaptive and risk-based approach to security in a world of mobile devices, cloud computing, and remote access. Despite its disbandment, its principles continue to influence modern IT security approaches, with ideas like zero trust architecture and data protection-focused security models becoming key concepts in the cybersecurity industry. The Jericho Forum's legacy continues to influence best practices and frameworks in the field.

#### **2.5.4 Default Gateway Platform Model (DGPM).**

The Default Gateway Platform is a cloud-based data centre security model. The model identified three types of data in the cloud system network: data transmission data, data storage data, and data processing data (Mohamed et al., 2013). As their names imply,

transmission data refers to data that is in transit, processing data to data that is being processed, and storage data to data that is at rest. Mohamed et al., (2012) believe that the majority of existing cloud computing data security models did not account for data at rest, creating a security gap that the Default Gateway Platform filled. The Default Gateway Platform employs a three-tiered defence system which is shown in Figure 2.3 below, with each defence level contributing its responsibilities to ensure the cloud system's data security. In the initial stage shown on Figure 2.3 below, at level 1, a One Time Password (OTP) is used to ensure a rigorous authentication process. The subsequent stage, level 2 employs a data encryption process to quickly and automatically encrypt data. End users can also encrypt their sensitive data manually using any of the modern encryption processes, such as Vera-Crypt software. Hashing is a cryptographic process that converts input data into a fixed-size string of characters, often representing a unique fingerprint of the original data. Additionally, the hashing process ensures the integrity of the encrypted data in transit. Hashing is a technique for ensuring data integrity and security, particularly for transmission data, because it ensures that the transmitted data is accessed only by the intended recipient. The data recovery phase is the final stage of the defence system structure; shown as level 3 in the Figure 2.3 below, this is the stage at which user data is quickly recovered on demand.

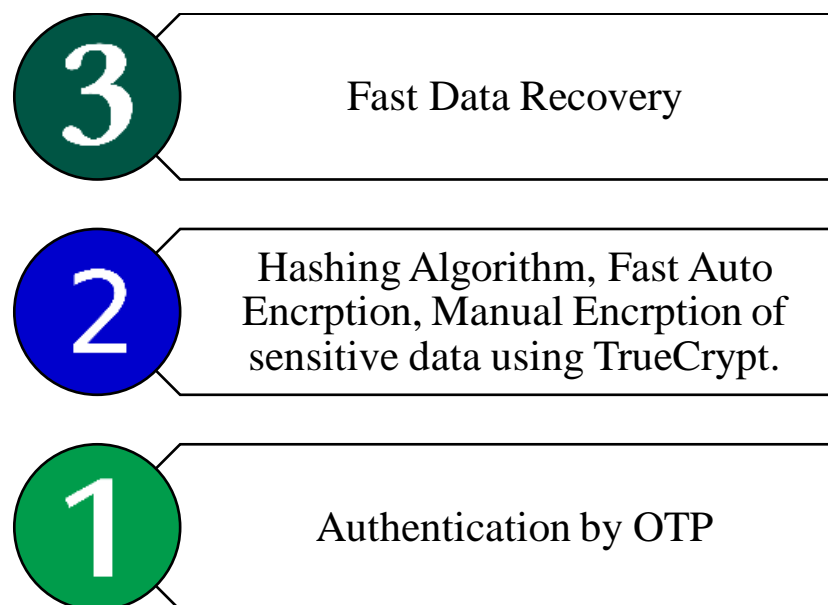


Figure 2.3: Three levels of the Default Gateway Platform (Eya, 2023).

### **2.5.5. Multi-Cloud Database Model (MCDM)**

Multi-Cloud Database Model is a type of cloud security model that applies to cloud systems whose databases are hosted by multiple Cloud Service Providers (CSPs) (Morozan, 2014); for example, when an enterprise subscribes to multiple CSPs' Database as a Service (DaaS). This is not the case with a typical scenario of a single cloud storage database managed by a single cloud service provider (CSP), such as the cloud services offered by Amazon. Because this model is concerned with multi-cloud databases, the security it provides is insufficient to cover single-cloud databases (AlZain et al., 2012). It does so by implementing "multi shares" across multiple cloud provider servers to ensure the cloud database's privacy and security. (AlZain et al., 2012) stated that the MCDM has numerous data security advantages over the single cloud, stating that the security risk posed by a malicious employee is greatly reduced in the MCDM. Although encryption is a secure process, it was believed to have some negative impact on the cloud network, which can be mitigated by using the MCDM.

The MCDM employs both data replication and multi-sharing techniques to ensure the privacy and security of the data in the various databases with the various CSPs. The data management system manages the communication between the cloud user and the CSP (DMS). The cloud network receives queries or entries to the server from the end-user; these are stored on the cloud server that is supposed to be a trusted cloud server; the issue arises when the cloud server is not sufficiently secured. Additionally, we propose that each CSP's database be further fragmented following data classification; this will increase the security of cloud data by ensuring that no single end-user has access to an enterprise's entire database at once.

### **2.6 Understanding the Concepts of Human Factors**

A human factor study, as defined by Trek et al., (2007), is the act of attempting to comprehend human behaviour or character, including their physical and cognitive characteristics, in a particular situation. Therefore, the role of human factors in cloud data security is simply studying how adopting enterprise employees will act concerning the cloud data security management process. Security technology

development has proven that it requires humans to operate it and still adhere to its principles to deliver the required security needs. Within an enterprise, the human factor becomes even more important because the security systems often have incidents triggered by either direct or indirect human factors.

The management of security incidents within the enterprise is not only looking at technical solutions but also human factors. When a security policy takes human factors into account, it has a high possibility of being accepted by an enterprise's personnel, hence enhancing the success rate of such a security strategy. This is also the case for security technical solutions. For example, security software that was developed taking usability into consideration will have a greater rate of success in helping employees to securing enterprise data. For this reason, it is important to understand human factors as they apply to the enterprise to be able to achieve an effective cloud data security management practice within the enterprise. Enterprise employees can be an asset as well as a threat when it has to do with cloud data security. Therefore, enterprises need to identify and address human elements when dealing with cloud data security incidents. Sarkar (2010) believes that the role of human factors in cloud data security has been underestimated and concluded by encouraging more research that will focus on how best to mitigate human factors to reduce their impact on data security systems.

Organizations frequently overlook the human factor, which is critical to security. There is a scarcity of research on human factors in cloud data security. (Luo et al., (2011). Regardless of design or implementation, a security system will have to rely on the human factor. According to Luo et a., (2011), the administration of information systems security effectively combines administrative and technological efforts. Information security may be threatened by social engineering, which is why it should be given the same importance as technological threats. Their article explores many social engineering attacks and the key human characteristics that contribute to them, as well as multiple strategies for defending against social engineering, including education, training, procedure, and legislation. Human error accounts for 65% of the economic loss in information security breaches, with malicious outsiders accounting



for only 3% (Carstens et al., 2004). People are, without a doubt, involved in technology, regardless of the partial automation that has been introduced. So, there is a chance that a person will make a mistake, which could leave the system vulnerable. When employees have more skills, there may be problems with security. This could happen if users need to use additional software or believe they have the knowledge to exploit any existing system vulnerabilities (Hadlington, 2021).

Data security in the cloud is characterised as an ongoing process that requires ongoing investment in both technology and user education. With the workstation identified as the weakest link in an ERP information technology system, an organisation can only succeed by integrating workstations and their users into the forefront of defence. (Gunasekaran et al., 2006). The security issue is essentially human-caused; the proposed remedies are primarily software-based, aiming to resolve a human-caused issue by altering the system's technology component. (Hughes-Lartey et al., 2021)

Even though there is a distinct likelihood of a security event owing to a lack of understanding of the human element, the probability of human factor intrusion is only defined as intentional human threats. The vast majority of defence mechanisms are implemented in software or hardware. The likelihood of a user's unintentional system exposure is not assessed. Coronado, (2012) recommends that clearly defined roles be followed and that users receive training in self-defence, accountability, and self-awareness. Vulnerability assessments are conducted solely based on previously discovered technical flaws. Unaddressed is a significant portion of the human factor, the non-technical unintentional vulnerabilities. A critical component of information security is the human being.

In a typical enterprise, the work performed by employees can be categorised in the following ways: teamwork, management work, customer-oriented work, and individual work (Guo et al., 2008). Furthermore, in an enterprise, because the employees are normally from various backgrounds of knowledge, their attitudes to cloud data security or their cloud data security culture are not always the same. Since

security in every sense is an individual habit that is normally formed over time, Individuals who have IT background knowledge may tend to be more data security conscious and aware when compared to their colleagues who are from other backgrounds. The employee of an enterprise are individually different, they would normally have their different personal values, skills, and behaviours that are peculiar to them alone. These characteristics of an individual employee are highly subjective and difficult to measure, especially their impact on cloud data security processes. But this is not to say that their impact is not felt because these characters will always interact with the technological components of data security. (Herzog, 2010).

Since individual interactions with computing devices at work are individually unique and the actions that they take concerning cloud data security are very dynamic and difficult to measure, this would mean that measuring human factors as they affect cloud data security is an issue of concern (Wu, 2011). This is a very subjective field of study, and it can be very hard to figure out how accurate it is because the study will be about humans and their cloud data security attitudes, and attitudes are challenging to measure.

Mortazavi-Alavi, (2016) believe that human factors can be divided into two groups using their degree of relation to the individual employee as a yardstick: direct human factors and indirect human factors. The direct human factors are those human factors that must do directly with the individual, for example, human error, skills, ignorance, stress, etc., which affect an individual employee's output with the organisation and, in turn, have an impact on the cloud data security process. On the other hand, the indirect human factors are more on the enterprise level but will have a degree of impact on the direct human factors. For example, factors like the enterprise budget for cloud data security, management support for cloud data security, and incentives for adhering to cloud data security policies will influence the way the individual employees of the enterprise adhere to cloud data security policies (Mortazavi-Alavi, 2016). The Figure 2.4 below shows the summary of the categories of human factors we discussed. These include the direct and the indirect human factors. Factors like IT skills, Human error,

Management support, Enterprise budget, Stress, Negligence, Data security awareness, Experience, Enterprise incentives, Security policy enforcement etc where all shown in the Figure 2.4 below.

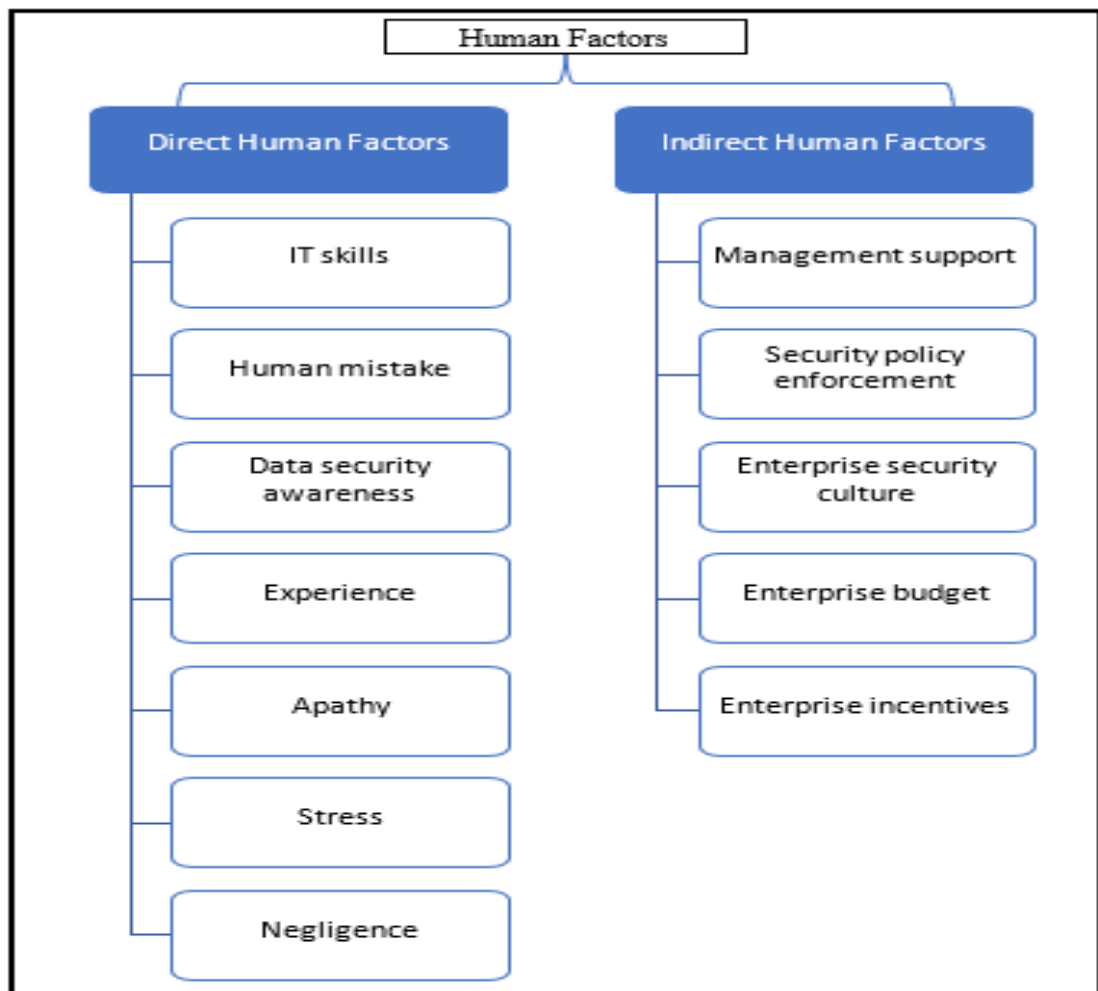


Figure 2.4: Summary of the categories of human factors (Mortazavi-Alavi, 2016) ;(Eya, 2023).

### 2.6.1. Direct Human Factors

As defined above, these are human factors that directly involve the individual employees of an enterprise. Pollini, et al., (2022) believed the typical approach to computer and information security (CIS) takes a technology-centric stance with little regard for the cognitive traits of the end users. To demonstrate how direct human vulnerabilities may affect cybersecurity risks, the authors take a direct human aspects approach, looking at adopting enterprise end-user, organizational, and technology factors in their research. Their findings demonstrate that increased rule compliance does not always follow from a stronger cyber-security culture and conflicts between

cybersecurity policies and practices may also lead to human vulnerabilities. The authors reaffirm the impact of direct human factors on any enterprise data security in cloud. Direct factors directly impact an organization's data security in the cloud, while indirect forces like security, policy enforcement, and management support have little bearing on the character or personality of individuals. Due to the subjective nature of these human factors, it will not be possible to identify all the direct human factors that affect an individual employee, but it is possible to focus on the critical direct human factors that have an impact on data security especially if they will have the same degree of impact in a cloud environment.

The following are the critical direct human factors as identified by Mortazavi-Alavi (2016): IT skills, experience, awareness, apathy, human mistakes, stress, negligence, or carelessness. Mortazavi-Alavi (2016). went on to identify these critical direct human factors as social elements that cannot be measured or controlled through technological means. It is proposed by Iivari and Hirschheim, (1996) that an approach that considers both social and technological factors will be the best when trying to define these elements of human factors in cloud data security. Each of the identified critical direct human factors below.

#### **2.6.1.1 IT Skills**

It is a known fact that a highly skilled employee will perform better compared to his colleagues who are under-skilled, irrespective of their profession (Driouchi et al., 2009). This is truer when you come to information technology professionals, who require extensive training and experience to have the necessary skills required to carry out the job. According to scholars, skills are one of the main strengths when handling data security incidents within an enterprise (Kraemer, 2006). This is because employees of the enterprise need to have the skills to be able to manage data security incidents whether they are in a cloud environment or not (Kraemer, 2006; Werlinger, et al., 2009; Kshetri, 2010). Another scholar believed that enterprises that have unskilled IT staff are more prone to data security incidents, especially in the cloud environment (Bushell, 2010). For example, when an employee lacks the required skills

to carry out the job, it brings about a lack of confidence in the systems and this also encourages unnecessary dependency on technology or other colleagues, thereby increasing the vulnerability of such an individual. Personnel vulnerability is an emotionally exposed state accompanied by a degree of uncertainty. It involves a person's readiness to bear the emotional risk inherent in being open to love and to be loved (Bagretsov, et al., 2017).

Colwill, (2009) explained that due to their lawful access to resources and information, organizational knowledge, and awareness of key locations for valuable assets, insiders pose security threats. However, it's possible that enterprises do not use efficient risk management procedures to deal with the speed and scope of change, such as the increase in outsourcing. Instead of responding to insider attacks after they happen, preventative steps must be taken. Therefore, it is important for an enterprise not to overrate or underrate an employee's skills, because an employee can be an asset as well as a treat (Driouchi, et al., 2009). As important as it is to identify and hire competent employees, it is also important that enterprises form a culture of training their employees with the minimum required skills to tackle any data security incident, especially in the cloud environment. It is important that this training has the support of the management team to encourage the employees to acquire these skills as new IT technology keeps changing with time (Brzycki and Dudt, 2005). This training, when conducted very well, will help enterprises be more prepared for any rapid changes in the computing or business environments (Bollinger and Smith, 2001).

Skills are one of the main forces in dealing with cloud data security issues such as incident response (Al-Darwish and Choe 2019). Cloud data security is crucial for incident response, and professionals need to possess key skills such as cloud security knowledge, forensics and investigation skills, threat intelligence analysis, security automation and orchestration, knowledge of cloud security tools, effective communication and collaboration, compliance and legal understanding, continuous learning, risk assessment and management, and soft skills. These skills help in identifying and addressing security risks, implementing risk mitigation strategies, and

ensuring compliance with data protection regulations. As cloud environments evolve, professionals must continuously update their skills and approaches to adapt to the changing threat landscape. The absence of adequate and appropriately skilled staff contributes to the weak performance of the cloud data security policy. (Hughes-Lartey, et al., (2021). People's skills should not be overestimated or underestimated. Organisations should not focus solely on people with complete technological competency but also ensure they train their employees to equip them with the required skills to handle cloud data security incidents.

### **2.6.1.2 Human Mistakes**

This refers to the actions of an enterprise employee that are inadequate or incorrect, thereby causing a divergence in a system that works perfectly (Kraemer, 2006). These actions are not deliberate but may be as a result of social engineering benefits. The impact of security incidents caused by human error on cloud data security, or any other security system is usually greater if those systems security are inadequate. (El-Bably and Amar Y (2021) When there is a security incident within an enterprise, it is difficult to measure and differentiate the different human factors that may have led to the incident because these factors are interdependent (Pearlin, et al., 1981). For example, a security incident caused by human error may occur because of poor communication among employees, stress, awareness, or even security culture. Thus, if an individual is highly stressed, it may make them prone to mistakes. (Pearlin, et al., 1981). However, it is encouraged that within an organization, security policies should be developed in a manner that manages behaviour to reduce mistakes. Wei and Blake (2010) said that human error is one of the many problems that cloud computing and service-oriented computing will have to deal with. This is because they are new technologies that are changing quickly and will need training before enterprise employees can use them correctly.

The term "error" refers to a divergence in the operation of a system that is otherwise accurate (Besnard and Arief 2004). Cloud data security incidents frequently occur when an adequate, but porous security measure is used. Consider the password as an

example. An end-user can be deceived to disclose the password or mistakenly write it down carelessly, allowing an unauthorised third party to gain access to enterprise systems using their password. The roles of individuals in cloud information security policies should be defined to make the auditability of errors possible. According to the findings of this investigation, indirect forces such as communication and human error can be traced back to security culture. El-Bably and Amar (2021) stated that by reducing the risk of a cyberattack, information security practices aim to safeguard data. Commonly, it involves preventing or lessening the likelihood of unwanted access, improper use, disclosure, and disturbance of data. The authors presented a set of useful guidelines like: "Keep your company's security policy up-to-date; teach your employees about security; use the principle of least privilege; keep an eye on your employees; encourage them to back up their data regularly; teach them good cyber hygiene; Limit how many files employees can get to" that may be implemented within an enterprise to maintain cybersecurity goals and safeguard data, particularly from situations involving human error. The developed guidelines are based on ISO/IEC 27001 which is an international standard to manage information security; the standard was originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005, revised in 2013, and again most recently in 2022 and their implementation inside enterprises will increase employees' awareness of their actions to lessen the effects of such occurrences on the systems and data of the firm. The ISO/IEC 27001 standard mandates that administration to conduct a methodical assessment of the information security risks that the organisation faces, considering the threats, vulnerabilities, and repercussions; secondly to propose and execute a standardised and all-encompassing collection of information security measures and/or alternative approaches to risk management (e.g., risk transfer or risk avoidance) to mitigate those risks that are considered unacceptable. Thirdly to establish and maintain an overarching management process to verify that the information security measures consistently fulfil the information security requirements of the organisation.

According to James Reason's twelve principles of error management: "Human error is both universal and inevitable; Errors are not intrinsically bad; You cannot change

the human condition, but you can change the conditions in which humans work; The best people can make the worst mistakes; People cannot easily avoid those actions they did not intend to commit; Errors are consequences do not cause; Many errors fall into recurrent patterns; Safety significant errors can occur at all levels of the system; Error management is about managing the manageable; Error management is about making good people excellent; There is no one best way; Effective error management aims as continuous reform not local fixes” (Reason and Hobbs , 2017).

### **2.6.1.3 Awareness of Data Security**

This refers to the employees of an enterprise being aware of cybersecurity threats and how to identify and manage such threats. It could be as simple as creating an awareness camp to educate employees on how to identify spam emails and how and to whom such emails to report to within the enterprise. Kemper, (2019) stated that many employees of an enterprise expose their data on social media, which has led to data breaches. He noted that it is not as if employees are unaware about the importance of data security, but rather that this is attributed to a lack of awareness of the data security concerns, compliance, and lack understanding of cybersecurity. He proposed that to minimise such a risk, enterprises should create data security awareness programmes that would involve every person within the enterprise. Such programmes should educate the employees on the enterprise cybersecurity policies and incentives of the enterprise on policy adherence.

Valentine, (2006) argued that it was not enough to just have a data security awareness programme that was one size fits all. He believed that for the data security awareness programme to deliver the required results, it must be tailored to the needs of the enterprise's different departments. He believed that the data security awareness programme should pass through different phases: the assessment phase, the identification phase, and the education phase. He stated that without proper tailored data security awareness training, enterprises will constantly be exposed to the vulnerability presented by employees who lack awareness of cyber security and their responsibility for the data security of their enterprise data. Data security awareness



programmes will go a long way towards ensuring that employees understand their roles and responsibilities, especially about enterprise data in the cloud. Data security awareness programmes help to clarify the enterprise's data security policies to avoid misinterpretation of the policies.

The Wilson and Hash (2003) NIST report stated that some factors, like roles and responsibility, have been ignored when creating most of the enterprise data security policies, and it is believed that these factors need to be understood by employees. Choi et al., (2008); Eminaolu et al., (2009), Rantos et al., (2012); Gundu and Flowerday (2013); Dharmawansa and Madhuwanthi (2020); Putra et al., (2020) believe that data security awareness programmes have a positive impact on the effectiveness of enterprise data security policies. Therefore, developing a robust information/data security awareness programme that will be tailored to different enterprise needs and promote a more effective understanding of the data security policies of the enterprise is still a grey area of research that needs to be extensively researched. Data security awareness programmes help employees understand their obligations and serve as a focal point for enterprise data security in the cloud. Because data security policies might be misread and misunderstood, the awareness programme is just as critical as any other information technology practice. An assessment by NIST for cybersecurity framework that tells private organizations in the United States how to evaluate and improve their ability to prevent, detect, and respond to cyber-attacks, found that employees often didn't know what their duties and responsibilities were and that they also need to know about awareness programs.

#### **2.6.1.4 Experience**

This refers to the subjective experience the employees of an enterprise have. It is hoped that the more an employee has experience with the ERP system or the data security policies of the enterprise, the less likely they are to be vulnerable to cyber-attack. This is to assume that more experienced professionals are less likely to be a weak link in a data breach of the enterprise data in the cloud. Subjective experience, according to Forte et al., (2017) and Keupp et al., (2020), contributes to knowledge. Although the

authors have different opinions on the impact of experience concerning enterprise data security, they both believe that experience is necessary for the team that is in charge of enterprise data security in the cloud. (Chadwick et al., 2020; Martynov 2020).

End-users' comprehension of information systems concepts and procedures is contingent upon a variety of human factors, including their prior experiences. According to some experts (Parkin et al., 2009; Sarkar, 2010), experience is the most critical component in determining whether an information security team will succeed in executing a cloud data security policy. Others think that appropriate security behaviour is more about interpersonal, management, and social skills than it is about security experience. For instance, a new access control imposes restrictions on shared data to safeguard corporate secrets. Employees may find this task particularly difficult and in conflict with established norms, especially if they lack experience with the new process.

#### **2.6.1.5 Apathy**

Apathetic withdrawal is a response to conflict and stress that manifests as a retreat inside oneself, a restriction of outside activities, and an affective state of indifference. Additionally, it is present in borderline or psychopathic characters, as well as in adolescence, when it can be detected at times of stress or moderate conflict (Lacey and David, 2009). The globalisation of a dominant market paradigm has resulted in a political, economic, social, and cultural crisis in both Northern and Southern Europe (Hallin and Stylianos, 2002). The intensity of competition for new markets, debt, austerity, and structural adjustment measures enforced by international and European financial institutions all contribute to an increase in disparities and social exclusion to varying degrees (Hermann, 2014). States are financially disengaged from social policies, beginning with education and health (Vis et al., 2011). In terms of control over a new state structure, liberal, technocratic, and market-oriented, which, far from fostering equality and well-being for everyone, eventually results in exclusion (Mares and Carnes, 2009). Individuals are reduced to the role of consumers because of the standardisation of development policies and behaviour, which crushes cultural

identities. In Europe, these dynamics of poverty, isolation, and assault on identity are coupled with disaffection with social movements. Individualization creates an atmosphere of political apathy, resulting in citizens' lack of participation in public affairs (Beck, 2002).

In many companies, this area has become a key managerial support process for the development of labour relations, the strengthening of the organisational climate, and the promotion of good work culture. (Lacey, 2009). It is the entity that develops the skills of officials, generates the quality of life at work, uses the human factor as a competitive advantage of the company, and harmonises business objectives with individual objectives in this way to greatly empower our internal partners who take the company to its peak. Hassan et al., (2022) stated that the objective of human talent management must be understood to work from this concept and that the strategic importance of talent management has grown for multinational enterprises. The general objective of human talent management is the correct integration of strategy, structure, work systems, and people to achieve from people the deployment of all their skills and abilities and achieve efficiency and organisational competitiveness (Pandita and Ray, 2018). In short, maximum productivity must be achieved in a good work environment. Several specific objectives emerge from this general objective (Thunnissen, 2016), such as:

- Help the organization to achieve its objectives and carry out its mission.
- Supply the organization with well-trained and motivated employees.
- Develop and maintain the quality of life at work.
- Provide competitiveness to the organization.
- Allow self-realization and employee satisfaction at work.
- Manage change.
- Establish ethical policies and develop socially responsible behaviours.

Subsequently in an organisational environment, apathy can be defined as employees' unwillingness to contribute to the accomplishment of the organization's aims and objectives. (Karimi-Ghartemani et al., 2022). Apathy about cloud data security processes and rules contributes to the ambiguity around cloud data security policies,

as individuals are unwilling to obey them. Additionally, Locke, (1970) states that employees who work in coercive environments are frustrated and dissatisfied.

#### **2.6.1.6 Stress**

In a world where organisations are becoming increasingly global and competition is becoming increasingly aggressive, success does not depend solely on technology or capital to ensure growth. More important than technology, competitiveness is achieved in a sustained way (Pfeffer, 1995). However, the pressure that members face to maintain the competitiveness of their organisation can substantially increase the levels of stress they experience (Panchal and Cartwright, 2001). In these circumstances, individuals hope to reduce their stress levels through the communicative interactions that they establish with their direct boss, their co-workers, friends, or sometimes with their family (Ray and Miller, 1991). To understand how messages with your boss can help relieve stress, you need to know how these interactions work (Brymer, 1982). Communication is the foundation of these interactions, and in most cases, your direct boss is your most important source of information.

From a leadership point of view, it is important to address the phenomenon of stress in the work context since leaders can exert more powerful influence than any other aspect of work (DeFrank et al., 1985). A relevant leadership approach to understanding the problem of work stress is the transformational one. It has been said that the transformational leader gives a very human approach to the relationship with his followers; he not only encourages them to have a great performance but also pays particular attention to the needs and well-being of each of his followers (Bass and Bernard, 1985). The understanding and management of communication by organisational leaders will largely determine individual, group, and organisational improvement. Regarding its relevance, stress plays an important role. Its effects can be extremely harmful to both individuals and organizations. Stress can cause serious physical and mental health problems for people. Sosik and Godshalk, (2000) reports highly negative impacts on the work of employees and the organization's economic, productive, and performance consequences. So, it's important to know what causes

people to be stressed at work, and what those things are and what can be done about it (Fenlason and Beehr, 1994; Sosik and Godshalk, 2000).

Although studies have been done on work stress and employee communication, of the relationship between leadership behaviours and work-related stress (Sosik and Godshalk, 2000), as well as leadership and communication, few have addressed in the same study the interaction between communication, leadership, and stressors in the organisational context. It is difficult to define stress. Scholars on the subject have not agreed on a single definition. Ramani, (2020) gives a simple and general meaning: "stress implies the interaction of the organism with the environment." The author state that most definitions of stress fall into one of three categories: those based on stimuli, responses, or those focused on the stimulus-response concept (Ramani, 2020). Within the organisational sphere, Bass and Bernard, (1985) explain that stress arises when individuals, groups, or organisations experience or are faced with threats to their stable well-being. Beer et al., (2021) explain that stress at work is inevitable, and its effects are generally negative for both the organisation and the stressed person. The causes or stimuli that provoke stress have been called stressors. Ivancevich et al., (1995) distinguish several levels of stressors: environmental, individual, group, organizational, and extra-organizational. The present research focuses on stressors at the individual level. Among the various personal-level stressors, role conflict and role ambiguity are causes of individual stress that have been repeatedly highlighted in the literature on the subject by Moss, (2015). Role conflict consists of having two or more obligations for the same job that are in opposition to each other or having expectations of the job role that conflict with each other, while role ambiguity implies uncertainty or lack of clarity about what should be done at work, which causes conflict and role ambiguity to be considered causes of stress because they add to the uncertainty of a work situation (Milbourn, 2006; Schumate and Fulk, 2004).

Role conflict and role ambiguity are the two most frequently studied stressors and represent chronic stressors because they are considered constants for an employee. They are conceptualised and measured generically, that is, similarly for any job

position. People with high levels of ambiguity and role conflict tend to communicate less openly and infrequently. The quality of interpersonal relationships or the social climate in the workplace can have a dampening effect on individual responses to these factors. Several studies (Kabay et al., 2012) have shown the strong influence of the supervisor in reducing stress, and although other studies show that co-workers have a role to play in reducing stress, it is also possible that friends or family can reduce it. Individuals' stress levels might be increased in organisations as a result of severe workloads or tight project deadlines. In particular, assigning too many tasks to people makes them feel even more stressed and can lower their morale in an organization. Stressed individuals may have a proclivity to violate cloud data security policies.

### **2.6.1.7 Negligence**

The conquest of new markets requires companies to send more and more staff, missionaries, or expatriates, to countries that are often sensitive in terms of security. For instance, when an expatriate from a developed country is sent to a developing country to establish more business market, it exposes such an employee to both physical security challenges and even the enterprise to information security challenges resulting from the new market. These personnel may face a variety of threats. In this context, companies must put in place special security measures to ensure the protection of their staff and even their contractors; companies should also put some measures in place to ensure information security in the new environment. This duty of protection is first imposed on the company from an ethical point of view. It is also a social responsibility and a lever to enable the company to operate in areas of high-security risk (Shaheen et al., 2021).

Finally, there is a legal obligation liable to be penalised in the event of a data security incident in many places including the EU and the UK. However, the company's responsibility is not limited to the duty to protect their personnel and their enterprise data. Indeed, companies must ensure that this duty of protection is balanced against other imperatives, particularly respect for human rights and the privacy of those who are protected.

Previously, importance was given to different factors within a company, which were believed to be fundamental to its success, such as machinery, financial resources, land, raw materials, and more; However, after decades of experiments and studies, the human being is now given greater importance. Today there is no doubt that people are the most important and fundamental element for business success (Jha, et al., 2021). You can have all the desired economic and financial capital, the best infrastructure, planning, initiative, and motivation for the development of the most successful business, but it cannot achieve this without the ideal human capital (Unger et al., 2011). Likewise, as in each institution and company, planning is carried out to optimise the return on financial capital and investments, greater efforts must be made to improve skills and therefore maximise the performance of employees to maximise human capital (Ndulue, 2012). On the other hand, talking about human talent becomes more complex since human capital is formed by people, and their experience inside and outside the company, and by their ability to solve problems almost instantly thanks to their knowledge and skills. These are thinking beings with desires, interests, and a desire to improve, with needs, problems, and emotions that managers should know how to channel it to enhance employees' skills, qualities, and leadership, develop gifts, dreams, and ambitions, unleash creativity, performance, proactivity, productivity, and dynamism.

Modern Human Talent Management goes beyond the administration of employees as it is oriented to management or administration (Yusuf et al., (2022). This is the challenge: to make employees feel and act like partners with the organization, to get them involved in a process of continuous personal and organizational development, and to make them the leaders of change and improvement when it comes to their data security (Hu et al., 2012). To understand how general managers and those in charge of the talent management area should proceed with the motivation and development of their employees, we must begin by fully understanding these basic concepts and the importance of human talent within an organization.

Employees frequently, and sometimes unintentionally, fail to adhere to security policies (Ismail and Yusof, 2018). When software piracy occurs as a result of employees' lack of awareness of software installation due to a variety of circumstances, including a lack of training, this is an instance of end-user ignorance. Individuals play a substantial role in triggering cloud data security incidents: accidental breaches account for the vast majority (Vroom and Von Solms, 2004). The impact of ignorance and incompetence on an information security system demands immediate response and supervision by information security specialists. While organisations are focusing on developing technological capabilities to address this issue, ignorance and neglect are human issues that demand a different approach. Additionally, auditing human behaviour is challenging. Numerous authors have addressed this issue by arguing in favour of deterrence theory (D'arcy and Herath, 2011), which advocates the use of the threat of criticism (Parker, 1999). Although it is not clear how fear and intimidation are productive methods of dealing with employee irresponsibility and/or ignorance of cloud data security policies.

### **2.6.2 Indirect Human Factors**

Indirect factors have a certain influence on direct factors as well as impact the organization's data security culture (Ključnikov et al., 2019). However, these factors affect people through elements that are largely controlled by organisations and over which individuals have no power (Mortazavi-Alavi, 2016). Therefore, these factors are collective matters managed by organisations (Mortazavi-Alavi, 2016). The indirect effects of ICT are linked to the organisation and characteristics of the workstation. The idea is that ICT combined with certain forms of work organisation can either generate a greater level of satisfaction or, on the contrary, induce more stress (Schraagen and van de Ven, 2011). If, for example, the use of ICT makes employees more autonomous, then the company can set up more versatile teams and a more flexible work organization, which will have repercussions on employee satisfaction: we have an indirect effect, or in other words, a cross effect, of ICT on the organisation of work (Nifakos, Sokratis et al., (2019).



The whole point of this review is to understand indirect human factor. This includes management support, security policy enforcement, enterprises security culture, enterprise budget and enterprises incentives (Mortazavi-Alavi, 2016). Starting from the fact that productivity is linked to the growth of a country, it is understood that government entities provide the necessary support for companies to apply these corporate improvement practices. It has also become a subject in international cooperation discussions, which is a clear example of the work of entities such as the International Labour Organization (ILO), the United Nations Development Program (UNDP), the United Nations Educational, Scientific, and Cultural Organization (UNESCO), and the Organization for Economic Cooperation and Development (OECD) (Naranjo et al., 2016).

To boost productivity, from the point of view of human capital, it is necessary to consider all the factors that stimulate it in the company (Bocigas, 2015). According to the author, companies must provide workers with an adequate workspace if optimal performance of their work is to be achieved. Similarly, adopting new technologies will enable us to increase capital efficiency and improve the way capital contributes to workers, thereby increasing human resource productivity (Aral, et al., 2012). Human capital: the qualification at the highest level of a worker, has a positive effect that directly results in productivity (Danquah and Amankwah-Amoah, 2017). The assumption is that the more preparation and knowledge a worker has about the work he does, the better his performance and the quality of the time he spends at work (Drucker, 2018).

Enterprise budget is an indirect human factor. Because running an organisation requires money, effective budget planning is essential to its continued survival (Berry, 2010). Enterprises need to have an efficient cost strategy in place in order to properly address the technological and personnel needs of a cloud computing security in order to ensure that it achieves its goals (Xue and Xin, 2016). Although enterprises are obligated to spend on enterprise data security, they might not be able to sustain a sufficient level of investment. This is especially so for SMEs who may not have the

required resources. As a result, an enterprise should focus its attention on the areas that are most vulnerable and at risk, such as backup and disaster recovery planning (Snedaker, 2013). According to Duncan et al (2022) in their paper “cost-effective permanent audit trails for securing SMEs systems when adopting mobile technologies” SMEs face peculiar security challenges due to the nature of their enterprise and more importantly the resources available in the enterprise. The authors proposed effective security solutions for SMEs taking into consideration their financial means. This gives small and medium enterprises the option of securing their data in cloud.

The impact of enterprise budget on their enterprise data security in cloud is evident as many security technologies and security personnel are expensive. The value of training becomes apparent when the topic of cost effectiveness is brought up. Evaluations are required to determine the number of trainees who use the skills taught, how long they continue to use them, and how long the training content complies with enterprise cloud data security policies. Better training effectiveness data are also required. It is possible to gauge effectiveness using performance standards like employee KPI after training, or by looking at interim results (O’Malley et al., 2013). Some cost-cutting strategies like automated user access provisioning, require less expensive training packages (Ni et al., 2009; Markus and Tanis, 2000). This demonstrates the link between direct human factors and budgeting.

Culture is people’s way of doing things in a particular context, that is, "culture is a set of shared assumptions and values, ways of looking at life, beliefs, rules, procedures, and ways of acting that affect but don't define each person's way of thinking and feeling about the way other people think and feel." (Spencer-Oatey and Franklin, 2012). Enterprise culture is the way an enterprise does things. The enterprise culture around enterprise data security in cloud will have a great impact on those data. According to Rebollo et al., (2015) enterprise information security culture (EISC) offers enterprises a behavioural framework that makes it easier for them to defend their information assets and enterprise data in cloud. However, some authors contend that EISC is a management issue and cannot be completely identified (Arbanas et al., 2021).

Enterprise security policy may be used as an example to show the EISC in organisations. Employees adhere to an enterprise security policy that is integrated into the EISC and the larger organisational culture. To ensure that EISC is promoted in order to improve the enterprise security policy, management support is required. (Alhogail and Mirza, 2014). But the study by EISC shows that an enterprise's culture will have an effect on their enterprise data security in the cloud (El-Gazzar, 2014). This is because its principles are complicated and difficult to understand.

In an enterprise setting, communication is the interchange of messages and concepts amongst individuals within and outside the enterprise. Employees can transmit the right message to the right employee through communication channel available within the enterprise (Bui, 2019). As a result of the importance of the flow of information within and outside the enterprise, this has led to the development of information communication technology channels, and this has played an important role in both traditional and cloud computing security. (Avstriyskaya and Voronova, 2022). There are numerous ways to communicate, but the most common is face-to-face and textual communication, both electronically and manually. The use of communication can increase IS awareness and inspire employees as expected, to abide by security regulations. On the other hand, if communication fails or is abused, the results could be damaging to enterprise information security systems.

Effective communication between management and employees makes sure they are aware of the enterprise security policy and comprehend why it is in place for successful execution. Efficient communication entails communicating with all the organization's personnel at all levels especially by moving from top to bottom (Zhang, et al. 2022). Communication examples include raising security awareness, posting on notice boards, workshops as well as communication over the phone, email, and in person (James et al., 1995; Warkentin and Beranek, 1999). When emails are exchanged between individuals from one enterprise to another enterprise, secrecy is crucial. Employees need to be made aware of the types of information that can be sent to outside parties without compromising confidentiality.

Regarding security policy enforcement within an enterprise, Sun et al., (2009) believes that data security policy is an enterprise blueprint that contains rules, regulations and processes of their data security both within and outside the enterprise. All employees are required to be aware of the enterprise data security policies and take part in its implementation as appropriate to their level. Clear loopholes exist in this area, and frequently unprovoked and unpunished violations of these enterprise data security policies occur. As part of the policy enforcement approaches, Herath and Rao, (2009) argue that incentives within the enterprise will encourage employee acceptance of the data security policies. Liu and Gao, (2022) argued that although incentives are okay, uncontrolled incentives can lead to unhealthy competitiveness among employees which can be damaging. The authors believes that moderation, monitoring and control of the enterprise incentives is important to achieve enterprise data security enforcement and encouragement of secure behaviours.

The support of top management in the achievement of any enterprise data security policies cannot be overemphasized. For any enterprise data security policy, management's job is to promote such policy and communicate it to the rest of the organisation (Kabanda and Mogoane, 2022). The distribution of an adequate budget, which is solely under the discretion of top management, is a clear example of this. Senior management needs to understand how closely linked enterprise data security policy is to how the company runs and then prioritize it especially because there are financial and reputational consequences if an enterprise faces any form of data security breach (Balawejder et al., 2019). Work logistics refers to all activities related to the managerial skills of a company. Here, the planning the work, its operational management, and the way the supervisor delegates, controls, and communicates within a company generates a positive effect on the worker.

The size of a company is closely related to the productivity of its human capital, the greater the number of qualified employees, the greater the productivity. Small and

medium enterprises (SMEs) have numerous disadvantages, as compared to larger ones, leading to reduced productivity (Aw, 2001; Taymaz, 2005). This is due to:

- It is more difficult to take advantage of economies of scale.
- Minimal bargaining power against the market.
- They present a great distance compared to economies of scope.
- low capacity to attract investment.
- Greater temporality that slows down long-term investments.
- Their small organizational structure makes it difficult for them to specialize at tasks.

Marvel et al., (2011) suggest to SMEs that they need to minimize the gap that allows them greater productivity to compete and be sustainable, working on three types of actions related to the individual:

- Employee motivation, skills, job satisfaction, and empowerment within the organization.
- General aspects such as participation, cohesion, and conflict management with the organization.
- Strengthen cooperativity by emphasizing organizational culture, climate, and leadership.

To determine the success of implemented initiatives and their impact on productivity, it is necessary to carry out permanent evaluations, to do this, management indicators are used: efficiency, effectiveness of information security that translate into productivity. In addition to measuring the level reached, it allows decision-making and actions to improve when the indices do not show the expected results (Daz, 2017).

The decision to move to the cloud for an SME is far from being a futile decision because it is neither easily reversible nor neutral (Bouaynaya, 2017). It stems first of all from an organisational obligation to minimise short-term IS investment costs. Any SME that is eventually led to benefit from an IaaS/PaaS-oriented cloud service,

whether directly or indirectly, will eventually need to develop a relationship between cloud providers and the SMEs. Therefore, this is not a simple romantic relationship but a working arrangement that needs to be guided by the service level agreement (SLA). Cloud computing connects several actors in a multi-level network and creates mutual reliance between the first layer's customer (SME) and its cloud provider(s). This is because for SaaS delivery model, adopting enterprise do not have the underlying infrastructure. They use the technological resources of PaaS and IaaS for the cloud service providers to be able to offer an appropriate application layer to the business of their customers. Interdependence in IS has always been the focus of several authors, such as De Corbière and Rowe, (2013); Marciniak et al., (2014); and David and Rowe, (2016), who have sought to explain the sharing of information and the modality of its sharing from an inter-organizational perspective. In particular, the work of De Corbière et al. (2010) distinguished between the nature (technology, information, process) and type (sequential, reciprocal, or pooled) of interdependence between organizations. Of course, it is not possible to affirm that the type of interdependence is pooled as compared to PaaS and IaaS providers, since there is a certain reciprocity between providers and customers.

The growing need to collect data for strategic purposes creates an informational dependence on the initial client, namely SMEs, and thus suggests that the relationship of dependence is rather reciprocal: a top-down technological interdependence and an informational interdependence. Information systems on both technical and application levels nonetheless directs decision-makers towards the adoption of these outsourced tools (Rajaeian, et al., 2017). These increasing numbers of adoption decisions demonstrate that cloud computing is a paradigm shift that has far-reaching implications for the company's strategy and business models (Stuckenberg, et al., 2011). The scope of this should not be underestimated, the risks in terms of confidentiality of data hosted in the clouds and the reversibility of the service.

As businesses evolved, the volume of information and transactions increased, so organisations felt the need to resort to the automation of their information systems. For

example, they had to automate accounting records and various operational processes, which had to be supported by technology assets such as servers, networks, specialised software, and hardware. However, as technology advanced, fraud and computer crimes became inextricably linked, to the point where a computer criminal can now steal economic resources from an organisation from the comfort of his own home, leaving no trace, when the enterprise manages the data breach incident poorly (Wall, 2017). This situation exacerbated the large financial embezzlement that has occurred worldwide. There is a need for auditors to develop new skills and knowledge, especially in the area of technology (Otero, 2018).

On the other hand, indirect variables can affect both direct and indirect factors, as well as enterprise cloud data security. We consider five indirect elements, including finance, culture, communication, the enforcement of security measures, and managerial support. To ensure that cloud data security policies fulfil their objectives effectively, enterprises must have an effective cost strategy in place, which should be used to meet cloud data security policies' technological and personal requirements. Communication can be used to raise employee understanding of cloud data security and to motivate them to follow security policies and procedures. To ensure that employees are aware of the cloud data security policy and understand why it must be implemented effectively, management must communicate this effectively. Enforcing cloud data security policies is critical for cloud-based ERP systems, and management should commit to properly implementing them. Assistance to the ERP implementation management team: If policies relating to cloud data security are to be implemented effectively, management must support them from the design stage through all review stages. Management's role in the deployment of an ERP system entails not just lobbying for the technology, but also sending a clear message to the rest of the organisation regarding the cloud data security policy (CHU et al. (2022).

Utilizing effective communication strategies can enhance employees' comprehension of cloud data security measures, fostering a culture of awareness and responsibility. By elucidating the importance of adherence to security protocols and procedures,

organizations can inspire employees to actively engage in safeguarding sensitive data within cloud environments.

## **2.7 A Systematic Literature Review on the Adoption of ERP Systems within Enterprises**

A Systematic Literature Review on the Adoption of ERP Systems within Enterprises refers to a methodical and structured analysis of existing academic and professional literature related to the implementation and utilization of Enterprise Resource Planning (ERP) systems in organizations. This type of review involves systematically identifying, selecting, evaluating, and synthesizing relevant research studies, articles, and publications to gain insights into the factors, trends, challenges, and best practices associated with ERP adoption.

### **2.7.1 Introduction**

Enterprise Resource Planning (ERP) systems are integrated software solutions designed to streamline and automate diverse business processes across all functional areas of a company (Gupta and Kohli, 2006). ERP systems have garnered a great deal of interest due to their potential to enhance operational efficiency and decision-making skills (Nofal and Yusof, 2013). The cloud-based ERP system is simply those ERP system that leverages the use of internet to host the ERP system on the Cloud Service Providers cloud network as against the traditional on the premises network (Saini et al, 2014). Offering scalable and cost-effective solutions for businesses of all sizes, cloud computing has garnered significant attention internationally. In recent years, Nigeria, one of the foremost economies in Africa, has seen a rise in the adoption of cloud-based ERP systems due to some of the benefits discussed in the subsequent paragraphs (Usman et al., 2019).

*Cost savings:* With cloud-based ERP systems, you don't have to spend a lot of money on hardware, software licences, and IT equipment up front. Businesses in Nigeria can get access to ERP functions through a subscription-based approach, which cuts down



on capital costs. Small and medium-sized businesses (SMEs) with limited funds will benefit the most from this cost cut (Usman et al., 2019). *Scalability and adaptability:* As a result of the scalability of cloud-based ERP systems, Nigerian businesses can simply modify their system tools to meet their requirements (Mallo and Ogwueleka, 2019). As a company develops or adapts with the seasons, it can scale up or down its ERP tools without significant difficulty. This enables businesses to enhance their processes and rapidly adapt to market changes. Cloud-based ERP systems *enable real-time access to data* and functions from anywhere with an internet connection (Lee et al., 2017). This makes it simpler for individuals to collaborate. This facilitates collaboration and communication between the various departments, branches, and even remote teams of Nigerian enterprises. Employees can collaborate on projects, exchange information, and simultaneously access the ERP system. This increases productivity and improves operation efficiency (Lee et al., 2017).

*Improved Data Security:* Cloud-based ERP systems frequently employ advanced security measures, including data protection, routine backups, and stringent access controls (Duan et al., 2013). By utilising the expertise and infrastructure of cloud service providers, Nigerian businesses can increase the security of their data in comparison to managing an on-premises ERP system on their own. This is especially crucial as the likelihood of cyber-attacks and data intrusions increases. Cloud-based ERP systems provide Nigerian businesses with *access to the most recent software versions and updates* without the need for manual installations or upgrades (Tongsuksai et al., 2023). Cloud service providers are responsible for system maintenance, problem fixes, and security updates (Tabrizchi and Kuchaki Rafsanjani, 2020). This frees up internal IT resources and makes ERP systems with numerous moving parts simpler to manage. *Business Continuity and Disaster Recovery:* Cloud-based ERP systems include disaster recovery tools (Orosz et al, 2019). Businesses in Nigeria can benefit from the automated data backups and robust recovery processes that cloud service providers have implemented. This feature ensures that vital business data is secure and can be restored in the event of an unforeseen event, such as a natural disaster or system failure.

Cloud-based ERP systems frequently provide users with *access to sophisticated features such as AI-driven data, machine learning, and predictive modelling* (Helo and Hao, 2022). Using these capabilities, Nigerian businesses can get more out of their data, make better decisions, use their resources more efficiently, and discover new growth opportunities. Even though cloud-based ERP systems have numerous advantages, Nigerian businesses must consider who possesses the data, how well the internet functions, and the vendor's dependability when selecting a cloud service provider. In addition, for cloud-based ERP systems to be the most beneficial to Nigerian businesses, appropriate planning, change management, and staff training are required (Kuranga et al., 2021).

We now look at the obstacles faced with implementing cloud-based ERP systems in Nigerian businesses. Factors such as limited internet infrastructure, data privacy and regulatory concerns, vendor selection, customization needs, and organisational change management. Understanding and addressing these obstacles is essential for the successful adoption of cloud-based ERP systems in Nigeria. *Internet Connection:* For cloud-based ERP systems to work well, they need to be able to connect to the internet quickly and reliably (Weng and Hung, 2014). But in some parts of Nigeria, the infrastructure and ability to link to the internet may be limited or unstable. This can cause problems like slow data sharing, downtime for the system, and trouble getting to the cloud-based ERP system. Businesses in Nigeria need to figure out how well they can connect to the internet and look into backup choices.

*Data Security and Privacy:* With cloud-based ERP systems, private business data is stored and processed on remote servers that are owned by cloud service providers (Malik et al., 2018). Nigerian businesses need to carefully look at the security steps that the cloud service provider they choose has in place. To keep the organization's data safe and private, things like data encryption, access controls, regular checks, and following data protection laws (like the Nigeria Data Protection Bill, 2023.) should be thought about. *Data Sovereignty:* Data sovereignty is a term for the legal and

regulatory rules that apply to where data is stored physically (Lukings and Habibi Lashkari, 2022). When Nigerian businesses use foreign cloud service providers, they need to think about where their data will be stored. To avoid legal or regulatory problems, it is important to follow local laws and rules about data security and to know who has control over the data.

*Reliability and support of the vendor:* For a cloud-based ERP application to be successful, it is important to choose a reliable cloud service provider (Al-Ghofaili and Al-Mashari, 2014). Nigerian businesses should look at the provider's track record, financial stability, reputation, and amount of customer support. It is important to make sure that the vendor can provide reliable system uptime, timely support, and a long-term commitment to meet the goals of the organisation (Grabski et al, 2011). *Data Migration and Integration:* It can be hard to move data from old systems to a cloud-based ERP system (Abd Elmonem et al., 2016). Businesses in Nigeria need to carefully plan and carry out data migration strategies to make sure that the shift goes smoothly, and that no data is lost or changed. Integration with other systems, such as financial software, customer relationship management (CRM) systems, or third-party applications, should also be thought about to make sure that data flows smoothly throughout the organisation and that all processes are automated (Abd Elmonem et al., 2016).

*Change Management and User Adoption:* When a cloud-based ERP system is put in place, processes and routines need to change in a big way (Hustad et al., 2020; Bjelland and Haddara, 2018). Businesses in Nigeria need to put money into change management programmes so that workers can learn about the new system, its benefits, and how it will affect their daily tasks. To get the most out of a cloud-based ERP system, it's important to make sure users accept it and deal with resistance to change; and this can be achieved through training and awareness programmes (Elragal and Haddara, 2013). *Customization and flexibility:* Most cloud-based ERP systems offer a basic set of features and functions (Imene and Imhanzenobe, 2020). Nigerian businesses should think carefully about whether or not the system can be changed to fit their needs. It's

important to think about how flexible the system is and how well it can adapt to future growth, changes in business processes, and the ability to work with new technologies or modules (Imene and Imhanzenobe, 2020).

To deal with these difficulties, the cloud-based ERP system in Nigerian businesses needs to be carefully planned, managed, implemented with the help of partners with experience, and constantly monitored and evaluated. Existing research has examined the challenges of adopting cloud-based ERP systems (Shatat and Shatat, 2021; Ahn and Ahn, 2020; Saa et al., 2017), but the knowledge gap of adopting enterprise end-users in Nigerian businesses has not been explored. When implementing their cloud-based ERP systems, these enterprises' differences and similarities must be taken into account in order to address the challenges of customization and flexibility posed by the fact that they come from various sectors of the Nigerian economy. This systematic review investigates the history of adoption of cloud-based ERP systems in Nigerian businesses, taking into account the factors that influence the adoption of cloud-based enterprise resource planning (ERP) systems, as well as the associated benefits and challenges of the adoption of cloud-based ERP systems in Nigerian enterprises. The following reviewing questions were adopted to guide the structure of researching:

- When did enterprises start using cloud-based ERP systems? **RQ1**
- When did enterprises in Nigeria start using cloud-based ERP systems? **RQ2**

### **2.7.2 Review Methodology**

The review adopts a systematic approach to identify relevant research articles. This is because using a systematic literature review approach makes it easy to map understating on the reviewing questions, it also quick using the tools available for text mining, data analysis and search the various databases (Newman and Gough, 2020). Key academic databases, such as Scopus and IEEE Xplore and other sources like Google Scholar are searched using specific keywords which are all related to ERP system adoption. The search is limited to articles published within a specified timeframe, typically within the past 10 years. To address the reviewing questions, a

systematic literature review was conducted using academic databases in accordance with the Preferred Reporting Items in Systematic reviews and Meta-Analysis (PRISMA) guidelines. The procedure involved identifying pertinent keywords, the years to limit the scope of the search, inclusion/exclusion criteria, and the databases that need to be examined. All articles were evaluated for inclusion, with data required by the reviewing questions extracted and insights from the papers harmonized. Figure 2.5 below depict Prisma diagrams for queries of literature and academic databases, respectively.

### **2.7.2.1 Search Strategy**

To find appropriate literature for this systematic search, we made a search strategy. This search was limited to three databases: Scopus, IEEE Xplore, and Google Scholar. The search terms used were "Cloud-based ERP systems" OR "Cloud-based ERP systems in Nigeria." All of the searches covered the time period from 2013 to 2023 and included Journal articles, Research articles, Review articles, and Conference articles that were free to read and were only written in English.

### **2.7.2.2 Selection Criteria**

The PRISMA Statement (Moher et al., 2009) was used to decide what the selection criteria were. The PRISMA Statement, established by Moher et al. in 2009, serves as a guideline for conducting systematic reviews and meta-analyses in various fields, ensuring methodological transparency and rigor. Its adoption in this context indicates a commitment to adhering to standardized procedures for selecting relevant literature. The PRISMA Statement outlines criteria for literature selection, including specific guidelines for identifying eligible studies and excluding irrelevant ones. By following the PRISMA Statement, researchers can mitigate bias and ensure the reliability and replicability of their systematic literature review process. This systematic approach helps maintain consistency and objectivity throughout the selection process, enhancing the credibility of the review's findings. Ultimately, utilizing the PRISMA Statement contributes to the quality and trustworthiness of the research output, promoting robust evidence-based conclusions.

The search was mostly about mapping the current literature on Cloud-based ERP systems in the fields of Computer Science, Engineering, Decision Science, Business Management, and Accounting. Even though the search was limited to Computer Science and Decision Science. The search documents generated were done between 2013 and 2023. The search did not look for any items from before 2013. This search was mostly focused on countries in Europe, the UK, and Africa, so articles from these countries were given more weight and although relevant stories from other countries were not left out. At this point, a total of  $n=256$  records had been pulled out. A total of  $n=169$  were excluded at this stage. There was a total of  $n=87$  records extracted at this stage.

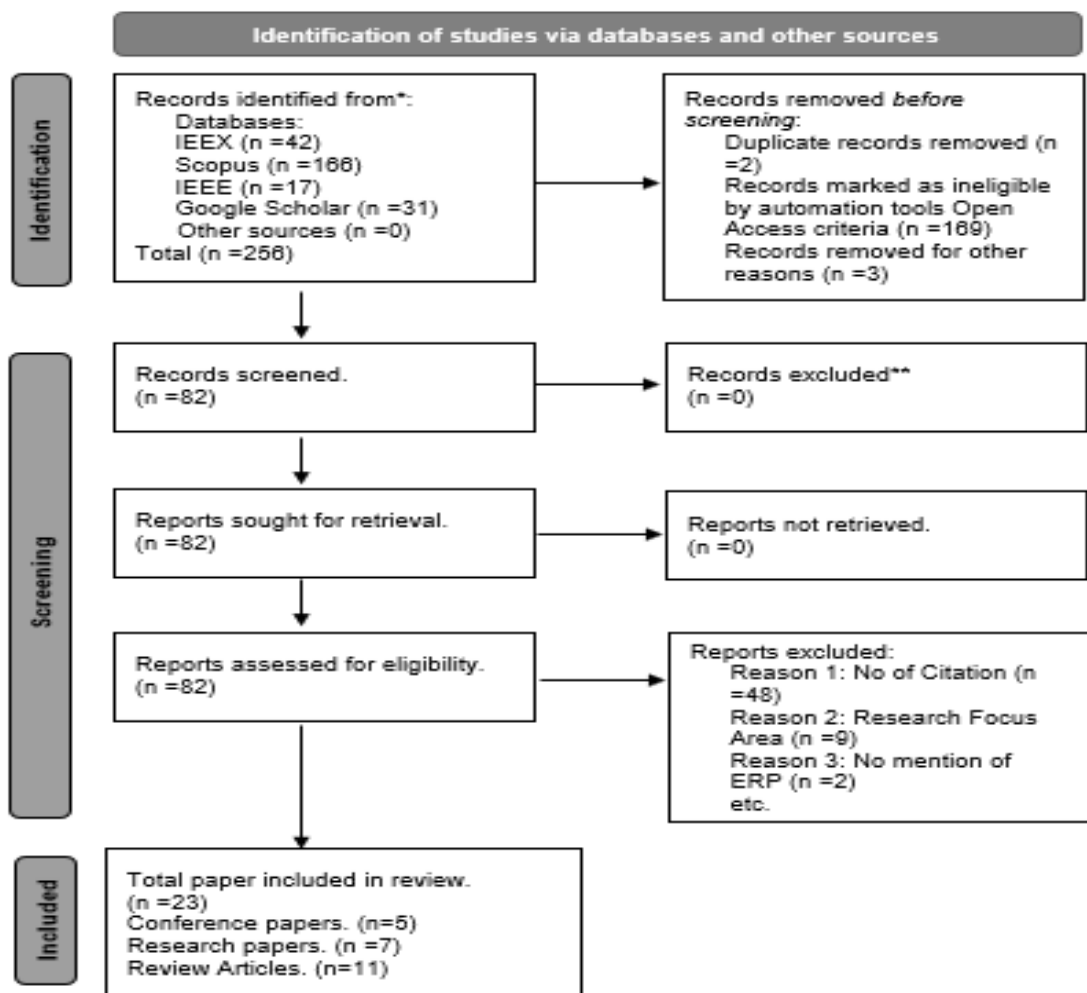


Figure 2.5: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews (MJ, et.al; 2021).

### **2.7.2.3 Evaluation of the Quality**

This study relied solely on previously published research in the form of journal articles, review papers, conference papers, and original research publications. In order to ensure that the quality of the review is not compromised, every instance of duplication was meticulously examined. The abstracts of the articles were scrutinised in great detail for the purpose of determining the level of analysis and level of purification of the articles in order to guarantee the high quality and relevance of the academic literature that was taken into consideration during the review process. At a subsequent stage, a careful assessment of each study report was carried out. The criteria for exclusion were restricted to only include publications to which we have access to the complete text via open access and papers that were published in the English language. In addition, following the removal of articles that were found to be identical to others in the database, the total number of articles excluded from the analysis increased by  $n=59$ . Following an analysis of each article based on the aforementioned inclusion and exclusion criteria, we chose  $n=82$  articles to be included in the study. Figure 2.5 above displays the inclusion and exclusion criteria at each stage.

### **2.7.2.4 Data Extraction**

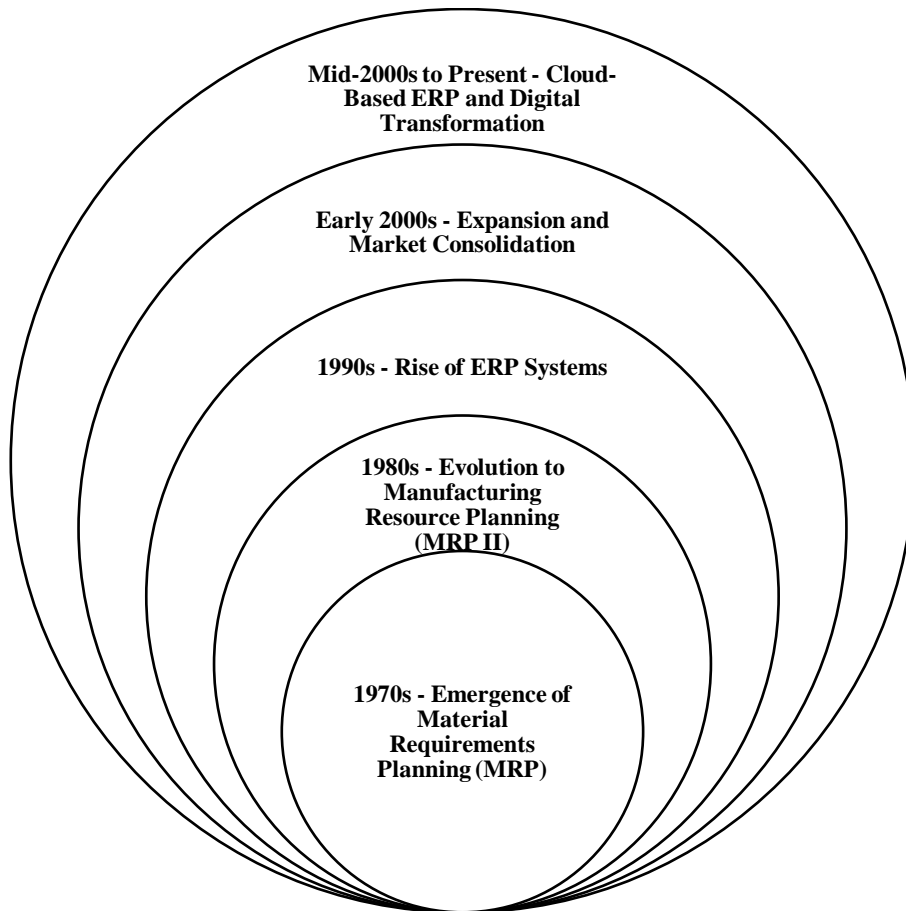
In the data extraction phase,  $n= 23$  articles were selected, and the characteristics extracted were:

1. The articles must be either original research papers, review papers, journal papers, or papers presented at conferences. It was decided not to include things like published reports, news publications, blogs, case studies, etc.
2. The article needs to be written in English and be from a discipline related to computer science, engineering, decision science, business management and accounting.
3. Extracted articles were published between 2013 to 2023.
4. The extracted papers were from UK, EU and African countries.
5. The extracted papers have at least 5 citation and a focus on cloud-based ERP systems.

6. The extracted papers were Open Access.
7. The extracted papers need to have at least one context focus on “cloud-based ERP history”, “Nigeria enterprise”, “SMEs”, ERP adoptions”.

### 2.7.3 RQ1: When did enterprises start using cloud-based ERP systems?

The enterprise adoption of Enterprise Resource Planning (ERP) systems has a lengthy, multi-decade history. Here is an overview of the most significant ERP system adoption milestones and trends as seen in Figure 2.6 below:



*Figure 2.6: The history of ERP systems in enterprises*

Material Requirements Planning (MRP) systems were introduced to aid in the management of manufacturing processes in the 1970s (Bjelland and Haddara 2018). MRP systems optimised production planning and inventory management, laying the groundwork for later ERP systems. The 1980s saw the development of Manufacturing



Resource Planning (MRP II) systems, which built upon MRP systems (Beleț and Purcărea, 2017). MRP II broadened the planning scope and incorporated additional functional areas, such as finance, human resources, and distribution. This signified the transition from departmental-specific systems to enterprise-wide solutions. In the early 1980s, Royal Philips Electronics of the Netherlands was an early adopter of enterprise resource planning (ERP) systems (Peeters, 2009). Philips was poised to develop its own ERP solutions in the 1960s, but in 1979/80 it ceased its own development and began purchasing IBM's integrated standard products. However, early adopters like Philips may have contributed to the beginning of the ERP industry.

MRP II systems evolved into full-fledged ERP systems in the 1990s (Kurbel and Kurbel, 2013). ERP systems integrated diverse business functions, such as manufacturing, finance, human resources, supply chain, and sales, across an organisation (Johnson et al., 2016). They provided organisations with a centralised database, standard processes, and real-time visibility, enabling them to streamline operations, enhance decision-making, and increase efficiency. According to Johnson et al., (2016), although the use of technology in Human Resource Management began in the 1940s, the field has frequently lagged behind other functional areas, such as accountancy and supply chain management, in the application of innovative technologies (DeSanctis, 1986). The human resource management (HRM) discipline did not acknowledge the significance and benefits of technology until the 1990s (Kavanagh, Gueutal, and Tannenbaum, 1990), and relatively little theory and research has been conducted on the topic (Gueutal and Stone, 2005).

Authors like Chofreh et al., (2014), stated that the 20<sup>th</sup> century witnessed a rapid expansion of distribution systems, which increased the demand for goods and services. This resulted in industry participants altering their production methods, resulting in environmental pressures and business responsibilities. The triple bottom line approach, which focuses on environmental, economic, and social objectives, is essential for achieving sustainability. Organisations that incorporate key sustainability drivers can benefit from market.

ERP systems continued to evolve throughout the early 2000s (Bjelland and Haddara 2018), implementing new technologies such as web interfaces, business intelligence, and mobile access. Larger software vendors acquired lesser ERP companies in order to expand their product portfolios and market presence (Bjelland and Haddara, 2018). Cloud-based ERP systems have acquired popularity in recent years (Haddara et al., 2022). Cloud ERP offers scalability, cost-effectiveness, implementation simplicity, and accessibility from anywhere (Haddara et al., 2022). According to Haddara et al., (2022), Cloud-based enterprise resource planning (ERP) systems are gaining popularity among businesses due to their accessibility and affordability. This author examines the obstacles associated with the adoption of cloud-ERP by SMEs, concentrating on the enterprise system experience cycle. The findings imply that SMEs should consider customization limitations, reliability issues, data security risks, and change management of the highest quality. In the pre-implementation phase, change management should be considered despite disagreements regarding the applicability of customization and data security. Managers should ensure that sufficient high-quality data and legacy systems are utilised during the implementation of the new cloud-based ERP system.

The author concurred that there is a dearth of literature on the challenges faced by SMEs in cloud-ERP implementations, and that technicalities are required to better comprehend the issues and their effects. The authors suggested that future research should concentrate on developing a suitable framework for the cloud-ERP lifecycle in SMEs, taking into account the implementation difficulties encountered by SMEs during cloud-ERP implementations.

Demi and Haddara, (2018) study investigate the effect of cloud-based ERP on the retirement phase of the ERP lifecycle, with a particular concentration on Xledger. According to the findings of the study, a shorter retirement phase is attainable through easier exits and extended ERP lifecycles. However, transferring costs and vendor lock-in continue to be significant barriers to the retirement of cloud-based ERP systems.

The author recommends that future research should investigate customer perspectives, the integration challenges between legacy systems and cloud-based ERP, and how to reduce vendor lock-in. The authors suggest that to evaluate the changes and effects of cloud technology on systems, lifecycles, and organisations, additional research is required.

ERP systems have become crucial enablers for organisations to adapt to changing business landscapes, leverage data analytics, automate processes, and embrace emerging technologies such as artificial intelligence and Internet of Things (IoT) as the significance of digital transformation grows (Johansson et al., 2015). Focusing on user experience, integration with external systems, and intelligent automation, ERP systems continue to evolve in the present day. Modern ERP solutions frequently feature modular architectures, allowing businesses to select and incorporate specific functionalities based on their needs. Integration with other software applications and external collaborators is another important aspect of ERP implementations.

In the late 2000s and early 2010s, businesses adopted cloud-based enterprise resource planning (ERP) systems. During this period, an increasing number of businesses adopted cloud technology and cloud-based ERP systems. This was due to the improvement of internet connections and the realisation by businesses of the benefits of cloud computing. According to Johansson et al., (2015), their study examines the relationship between organisational size and cloud ERP adoption. It was discovered that cloud ERP adoption is not an apparent solution for all organisations, as the number of ERP users and the sensitivity of the organization's data are critical factors.

The adoption of cloud-based ERP is contingent upon the integration of other systems and the organization's advanced ERP usage. Cost and financial resources are the primary factors influencing SMEs' adoption of cloud-based ERP, with modest capital expenditures serving as the primary driver. Small and medium-sized enterprises are concerned with jurisdictional compliance and security issues, whereas large organisations are more concerned with perceived insecurity.

Johansson et al., (2015), mentioned that much of the current research on cloud-based enterprise resource planning systems (ERPs) has focused on small and medium-sized enterprises (SMEs), rather than businesses of all sizes. Future research could evaluate the perceptions of cloud ERPs by small and medium-sized businesses and investigate the underlying differences. In addition, companies operating in distinct industries or markets may perceive opportunities and concerns differently, suggesting that future research could investigate and compare the value of cloud ERPs for companies operating in distinct industries and countries.

According to Bjelland and Haddara, (2018) their study analyses the evolution phase of the ERP lifecycle framework, with a particular emphasis on forced continuous updates in cloud-based ERP systems. It investigates factors including change management, process, people, and product. The results indicate that the evolution process for consumers is prolonged and more comprehensive than for on-premise ERP systems. Further research is required to comprehend the perspectives and workarounds of consumers and vendors. It is essential to investigate cloud-based ERP systems in other lifecycle segments.

Before cloud-based ERP systems came along, most businesses used standard ERP systems that were installed on-site (Aghimien et al., 2021). With these on-premises systems, organisations had to host the software and infrastructure on their own property, which meant they had to pay a lot of money up front for hardware, software licences, and upkeep. When cloud computing came along, it changed the way ERP systems work (Bjelland and Haddara, 2018). The infrastructure and hosting of cloud-based ERP systems are now taken care of by third-party cloud companies. Organisations could access ERP software and data offline through the internet, so they didn't need infrastructure on-site and didn't have to pay as much up front. Authors like Akin et al., (2014), argued that the poor state of ERPs in Nigerian universities has limited its influence on socioeconomic development, the calibre of graduates, and research outputs. It states that cost is a significant barrier to the survival of ERPs in

education in Nigeria, which cloud computing can help overcome. Cloud computing can reduce hardware, software, and IT maintenance costs, as well as offer improved availability, minimal environmental impact, reduced IT complexities, mobility, scalability, increased operability, and decreased investment in physical assets. However, data insecurity, regulatory compliance concerns, lock-in, privacy concerns, unsolicited advertising, reliability challenges, and resistance to change in technology are obstacles to successful adoption within the Nigerian universities, the authors noted. Recommendations for cloud adoption given by the authors, include accommodating mobile device dependence, opening technology infrastructures for research advancements and that future research should investigate the management of constraints and the evaluation of Nigerian universities' readiness to implement ERPs for various services.

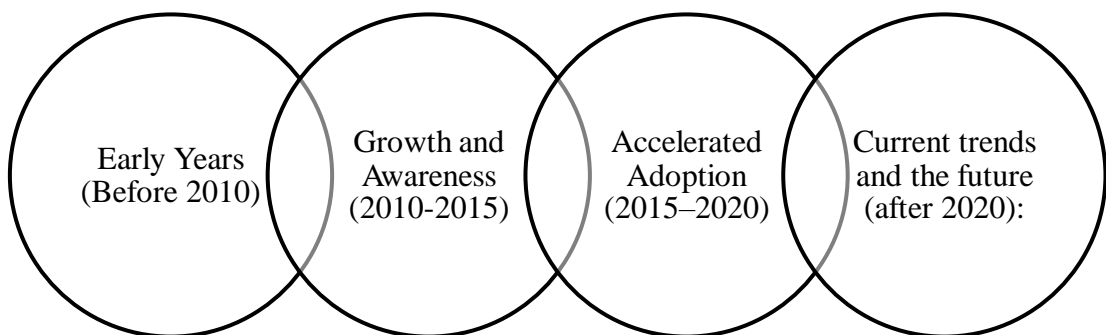
Around the end of the 2000s and the beginning of the 2010s, cloud-based ERP systems started to gain popularity as companies saw the benefits of the cloud's scalability, low cost, accessibility, and flexibility. During this time, standard on-premises ERP systems gave way to cloud-based options. According to Uchenna et al., (2015), not many fully virtualized organizations deploy cloud computing environments for organizational practices in Nigeria. However, many organizations exhibit characteristics indicative of cloud computing adoption. The economic benefits of cloud computing adoption and potential for corporate value creation make virtualization a strategic asset for visibility, competitiveness, customer satisfaction, shareholder wealth creation, and stakeholder value creation.

Since 2010s, the number of businesses that use ERP systems in the cloud has slowly grown. This growth is driven by several factors, including the benefits that cloud-based ERP systems offer. The specific rate of growth may vary across industries and regions, and it's essential to note that the landscape is continually evolving. Factors such as data privacy regulations, industry-specific requirements, and the overall maturity of cloud adoption in different sectors can influence the pace of ERP migration to the cloud. Cloud technology has grown up, and cloud service companies have improved their

services to meet the changing needs of businesses (Hrishev, 2020). Today, companies of all sizes and in all industries use cloud-based ERP systems (Llave, 2017). These systems drive digital transformation and give businesses a competitive edge. Overall, the history of ERP systems reflects a progression from focused planning systems to comprehensive enterprise-wide solutions that drive operational efficiency and support strategic decision-making in organizations of all sizes and industries as seen in Figure 2.6 above.

## **RQ2: When did enterprises in Nigeria start using cloud-based ERP systems?**

Cloud-based ERP systems have gotten a lot of interest and use around the world because they are scalable, cost-effective, easy to access, and flexible (Salim et al, 2015). Cloud-based ERP solutions have been used more and more in Nigeria over the past few years. Here is a brief history of the adoption as seen in Figure 2.7 below:



*Figure 2.7: The history of adoption of cloud-based ERP systems in Nigerian enterprises*

**Early Years (Before 2010):** During this time, Nigerian businesses didn't use cloud-based ERP tools as much as they do now. In Nigeria, many businesses used traditional on-premises ERP systems or manual methods to run their businesses. Still in its early stages, cloud computing raised concerns about data protection, reliability, and connectivity (Mallo and Ogwueleka, 2019).

**Growth and Awareness (2010-2015):** Beginning around 2010, Nigerian businesses became more aware of cloud computing and its possible benefits (Abubakar et al, 2014). As internet connections got better and cloud technology got better, more

companies began to think about cloud-based ERP systems as a good option to traditional solutions (Nasim et al., 2020). But adoption was still slow because of things like a lack of infrastructure, worries about who owns the data, and a desire for keeping control in-house (Awan et al, 2021; Venkatraman and Fahd, 2016; Uchenna et al, 2015). Accelerated Adoption (2015–2020): In Nigerian businesses, the use of cloud-based ERP systems has grown a lot faster in the last few years. This rise has been caused by things like more people using the internet, better connections, and a move towards digital transformation (Tulinayo et al., 2018). Although the study by Tulinayo et al., (2018), it suggests that sub-Saharan Africa faces slow digital technology transitions, but effective exploitation can reduce the knowledge and economic gap between developed and developing nations. It states that technical and pedagogical efficacy are crucial in higher education institutions in these regions, in order to increase technology adoption and acceptance. The authors suggest that understanding user acceptability and usage of digital technologies is crucial in light of the Internet's rapid expansion and educational transformation. Organisations saw the benefits of cloud-based ERP systems, such as lower up-front costs, easier implementation, scalability, and the ability to view real-time data from anywhere (Liu et al, 2019). Cloud service providers and ERP companies also made changes to their products to fit the needs of Nigerian businesses (Uchenna et al, 2015).

According to Mallo and Ogwueleka (2019), the first cloud computing services have been available for less than a decade in Nigeria, but organisations ranging from tiny startups to multinational corporations, government agencies, and non-profits have already adopted the technology for a variety of reasons, including cost reduction, speed, global scale, increased productivity, and high reliability. Current trends and the future (after 2020): Businesses in Nigeria are likely to keep using cloud-based ERP systems more and more. Although authors like López and Ishizaka (2017), choosing a cloud-based enterprise resource planning (ERP) system can be difficult due to its novelty and unfamiliarity compared to conventional systems. It is difficult to choose a cloud ERP system due to the cloud provider market's lack of transparency. Companies frequently implement on-premises ERP, which demonstrates a lack of comprehension of cloud products and perceived security risks (Morawiec and Sołtysik-Piorunkiewicz, 2022).

The COVID-19 pandemic showed how important cloud technology is because companies needed solutions that could be used from anywhere (Alhomdy et al, 2021). As Nigeria's businesses work to become more digital, more companies are likely to look at cloud-based ERP systems as a smart investment. Also, cloud providers are improving their services to meet the needs of the Nigerian market. They are addressing concerns about data security, compliance, and local data residency standards (Chofreh et al, 2014). It is important to keep in mind that different businesses and organisations in Nigeria use cloud-based ERP systems in different ways. The speed of adoption can be affected by things like industry rules, government policies, cash limitations, the size of an organisation, and how complicated business processes are (Chen et al, 2014).

According to Salim et al (2015), using theoretical lenses such as the Technology Acceptance Model (TPM) and technology adoption stages, this study examines the adoption of cloud ERP systems by SMEs. In two phases, evaluation and trial, the relationship between a SME owner's attitude, subjective norms, and perceived behavioural control is examined. A significant positive relationship exists between attitude and subjective norms, while a negative relationship exists between perceived behavioural control and attitude. The study indicates that SMEs may be subject to external pressure to implement cloud ERP, but their adoption intent is high due to subjective norms.

### 2.7.5 Result and Interpretation

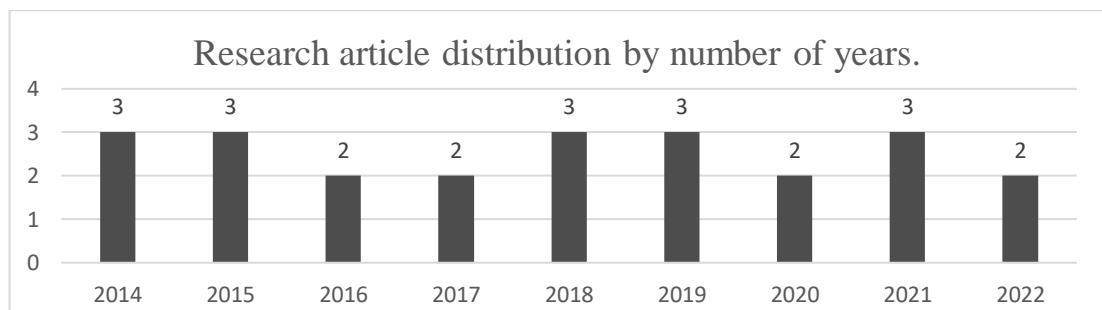


Figure 2.8: Chart showing the research article distribution by number of years.



The papers under scrutiny encompassed a broad spectrum of topics revolving around enterprise Enterprise Resource Planning (ERP) adoption, extending to the realm of cloud ERP adoption. They delved into the intricate dynamics of diverse enterprises, shedding light on their unique challenges and requirements in adopting ERP systems. The research captured not only the overarching trends but also the nuanced variations in ERP adoption practices across different types of enterprises. These papers provided invaluable insights into the evolving landscape of ERP implementation strategies and the evolving needs of enterprises in this domain.

The temporal distribution of the analysed papers, as depicted in Figure 2.8 above, spanned from 2014 to 2022, offering a comprehensive snapshot of ERP adoption literature over nearly a decade. The figure elucidates the distribution of publications across the years, showcasing the varying intensities of research activities during different time periods. For instance, it elucidates that three papers were published in 2014, followed by an equal number in 2015, and two in 2016, illustrating fluctuations in research output over time. This temporal analysis provides valuable context for understanding the evolution of scholarly interest and focus areas within the field of ERP adoption, highlighting potential shifts in research priorities and emerging trends.

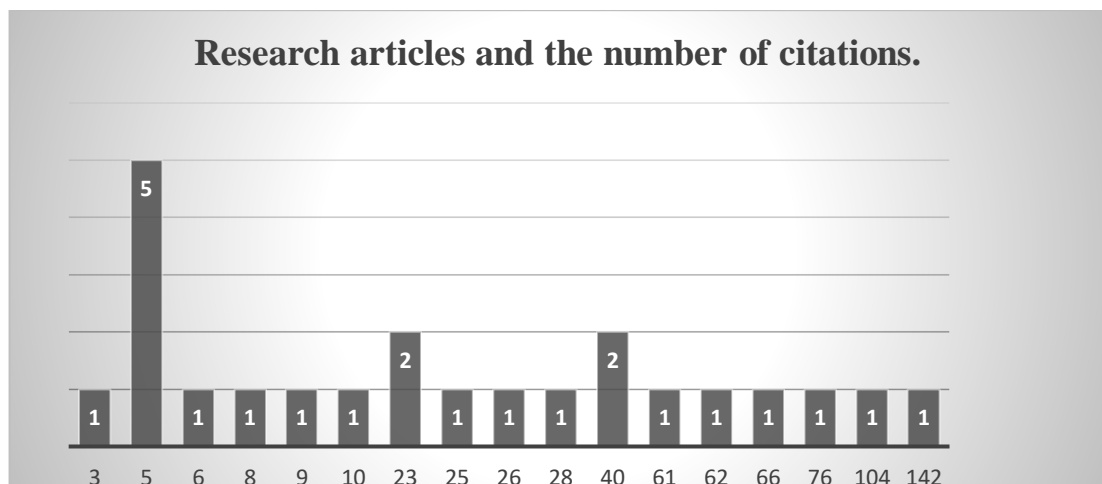


Figure 2.9: Chart showing the research articles and the number of citations

The Figure 2.9 above shows the number of citations of each of the papers we studied. The highest cited paper had 142 citations at the time of this analysis, five of the papers have been cited five times and just one of the papers had 3 citations but was included

in the analysis after it showed great content regarding Nigerian adoption of ERP systems.

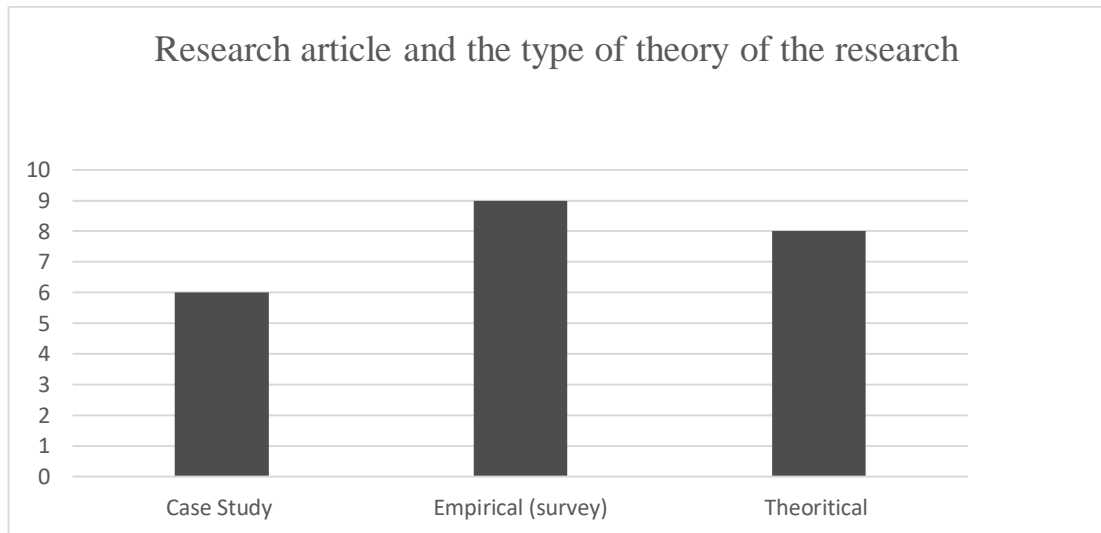


Figure 2.10: Chart showing the research article and the type of theory of the research

The Figure 2.10 above shows theoretical classification of the papers analysed. We looked at the papers considering the type of study done. From the chart above, six of the papers were case study, nine were empirical study involving a survey and eight were purely theoretical papers.

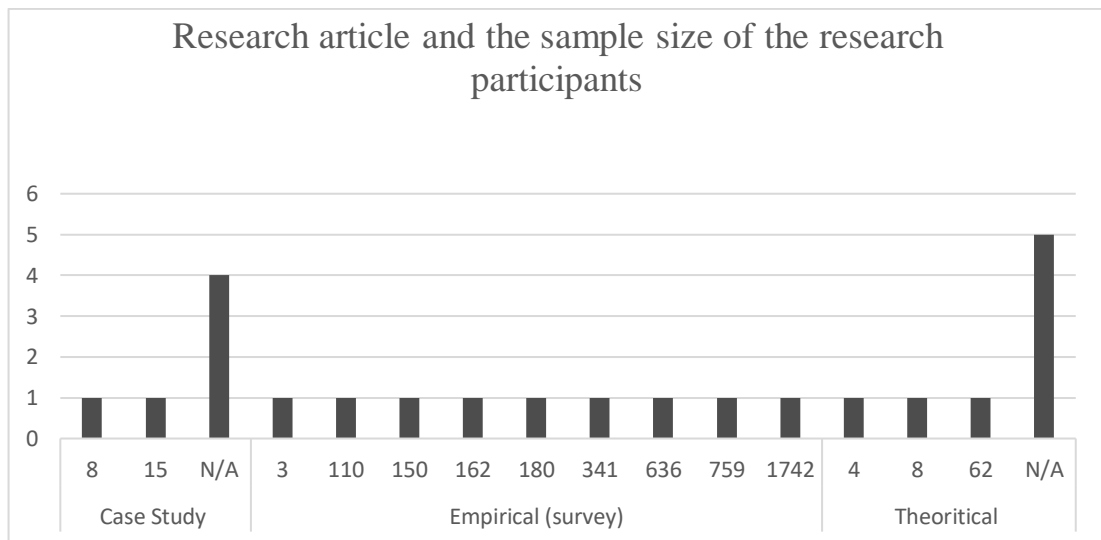


Figure 2.11: Chart showing the research article and the sample size of the research participants

We also looked at the sample size of the research participants in all the papers reviewed. Some of the papers had no research participants especially the theoretical

papers as seen in the Figure 2.11 above. One study had a large sample size of 1742 participants, and one paper had the least sample size of 3 participants for their study.

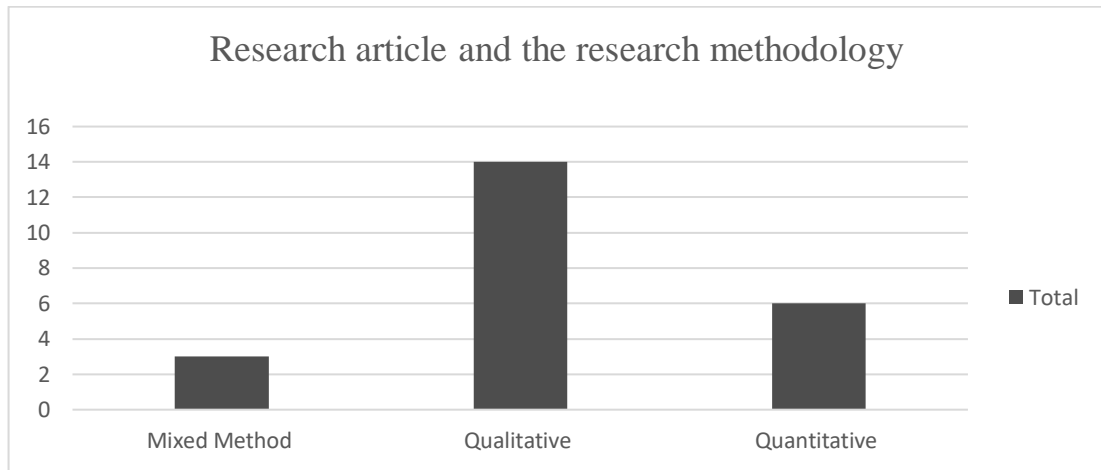


Figure 2.12: Chart showing the research article and the research methodology

The Figure 2.12 above shows the research methodology of the papers reviewed. About three papers used the mixed-method approach, fourteen papers used qualitative method and six papers used the quantitative methodology.

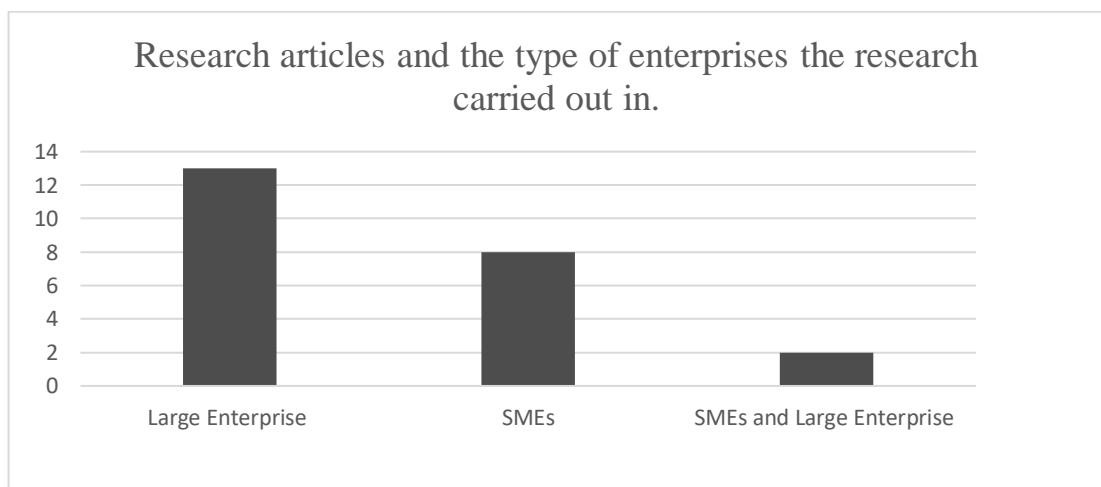


Figure 2.13: Chart showing the research articles and the type of enterprises the research carried out in

An interesting aspect of the papers reviewed was also our focus on the type of enterprise the paper is focusing on. For this we classified it large, SME or a mixture of both. Thirteen of the papers had their focus on large enterprises, eight of the papers had their focus on SMEs and two of the papers had their focus on both the large enterprises and the SMEs.

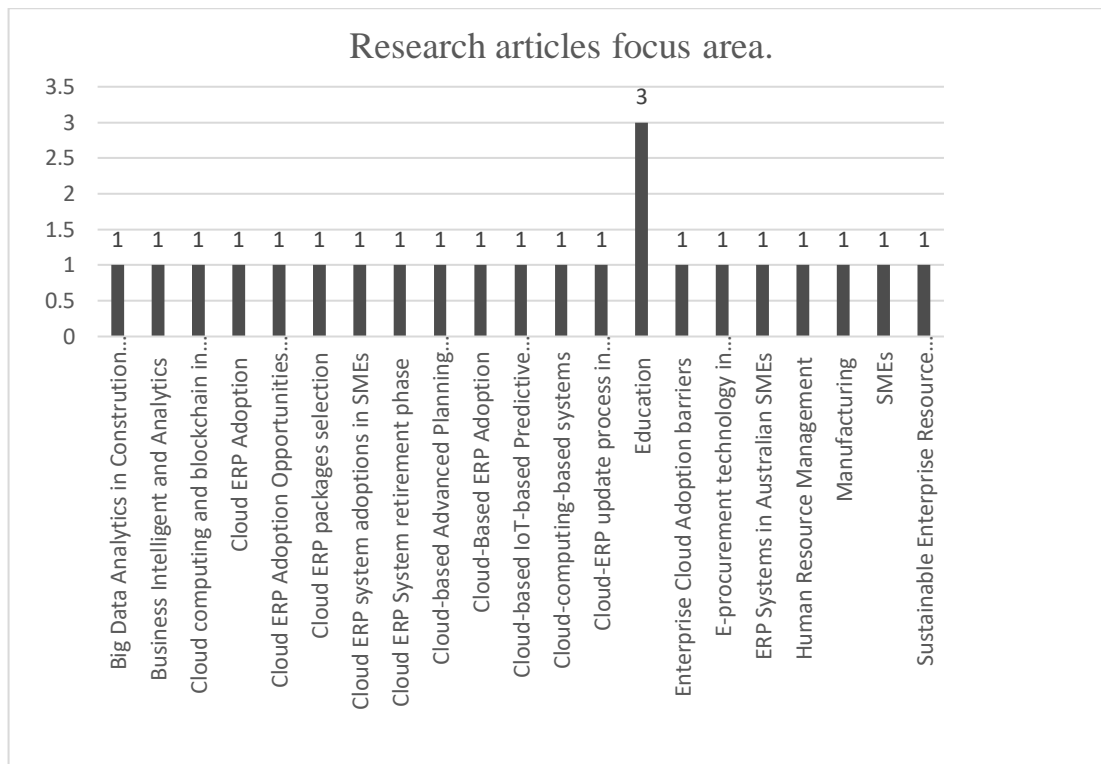


Figure 2.14: Chart showing the research articles narrowed focus area

Going a little more detail on the type of focus the papers reviewed had, the Figure 2.14 above shows a more detailed focus area of the papers reviewed. Interestingly, three of the papers had a narrowed focus on education, talking ERP in universities, it impacts on education with a learning environment. The rest of our papers have various narrowed focus although majority of the reviewed paper talked about clou-based ERP systems.

### 2.7.6 Discussion

SMEs in Nigeria can decide whether or not to use Enterprise Resource Planning (ERP) tools based on a number of factors, such as cost, resource limitations, perceived benefits, organisational size and complexity, and organisational size and complexity. Cost is a big factor in whether or not a company uses an ERP system (Karimanzira and Rauschenbach, 2019). Small and medium-sized businesses (SMEs) often don't have enough money to buy and implement ERP systems (Seethamraju, 2015). Resource limitations include a lack of technical knowledge and IT infrastructure. Perceived benefits include increased practical efficiency, streamlined processes, better decision-

making, and higher productivity (Seethamraju, 2015). The size and complexity of an organisation can affect whether or not it adopts ERP (Johansson et al, 2015). SMEs in Nigerian, I imagined will need to know how ERP systems can improve their business efficiency, streamline their processes, help them make better decisions, and make them more productive. SMEs with simpler structures and processes may choose ERP systems that are simpler or run in the cloud (Elbahri et al., 2019).

Needs that are specific to an industry: Each industry may have its own rules, laws, or compliance standards which needs to be taking into consideration before adopting ERP solutions. Organisational Readiness: It is important that the SMEs in Nigeria are ready to accept change and use new tools. We also note that CSP's reputation, dependability, and support services of ERP providers can affect how well they are used. Connectivity and Infrastructure: For an ERP system to be adopted successfully, it needs to have a reliable power source, internet connection, and IT infrastructure (Weng and Hung, 2014). These are not the only things to consider, and each SME's situation may be different. When a small or medium-sized business (SME) is thinking about getting an ERP system, it is important for them to take a close look at their unique needs, skills, and limitations.

The factors influencing the adoption of ERP systems in Nigerian enterprises, including both small and large businesses, may be similar to those influencing the adoption of ERP systems in Nigerian larger enterprises, but may also include additional factors. Cost is a major factor in the adoption of an ERP system, as it effects the initial investment, licencing fees, customization expenses, ongoing maintenance costs, and training expenses (Weng and Hung, 2014). Scalability and growth are also essential for SMEs in Nigeria, as the system must be able to accommodate expanding data volumes, user counts, and transactions as these enterprises grows. The ERP system should be able to accommodate organisational complexity and support multiple functional areas. Important as well are industry-specific requirements, as distinct industries in Nigeria may have specific regulatory compliance, reporting standards, or industry-specific needs.

For instance, several industry-specific factors may influence the adoption of ERP systems in Nigerian oil and gas organisations. Included among these are regulatory compliance, complex operations, health, safety, and environment (HSE) considerations, project management and cost control, and integration with project scheduling and monitoring tools (Tob-Ogu et al, 2018). Reporting, safety regulations, environmental standards, and tax regulations comprise regulatory compliance (Tob-Ogu et al, 2018). Considerations for health, safety, and the environment (HSE) include the management of HSE processes, incident reporting, risk assessments, safety protocols, and compliance monitoring.

Project management and cost control involve large-scale, financially intensive endeavours (Kiran and Reddy, 2019). Integration with project scheduling and monitoring tools can be essential to the success of project management (Kiran and Reddy, 2019). The supply chain network in the oil and gas industry in Nigeria is comprised of multiple suppliers, vendors, contractors, and logistics operations (Amue and Ozuru, 2014). ERP systems should have robust asset management modules to handle the lifecycle management of assets, support maintenance planning, tracking of maintenance activities, and predictive maintenance, and supply chain management capabilities to optimise procurement, inventory management, logistics, and supply chain management (Iluore et al, 2020). Additionally, we believe ERP systems should have data security and privacy measures to prevent unauthorised access to sensitive information and data breaches. ERP systems should also be able to integrate with IoT devices to facilitate real-time data exchange, remote monitoring, and predictive analytics for enhanced operational efficiency (Durana et al, 2021). In evaluating and selecting an ERP system for Nigerian oil and gas enterprises, these factors, along with the general factors mentioned previously, must be considered.

A number of human factors, including knowledge gap, awareness and comprehension, change management, skills and training, leadership and support, can influence the adoption of cloud-based ERP systems in Nigerian businesses (Mohammed et al, 2023).

Awareness and comprehension of cloud-based ERP systems among employees and stakeholders is crucial, and this factor can be addressed by providing comprehensive training and communication regarding the benefits, features, and security aspects of cloud-based ERP systems (Huang et al, 2021). We believe that strategies for change management that include employee engagement, employee security responsibility, communication, and training can help reduce resistance and foster acceptance among adopters' end-users in Nigeria. ERP adoption requires skills and training to be successful, and enterprise leadership needs to support it, in order to cultivate a positive environment for adoption. Training ensures that employees can maximise the system's capabilities, bridge the knowledge gap among adopting enterprise end-users and contribute to its successful implementation.

For encouraging employee buy-in and ensuring a smooth implementation of cloud-based ERP systems, support from managers and supervisors at various levels is crucial (Zhu and Spidal, 2015). To increase the adoption and acceptance of cloud-based ERP systems in Nigerian enterprises, it is necessary to address organisational culture, trust and security concerns, communication and collaboration among stakeholders where sharing security responsibility is encouraged, vendor selection and trust, and trust in the vendor's ability to deliver on promises and provide ongoing support. For businesses to feel confident in adopting their cloud-based ERP systems, they must have faith in the vendor's ability to fulfil promises and provide continuous support (Awan et al, 2021).

Finally, it is hoped that enterprises should evaluate ERP systems capable of meeting their needs. Adoption of an ERP system necessitates change management efforts to ensure a seamless transition and adopting enterprise end-user acceptability. Effective communication, training programmes, and involvement of key stakeholders throughout the adoption process can assist in overcoming resistance and increasing user acceptance. Considerations such as vendor reputation, experience, financial stability, and customer support services are essential for enterprise vendor selection and maintenance. In order to make informed decisions regarding ERP system adoption, it

is essential for businesses to conduct a thorough analysis of their unique needs, objectives, and obstacles.

## **2.8 A Narrative Literature Review on the Adopting End-User Security Responsibility in Ensuring Enterprise Data Security in Public Cloud.**

Adopting enterprise end-users are the individuals or groups within an enterprise responsible for entering data, operating processes, and generating reports during the ERP implementation process (Rajan and Baral, 2015). These end-users are crucial constituents because they have direct influence over the ERP system and are responsible for entering data, executing processes, and generating reports. Employees of Finance Department, Human Resources Department, Supply Chain/Logistics Department, Sales and Marketing Department, Production/Manufacturing Department, IT Department, and Executives and Management are typical examples of adopting enterprise end-users. Through seminars, training sessions, and user acceptance testing (UAT), these end-users must be involved early on in the process (Rajan and Baral, 2015). Their input, feedback, and buy-in are essential for the successful adoption of an ERP system and for ensuring that the system aligns with the organization's unique requirements and workflows (Alzahrani et al., 2021). By involving end-users from the outset, the implementation team can identify potential obstacles, customise the system to meet their needs, and ensure a more seamless transition to the new ERP environment (Abd Elmonem et al., 2016).

In a public cloud environment, adopting enterprise end-users play a crucial role in ensuring the security of their enterprise data (Rajan and Baral, 2015). While cloud service providers (CSPs) like AWS, Microsoft Azure, and Google Cloud take significant measures to provide a secure infrastructure, the responsibility for data security is shared between the CSP and the customer (adopting enterprise) (Eya and Weir, 2021). This shared responsibility model means that while the CSP is responsible for securing the underlying infrastructure, the customer is responsible for securing their data, applications, and user access. Below are some of the current security



responsibilities of adopting enterprise end-users in ensuring their enterprise data security in a public cloud environment:

### **2.8.1 Identity and Access Management (IAM)**

Identity and Access Management (IAM) is essential in a public cloud environment for ensuring the security and appropriate management of user identities and access to cloud resources. End-users are responsible for managing user accounts, employing strong passwords and Multi-Factor Authentication (MFA), understanding access permissions and roles, sharing resources with caution, monitoring and alerting, revoking access, adhering to the organization's policies, and implementing security awareness training (Indu et al., 2018). User account administration entails the creation, modification, and deactivation of accounts, as well as the maintenance of access levels based on roles and responsibilities (Younis et al., 2014). Strong passwords and multi-factor authentication are essential for user security. According to Younis et al., (2014) access permissions and duties should be assigned according to the principle of least privilege, and only authorised individuals should have access to shared resources.

Essential for monitoring cloud resources and preventing unauthorised access are monitoring and alerting (Indu et al., 2018). End users should configure alerts and notifications to be notified of suspicious logon attempts and changes to access permissions. It is necessary to revoke access privileges when employees or users no longer require access to particular resources. Compliance and governance are essential for IAM in the public cloud, and regular security awareness training is required to remain abreast of the latest security threats and best practises (Kumar and Goyal, 2019). Integrations with third parties should be circumspect and should not compromise the security of the IAM infrastructure. End-users should promptly report any suspicious activity or potential security incidents to IT or security personnel (Indu et al., 2018). End-users can maintain a strong security posture for IAM in the public cloud by adhering to these responsibilities, thereby reducing the risk of unauthorised access, data breaches, and other security incidents (Eya and Weir, 2021). Collaboration

with the organization's IT and security departments is crucial for implementing IAM best practises successfully (Indu et al., 2018).

### **2.8.2 Data Encryption**

End-users are responsible for encrypting sensitive data at rest and in transit (Nandakumar et al., 2021). Cloud providers typically offer encryption services, but the customer needs to implement and manage these encryption mechanisms for their data. End-users are responsible for encrypting sensitive data at rest and in transit in public cloud environments, as it is not the cloud service provider's obligation to ensure data security (Nandakumar et al., 2021). It is essential to encrypt sensitive data to protect it from unauthorised access and potential data breaches. End-users must ensure that data at rest is encrypted using encryption algorithms and keys (Melara et al., 2015). Data at rest refers to stored information that is not actively being used or transmitted. Data in transit refers to information that is moving between locations or being transmitted over networks (Shaikh and Sasikumar, 2015); end-users must encrypt it during transmission to prevent interception and unauthorised access. Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols are frequently employed to encrypt data in transit across the internet (Parmar and Gosai, 2015).

Although cloud service providers provide encryption capabilities and services, it is the responsibility of end users to configure and administer encryption for their own data; this is something our research is hoping to improve, more security responsibility for the end-users of the public cloud within the enterprises. The cloud provider may provide encryption tools and mechanisms, but it is up to the end users to implement encryption appropriately. Encrypting sensitive data at rest and in transit adds an additional layer of security to the cloud environment, even if cloud infrastructure or network security breaches occur. Encryption ensures that unauthorised parties cannot comprehend or use the information without the correct decryption keys, making it a fundamental aspect of data security in public cloud environments and a requirement for compliance with numerous data protection regulations and standards (Shaikh and Sasikumar, 2015).

### **2.8.3 Security Group and Firewall Configuration**

End-users must properly configure security groups, network access control lists (ACLs), and firewalls to control traffic flow to and from their cloud resources (Cavusoglu et al., 2009). In cloud computing, end-users are the individuals and organisations responsible for hosting and administering their applications, data, and resources (Van Niekerk and Jacobs, 2013). To control traffic flow to and from their cloud resources, end-users within the enterprise must configure security groups, network access control lists (ACLs), and firewalls (Shatat and Shatat, 2021). Security groups are virtual firewalls that regulate the incoming and outgoing traffic of virtual workstations within a particular network (Bellovin and Cheswick, 1994). By defining criteria through classification, end-users can ensure that only authorised traffic is allowed and that any malicious or unwanted traffic is blocked.

Network Access Control Lists (ACLs) operate at the subnet level, allowing cloud network end users within the enterprise to control traffic between subnets (Qian et al., 2001). By specifying which connections are permitted or denied, ACLs enable users to enforce security policies and restrict unauthorized access within their cloud infrastructure. End-users can permit or deny specific categories of traffic between subnets by defining ACL rules based on source and destination IP addresses and ports (Qian et al., 2001). Firewalls are an essential component of network security that safeguard cloud resources from unauthorised access and cyber threats (Cavusoglu et al., 2009).

End-users can ensure enhanced security, compliance with regulatory requirements, traffic control, and isolation by taking responsibility for the proper configuration of these security measures. It is essential to observe, however, that cloud service providers typically employ a model of shared security responsibility. End-users are responsible for securing their applications, data, and access to cloud-based resources. Therefore, end users must proactively implement and maintain these security measures

to effectively defend their cloud assets. This helps protect against unauthorized access and network-based attacks.

#### **2.8.4 Patch Management**

End users are responsible for maintaining their cloud resources and applications up-to-date with the most recent security patches and updates (Sundareswaran et al., 2012). This includes maintaining and updating the cloud infrastructure's software, applications, and configurations. Applications are software programmes, web applications, and other services that operate on top of cloud computing resources (Zhou et al., 2010). Software developers and cloud service providers release security patches and updates to address known security vulnerabilities and flaws in their products. Protect against the exploitation of known vulnerabilities by maintaining systems and software up-to-date with the most recent security patches. End-users must remain abreast of the most recent security updates and patches provided by their cloud service provider in order to minimise the risk of security breaches and safeguard their data from potential threats (Sundareswaran et al., 2012). Software not being kept up-to-date may expose systems to known vulnerabilities that attackers may exploit, resulting in compromised security and possible data intrusions (Gascon et al., 2011). In order to maintain a secure cloud environment, proactive and regular patch management is essential.

#### **2.8.5 Data Backup and Disaster Recovery**

Cloud service providers offer robust infrastructure and services for data redundancy and backup (Rasheed, 2014), but the CSP and end-user must share responsibility for administering and securing data (Eya and Weir, 2021). The provider is responsible for the security of the cloud infrastructure, while the end user must secure and manage their data and applications (Sundareswaran et al., 2012). Data availability and business continuity are crucial for cloud service providers, as they cannot prevent data loss entirely or guarantee continuous service access in all circumstances (Tahboub and Saleh, 2014). In uncommon instances, such as extensive outages or data centre failures, cloud services may have a temporary effect on end-user enterprises (Taylor, 2021).

End-users must develop and implement their own data backup and disaster recovery strategies, tailored to their specific requirements and risk tolerance, in order to mitigate risks associated with potential cloud service disruptions, data loss, and other unforeseen incidents (Taylor, 2021). This includes regular data backups to alternate locations, maintaining copies of critical data on-premises, and the use of third-party backup and recovery solutions.

### **2.8.6 Monitoring and Logging**

End-users should be responsible for the security of their data and applications in public cloud environments by implementing monitoring and archiving solutions to detect and respond to security incidents and potential threats in order to protect their data and applications (Tabrizchi and Rafsanjani, 2020; Sundareswaran et al., 2012). These solutions gather data and metrics from a variety of cloud resources, including virtual machines, databases, storage, networking, and applications (Tabrizchi and Rafsanjani, 2020). Through monitoring and logging solutions, security incidents such as unauthorised access attempts, data breaches, malware infections, and denial-of-service attacks can be detected and countered (Razzaq et al., 2013). It is possible to identify potential hazards, such as internal or external actions or events, prior to their escalation into actual security incidents. Regular surveillance and logging can assist in identifying patterns and anomalies that may indicate threats before they become actual security incidents (Choudhary et al., 2018). End-users should be responsible for the security of their data and applications in public cloud environments, and implementing monitoring and logging solutions can assist them in achieving faster response times, early detection of suspicious activities, and an improved overall security posture in this dynamic and complex environment.

### **2.8.7 Compliance and Regulatory Requirements**

End-users are responsible for comprehending industry-specific compliance standards and regulatory requirements pertinent to their data, applications and industry, and for adhering to them (Kundur, 2023). These standards are intended to resolve specific risks and obstacles in various industries, including healthcare, finance, and regulatory

requirements. End-users must have a thorough understanding of these standards, which includes knowledge of the applicable rules, guidelines, and laws for their business, data, and geographic regions.

Regulatory requirements are government-issued laws, regulations, and directives that govern how businesses and organisations operate within a given jurisdiction (Charles and Le Billon, 2021). Typically, these regulations emphasise the protection of consumer rights, data privacy, security, and equitable business practises. Adopting enterprise end-users are responsible for protecting data, assuring data security and privacy, and preserving data integrity (Sundareswaran et al., 2012). Additionally, they must ensure that the applications they use to manage data or provide services comply with applicable regulations. End-users are responsible for holding accountable those with direct control over data and applications for their actions. Compliance requirements and regulatory standards safeguard consumers, individuals, and businesses while preserving the integrity and security of the data ecosystem (Kumar and Goyal, 2019). Failure to comply can result in legal consequences, fines, reputational harm, and a loss of customer and partner confidence. Therefore, end-users must be proactive in educating themselves on pertinent regulations and implementing compliance measures.

### **2.8.8 Employee Training and Awareness**

It is imperative to provide comprehensive training to adopting enterprise end-users regarding cloud security best practises, potential hazards, and appropriate protocols for managing data in order to mitigate the occurrence of human errors and insider threats (Mather, 2009; Kumar and Goyal, 2019). The aforementioned practises encompass a range of facets, including but not limited to access control, data encryption, network security, authentication systems, regular backups, and vulnerability management. These rules facilitate end-users' comprehension of the secure and responsible utilisation of cloud services within their enterprise. Public cloud environments present various potential dangers, such as the compromise of sensitive data, unauthorised entry into the system, the inadvertent loss of data, and interruptions

in service provision (Barona and Anita, 2017). It is imperative for adopting enterprise end-users to possess an understanding of these dangers in order to exercise vigilance and implement suitable measures to prevent security mishaps.

The implementation of proper protocols for data management encompasses several aspects such as data storage, access, processing, and transmission (Chen and Zhao, 2012). These protocols encompass guidelines for data classification and the implementation of suitable controls. Providing adopting enterprise end-users with comprehensive training on data handling processes facilitates responsible management of sensitive information, hence mitigating the potential risks associated with data leaks or exposures (Mather et al, 2009; Sundareswaran et al., 2012).

The prevention of human errors is of utmost importance, as adopting enterprise end-users have the potential to inadvertently commit errors that can compromise the security of cloud systems (Ifinedo et al., 2019). The implementation of comprehensive education and training programmes can equip adopting enterprise end-users with the necessary knowledge and skills to identify potential risks and embrace more secure practises. This, in turn, can effectively mitigate the occurrence of security events resulting from human errors. Insider threats, originating internally within an enterprise, can be attributed to personnel such as employees, contractors, or others with authorised access to the enterprise's systems (Nurse et al., 2014). The dissemination of knowledge on cloud security to employees can foster comprehension of the significance of safeguarding sensitive data and the potential ramifications associated with insider threats (Kumar and Goyal, 2019). This, in turn, can promote a culture of heightened awareness and accountability towards security.

The cultivation of cultural awareness within cloud security education is of utmost importance, as it facilitates the development of a security-conscious culture among enterprise personnel (Khando et al., 2021). Through comprehension of the potential dangers and optimal methodologies, adopting enterprise end-users can assume an engaged role in protecting the assets and data of the organisation. This entails reporting

any suspicious activity, exercising prudence in their actions, and fostering effective collaboration with IT or security teams to effectively mitigate potential security concerns. In brief, the dissemination of knowledge to employees on optimal cloud security protocols, potential vulnerabilities, and appropriate protocols for managing data is vital in cultivating a workforce that prioritises security measures and minimising the likelihood of inadvertent mistakes and internal threats. This training programme provides end-users with the necessary knowledge and abilities to make well-informed decisions, responsibly manage data, and contribute to the overall security posture of the enterprise within cloud environments.

### **2.8.9 Cloud Service Provider Selection**

Adopting enterprise end-users share in the responsibility of selecting a reputable and trustworthy cloud service provider to ensure the security, confidentiality, and integrity of their enterprise data (El-Gazzar, 2014). Reputable providers invest in security measures, adhere to industry standards, undergo certifications and audits, ensure data redundancy and disaster recovery, have transparent privacy policies, provide excellent customer support, have a solid track record, and offer flexible plans to meet the needs of end users (El-Gazzar, 2014). End-users can make an informed decision that aligns with their security requirements and protects their valuable data by thoroughly considering these factors. Enterprises can protect their valuable data and maintain a competitive advantage in the cloud computing market by conducting research, comparing options, and making the best decision.

### **2.8.10 Incident Response**

Having a well-defined incident response plan is essential to effectively address security incidents and minimize potential damage (Mitropoulos et al., 2006). Enterprise end-users must have a well-defined incident response plan to effectively address security incidents and minimise potential data loss in the public cloud. This plan should provide clear guidelines for detecting and responding to security incidents, mitigating their impact, delineating specific roles and responsibilities, implementing threat mitigation strategies, adhering to compliance requirements, and continuously



learning and improving (Mitropoulos et al., 2006). It should address their cloud-specific challenges, encourages collaboration and communication between teams, ensures preparedness, and fosters trust by demonstrating a proactive security approach. An enterprise's cybersecurity strategy must include a well-defined incident response plan, especially in the public cloud (Razzaq et al., 2013). It allows for prompt and coordinates action, reduces the impact of security incidents, and ensures regulatory compliance. By understanding and fulfilling these security responsibilities discussed above, adopting enterprise end-users can significantly enhance their data security in a public cloud environment and reduce the risk of data breaches and cyber-attacks. Regular security assessments and audits can also help identify potential vulnerabilities and areas for improvement.

## **2.9 Summary of Chapter 2**

This chapter provides an overview of the various concepts related to cloud adoption by enterprises in section 2.4.1 An enterprise can be classified according to a variety of factors, including the number of employees, the legal entity type, the nature of the legal subject, and the type of operation. Data is viewed as a collection of quantitative or qualitative variables that can be combined to form a single piece of information in any given situation. Data security refers to the process of ensuring that digital data maintains acceptable levels of confidentiality, integrity, and availability. According to Liu, et al., 2010 a protected corporate network whose security is ensured through the use of virtual private network (VPN) technology, a server, and an access list may be the answer to enterprise data security in cloud. Another article proposed a data-sharing scheme based on binary parsing that enhances data confidentiality and the data owner's anonymity. Information security is the process of accounting for the events and actions of end-users while interacting with a dataset in a system, ensuring that information is used transparently. By 2012, Rowsell-Jones and Gomolski predict that 80 % of Fortune 1000 companies will be utilizing some form of cloud computing. Cloud computing enables the efficient delivery of on-demand services to end-users via the internet (Schaffer, et al., 2009). Cloud computing may be the answer to Africa's small and medium-sized businesses (SMEs) challenges (Mohlameane and Ruxwana, 2013).

Confidentiality, integrity and availability of data (i.e., the CIA properties) are considered in an enterprise context in section 2.3. Cloud service providers are solely responsible for data security in the SaaS model. This presents a significant difficulty because the service user relinquishes control over their data. Cloud computing enables an ERP software application, such as big data analytics software, to have a greater storage requirement. Examining the various Cloud Computing Security Models were identified, with a particular emphasis on the model that addresses the data security challenges associated with cloud-based ERP systems. It is critical to understand the layer dependency of various cloud service models to properly analyze cloud computing's security risks. Human factor analysis studies human error and its potential for exposing the system. Cloud data security is a continuous process that requires ongoing investment in technology and user education (Mircea, 2012).

## Chapter 3. Research Methodology

A research methodology is a systematic approach to researching a subject; it includes the theoretical foundation of the study as well as data collection, analysis, and interpretation. It includes the strategy, plan of action, process, or design that underpins the selection and use of specific resources. It also specifies and develops the actions required to complete the task. In the previous chapter two, we examined the theoretical foundation for this research in sections 2.5, section 2.6, section 2.7, and section 2.8, as well as relevant scholarly literature regarding our research assumptions in Chapter 1 section 1.6 and our research questions in Chapter 1 section 1.5. This Chapter three describes the research methods employed in this study in great depth. There are numerous methods for collecting and analysing data, but they are distinct from research methodologies, which are the general procedures followed when conducting research.

Following the introduction of the study question and hypotheses, this chapter examines research methodological concerns such as describing philosophical frameworks, research design and strategy in section 3.2, and research methodologies that include quantitative and qualitative (mixed method) techniques. The sample of participants as well as the instruments utilised to collect data are also described in section 3.3. This section of the thesis outlines how the research data was collected for the analysis in the subsequent section and how the survey research tool was designed. The chapter's final sections address questions of validity, reliability, and ethics in section 3.4, the ethical consideration was outlined in section 3.5, and it concludes with a summary of the important points in section 3.6.

Understanding Research Methodology: Eldabi et al. (2002) emphasize the importance of a clearly defined research methodology based on scientific principles for conducting any study. Hussey and Hussey (1997) classify different types of studies into four

categories: the study's objective, the strategy used to collect and evaluate data, the narrowing of the focus, and the purpose of the research. The researcher's research philosophy or paradigm should guide their decision on the research method, as it should be based on scientific principles and the researcher's philosophy or paradigm (Creswell, 2003).

The purpose of this study is to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. This study goal is accomplished by analysing the present status of cloud computing security models. It also examines the essential human factor elements that influence the adoption of a cloud-based ERP systems in such organisations. We examined the relationship between the role of adopting enterprise end-users and the cloud security of their enterprise data. This gave us a starting point for comprehending the relationship between these two concepts. The objective of the study is not to discover the absolute truth or effect change, as that is beyond the scope of the researcher's training. However, the researcher does make some recommendations concerning the research topic. For instance, we propose a framework for a company to implement a cloud-based ERP system while taking the security responsibilities of the adopting end users into account.

The suitable research approach for a research project is determined by the nature of the investigation and the purpose of the researcher. The researcher selected to look at the research topic from the following perspective in this study.

- A review of relevant work that has been consolidated in order to identify the need for adopter end-user security responsibility in ensuring enterprise data security in public cloud, and to provide knowledge and appropriate methodologies. The aim of the study is to promote discussion of the research subject and help identify key areas for improvement within the cyber security field putting into consideration the role of human factor.

- An integrated mixed-methods approach (e.g., qualitative and quantitative) was used to analyse the degree of the need for adopter end-user security responsibility in ensuring enterprise data security in public cloud within SMEs in Nigeria and the degree of acceptability of the attributes of the proposed implementation approach. A quantitative approach was justified by the necessity for a large survey questionnaire with hypothesis testing. The study was based on the opinions and perceptions of 43 senior security and IT managers.
- The third perspective is the researcher's personal observations and professional experiences.

Any investigation must be backed up by a set of underlying philosophic assumptions. It is expected that a research assumption will be created and put to the test utilising certain measurement techniques (Bryman, 2012). Another idea is that certain aspects of people and social structures are talked about in a sensitive way (Creswell, 2012). These presumptions regarding how a subject is investigated are known as epistemological assumptions or paradigms (Creswell, 2012). Epistemology is the study and explanation of how we know what we know (Crotty, 2003). Furthermore, epistemology is concerned with providing a philosophical foundation for determining what types of knowledge are possible and how to ensure that they are both adequate and legitimate.

Our epistemological position is Post-positivism: This position acknowledges the limitations of pure positivism and emphasizes the role of values, assumptions, and subjectivity in the research process. Researchers influenced by post-positivism often employ mixed methods, combining quantitative and qualitative approaches to gain a more comprehensive understanding of a phenomenon. Other paradigm can be seen in Table 3.1 below, where pragmatists argue that academics in social science should stop addressing questions about reality and natural laws (Kaushik and Walsh, 2019). The focus should be on applications and issue solutions; the problem is more essential than

the methodology. As a result, researchers should employ all possible methodologies to comprehend the problem and identify answers.

Understanding research principles can assist researchers clarify study designs and suggest ways to apply them to various fields of knowledge. It can also help academics identify and build new sorts of design that are outside of their experience. It may also demonstrate how to adjust a study design to the limits of various subject matter. It is also possible that it will explain how to adjust a study plan in order to accommodate the limitations of the various disciplines of knowledge (Smith et al. (2013). Brennan et al. (2011) argue that the classification of social research processes is based on four main factors: epistemology, theoretical perspective, methodology, and methodologies. Creswell (2009) says that a study approach's philosophical assumptions give rise to four different worldviews.

Researchers want to know what to investigate and how to do it in the best way for their needs and goals. Bryman et al. (2008) think that a paradigm could have more than the three sets of assumptions listed. Some of these are post-positivism, constructivism, advocacy and participatory research, and pragmatism. Pragmatists believe they can use any method, whether it's quantitative, qualitative, or a combination of the two.

Evaluation research is about the goal of the research, not the method. It tries to reach a certain goal rather than a certain method. It just means that the goal of the research is to judge a certain idea. Even though the methods used to evaluate a concept are similar to traditional research methods, such as quantitative or qualitative, evaluation research is very different in that it requires the researcher to have certain skills, such as management skills, interpersonal skills, team skills, and a close focus on the things being evaluated (organizational skills). The goal of incorporating evaluating techniques is to get useful information from the people who took part in the study and give the researcher valuable insights. Evaluations help the researcher learn more about

Table 3.1: An Overview of Paradigm. By Salma Patel (2015)

<b>Paradigm</b>	<b>Positivism</b>	<b>Constructivist /Interpretive</b>	<b>Pragmatism</b>
<b>Ontology</b> What is reality?	There is a single reality or truth (more realist).	There is no single reality or truth. Reality is created by individuals in groups( less realist).	Reality is constantly renegotiated, debated, interpreted in light of its usefulness in new unpredictable situations
<b>Epistemology</b> How can I know reality?	Reality can be measured and hence the focus is on reliable and valid tools to obtain that.	Therefore, reality needs to be interpreted. It is used to discover the underlying meaning of events and activities.	The best method is one that solves problems. Finding out is the means, change is the underlying aim.
<b>Theoretical Perspective</b> Which approach do you use to know something?	Positivism Post-positivism	Interpretivism (reality needs to be interpreted) <ul style="list-style-type: none"> <li>• Phenomenology</li> <li>• Symbolic interactionism</li> <li>• Hermeneutics</li> </ul> Critical Inquiry Feminism	Deweyan pragmatism Research through design
<b>Methodology</b> How do you go about finding out?	Experimental research Survey research	Ethnography Grounded Theory Phenomenological research Heuristic inquiry Action Research Discourse Analysis Feminist Standpoint research etc	Mixed methods Design-based research Action research
<b>Method</b> What techniques do you use to find out?	Usually quantitative, could include: Sampling Measurement and scaling Statistical analysis Questionnaire Focus group Interview	Usually qualitative, could include: Qualitative interview Observation Participant Non participant Case study Narrative Theme identification ect.	Combination of any of the above and more, such as data mining expert review, usability testing, physical prototype

a subject, improve practise, measure effects, and build capacity by giving them development points. Some people might think that evaluation is just getting organised feedback on any subject that interests them. Powell (2006) says that evaluation research includes planning, doing the research, and analysing the results. This includes using techniques for collecting data and statistical methods.

Having a certain paradigm involves "seeing the world in a specific way". According to Creswell (2009, p 7) a research paradigm is a collection of interconnected beliefs and assumptions that determine how researchers approach and carry out their research. It acts as a framework that influences study design, methodology, and outcomes interpretation. study paradigms serve as the intellectual and methodological framework for study in a specific topic or discipline. According to Creswell (2009, p 7), pragmatism focuses on how to comprehend the research topic and frees the researcher from being tied to a single approach or technique. As such, a mixed-methods strategy with pragmatic viewpoint philosophical assumptions was the best way to accomplish the study's major purpose and objectives. This is because pragmatism is characterized by an approach that values both quantitative and qualitative methods, with an emphasis on practicality and problem-solving. Researchers in this paradigm seek to use the most appropriate methods for the research question at hand.

To offer a wide foundation for the inquiry, a mixed method, also known as deductive/inductive (Creswell, 2009), design with a pragmatic viewpoint was used. Mixed approach is the most effective method to use when evaluating models. This is because research conducted using mixed methods involves both quantitative and qualitative methods. Consequently, the utilisation of mixed techniques will make it possible for us to acquire both quantitative and qualitative knowledge regarding our research issue (such as the percentage of our study participants who agree with us) (the in-depth understanding of the reasons and justification for the responses they provide). For the purpose of this research, which aimed to evaluate the model's underlying principles, and gaining an understanding of the end-user security responsibility in their enterprise data in cloud, the mixed approach proved to be the strategy that was most suitable. We will be able to identify the percentage of people who participated in the research who agreed with the model principles as well as the reasoning behind their agreement with the model's proposed characteristics. This will feed into the conclusions and the proposed implementation approach. Mixed-methods approach was chosen to offer a comprehensive and holistic perspective of the model's underlying principles and an understanding of the end-user security responsibility in their



enterprise data in cloud, while also allowing detected concerns to be investigated in depth. To offer a wide foundation for the inquiry, a design with a pragmatic viewpoint was used. According to Creswell (2009), pragmatism "opens the door to numerous methods, distinct worldviews, and different assumptions".

The next section addresses the main research question and sub questions and the related hypotheses.

### **3.1 Research Questions and Research Assumptions**

In order to fulfil the research objectives and provide an answer to the following research question and its sub-questions, this study makes use of a number of research assumptions which detailed explanation can be found in section 1.6 of Chapter 1 and section 3.1.2 of Chapter 3.

#### **3.1.1. Research Questions**

When deciding on a research approach, one of the most significant skills to possess is the ability to formulate appropriate research questions for an investigation. This study aims to answer the following major research main (RM-Question) and sub questions (RS-Questions) that have arisen from the preliminary related work review. These help to focus the research and accomplish its purpose.

**RM-Question:** How important is adopter end-user security responsibility in ensuring enterprise data security in public cloud? Also to validate or refute the position taken in the proposed implementation approach for a cloud-based ERP systems within an enterprise.

The above main research question was backed up by the following sub questions which detailed discussion is found in the below sections 3.1.1.1 to 3.1.1.5, each of which has a number of research assumptions that are talked about in section 1.6 in Chapter 1 and section 6.2 in Chapter 6 of this thesis.

**RQ1:** How important is end-user access control in ensuring enterprise data security in the cloud?

**RQ2:** How important is shared security responsibility between a CSP and an enterprise end-user in ensuring enterprise dataset security in a cloud-based ERP system?

**RQ3:** To what extent should enterprise dataset classification form part of a cloud-based ERP implementation to promote enterprise data security in the cloud?

**RQ4:** To what extent can enterprise database fragmentation in the cloud improve the enterprise data security of a cloud-based ERP software system?

**RQ5:** To what extent can cloud computing have an impact on enterprise system data security

### **3.1.1.1 RQ1: How important is end-user access control in ensuring enterprise data security in the public cloud-based ERP?**

Controlling end-user access is essential for securing enterprise data in public cloud ERP systems (Bradford, 2014; Eya and Weir, 2021). It safeguards sensitive data, prevents unauthorised access, enforces least privilege, and ensures that only authorised users have access to sensitive data (Bradford, 2014; Eya and Weir, 2021). This reduces the likelihood of unauthorised disclosure and data breaches. Public cloud-based ERPs are susceptible to cyberattacks; therefore, adequate access controls prevent unauthorised users from gaining access to the system (Alzahrani et al., 2021). Multi-factor authentication (MFA) and other access control mechanisms help verify user identity and limit the exposure of sensitive data (Anakath et al., 2019). Monitoring user activity is necessary for detecting and investigating suspicious behaviour, as well as identifying potential security hazards or policy violations (Tabrizchi and Rafsanjani, 2020).

Compliance requirements are crucial for a variety of industries, and robust access controls are required to meet these requirements (Kunduru, 2023). Insider threat mitigation is another crucial aspect of data security (Mather, 2009; Kumar and Goyal, 2019). Access controls reduce the likelihood that malicious insiders will abuse their privileges to cause damage to the organisation or its data. Separating data is another crucial aspect of data security (Melara et al., 2015). Access controls enable

organisations to segregate data according to user roles or departments, thereby reducing the risk of accidental data exposure or unauthorised access. Access controls allow for centralised administration of user permissions, and continuous adaptation is required to maintain an appropriate level of security over time. Hence, we believe that end-user access control is essential for sustaining data security in a public cloud ERP system. By instituting robust access controls, organisations can protect sensitive data, prevent unauthorised access, monitor user activities, comply with regulatory requirements, and mitigate risks posed by both external and internal threats. Therefore, our first research question seeks to understand how important an end-user access control is, at ensuring enterprise data security in the public cloud-based ERP from the perspective of our research participants, this will give us a clue of what is currently obtainable from the industries and a better understanding of our viewpoint.

**3.1.1.2 RQ2: How important is shared security responsibility between a CSP and an adopting enterprise end-user in ensuring enterprise dataset security in cloud-based ERP system.**

The shared security responsibility model is a collaborative approach between the Cloud Service Provider (CSP) and the adopting enterprise end-users, focusing on ensuring the security of data and resources in cloud-based services. This model is commonly applied in various cloud service arrangements, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The CSP is responsible for securing the underlying cloud infrastructure, including data centers, servers, networking equipment, and virtualization technology (Younis et al., 2014; Sehgal et al., 2020; Khan and Ullah, 2016). The CSP must ensure physical security measures are in place to protect their data centers from unauthorized access and environmental threats (Khan and Ullah, 2016). The network infrastructure, including firewalls, load balancers, and other security measures, is also secured by the CSP. The adopting enterprise end-user is responsible for data security, identity and access management (IAM), application security, compliance with industry-specific regulations, and security monitoring and incident response (Sundareswaran et al., 2012). The extent of responsibility for each party can vary depending on the cloud

service model, with the CSP typically taking on more responsibilities for managing the underlying infrastructure and platform, while the adopting enterprise focuses on securing its data and configuring the application (Subashini and Kavitha, 2011). The shared security responsibility model promotes cooperation between the CSP and the adopting enterprise, creating a more secure cloud environment and emphasizing the importance of clear communication and understanding of roles to ensure comprehensive protection against various security threats.

The model of shared security responsibility between a Cloud Service Provider (CSP) and adopting enterprise end-users offers numerous benefits, thereby augmenting the overall security posture of cloud-based ERPs (Singh et al., 2016; Subashini and Kavitha, 2011). Key benefits include a comprehensive security approach, specialised expertise, cost-effectiveness, simpler compliance management, quicker deployment and scalability, reduced operational complexity, shared learning and continuous improvement, redundancy and disaster recovery features, and increased transparency (Ahmed and Zakariae, 2018). The adopting enterprise can concentrate on securing its data and applications due to the CSP's expertise in securing cloud infrastructure, while the CSP manages the underlying cloud infrastructure, including physical, network, and host security. This collaboration promotes shared learning and continuous development, to the advantage of all platform users (Ahmed and Zakariae, 2018). In addition, the shared responsibility will protect vital data from data loss and service disruptions by ensuring data availability and integrity. Overall, the shared security responsibility model encourages collaboration and transparency, allowing the CSP and adopting enterprise to jointly resolve security challenges, stay ahead of emerging threats, and create a more resilient and secure cloud environment for their data and applications.

The model of shared security responsibility between Cloud Service Providers (CSPs) and adopting enterprise end-users has a number of advantages, but also potential disadvantages. These include responsibility ambiguity, lack of control, reliance on the CSP's security, compliance challenges, integration complexity, varying security

postures, contractual and legal issues, limited customization, and operational dependencies (Chauhan and Shiaeles, 2023). Responsibility ambiguity can lead to security breaches or overlaps, resulting in vulnerabilities if critical aspects are not addressed adequately. If the CSP fails to meet expectations or a security incident occurs, the adopting enterprise may have limited control over the CSP's security measures, leaving them vulnerable. In addition, the adopting enterprise may experience security incidents or breaches, which may affect their data and applications in public cloud.

Compliance issues can arise when dealing with the security practises of multiple parties, as assuring compliance becomes more difficult (Herath and Rao, 2009). Integration complexity can result in additional costs and potential failure points (Madni and Sievers, 2014). When negotiating and defining security responsibilities in service-level agreements and contracts, legal and contractual issues can arise (Karadsheh, 2012). There may be restrictions on the adopting enterprise's ability to tailor security measures to specific business or industry demands. There may also be operational dependencies, as disruptions or outages on the provider's end may affect the enterprise's business continuity. Despite these obstacles, the shared security responsibility model continues to be widely adopted and viewed as beneficial when implemented properly. Clear communication, transparency, and cooperation between the cloud service provider (CSP) and the adopting enterprise are essential for addressing these challenges and enhancing the cloud environment's overall security posture. Hence our research seeks to understand our participants viewpoint on the important of shared security responsibility between a CSP and an adopting enterprise end-user in ensuring enterprise dataset security in cloud-based ERP system.

### **3.1.1.3 RQ3: To what extent should enterprises dataset classification form part of a cloud-based ERP implementation to promote enterprise data security in the cloud?**

Using machine learning and artificial intelligence techniques, enterprise dataset classification is the process of categorising and organising large volumes of data within

an enterprise or organisation (Suthaharan, 2016). The primary objective is to automatically designate labels or categories to various data points, making them easier to manage, search, retrieve, and analyse. Data collection, data preprocessing, labelling, feature extraction, model selection, model training, evaluation, refining, deployment, and maintenance and monitoring are essential steps in enterprise dataset classification (Biswas et al., 2022). Data collection entails gathering information from diverse sources, including text documents, images, videos, consumer records, and financial data. Data preprocessing includes cleansing, transforming, labelling, extracting pertinent features, and choosing an appropriate classification algorithm based on the data and the problem. Classification of enterprise datasets has numerous applications, such as document categorization, sentiment analysis, fraud detection, and customer segmentation, enabling organisations to manage and utilise their data assets more effectively, thereby facilitating better decisions and insights (Wankhade et al., 2022).

Enterprise dataset classification offers numerous benefits for data management, analysis, and decision-making within an enterprise. It streamlines data management, enhances search and retrieval, automates data processing, provides insights and analytics, aids decision-making, and helps understand customer preferences and behaviours. It also ensures regulatory compliance, predictive analysis, effective collaboration, resource optimization, reduced error and uncertainty, scalability, competitive advantage, and automation of repetitive tasks (Ng et al., 2021). By utilizing well-organized data and insights, enterprises can gain a competitive edge and free up human resources for more value-added tasks. Overall, enterprise dataset classification contributes to more efficient operations, better decision-making, and a deeper understanding of an enterprise's data landscape.

Cloud-based Enterprise Resource Planning (ERP) implementations can benefit greatly from the incorporation of enterprise dataset classification. Classification of datasets ensures proper data organisation, efficient search and retrieval, streamlined workflows, data-driven decision making, personalised and customised experiences, compliance and security, integration with analytics tools, scalability, collaboration,

automation of processes, change adaptability, and audit trails. By centralising data storage, classification of datasets enables users to rapidly locate specific data, reduce time spent searching, and streamline workflows. It also improves data-driven decision-making, personalization, and customization, resulting in improved data security and decision-making. Integration with analytic tools can result in more precise and insightful reports and visualisations (Ng et al., 2021). As the enterprise grows and the ERP system expands, scalability is maintained, while collaboration, automation, and adaptability to change are all advantages of appropriate dataset classification. To ensure the classification process correlates with the organization's objectives and maximises the benefits of a cloud-based ERP system, careful planning and consideration of factors such as data types, classification criteria, user roles, and ongoing maintenance are required (Gupta et al., 2019).

Enterprise dataset classification is crucial for promoting data security in a public cloud environment (Hababeh et al., 2018). The extent of integration depends on factors such as data sensitivity, regulatory compliance, the organization's risk tolerance, and the cloud provider's security offerings (Ng et al., 2021). To determine the appropriate extent of dataset classification, consider factors such as data sensitivity, regulatory compliance, data classification framework, access controls, encryption, data loss prevention (DLP), security incident response, data retention and deletion policies, cloud provider security features, continuous monitoring, employee training, and third-party services.

Data sensitivity refers to the level of data being stored and processed in the cloud-based ERP implementation. Regulatory compliance ensures that data classification aligns with industry-specific regulations and data protection laws (Mezgár and Rauschecker, 2014). A clear data classification framework defines categories or labels based on sensitivity, confidentiality, and criticality, guiding the classification process and determining security measures (Suthaharan, 2016). Access controls should be implemented, and encryption should be applied to classified data, both at rest and in transit. Data loss prevention (DLP) solutions should be integrated to monitor and

prevent unauthorized movement or sharing of classified data. Security incident response plans should be developed, and data retention and deletion policies should be defined based on classification. Cloud provider security features should be leveraged, and continuous monitoring should be conducted to identify gaps or vulnerabilities. Employee training should educate employees about the importance of dataset classification and data security practices, and third-party services should be classified and protected according to the organization's standards. By effectively classifying and securing data, enterprises can enhance their data security posture and reduce the risk of data breaches and unauthorized access in the public cloud environment. Therefore, our research seeks to understand to what extent should enterprises dataset classification form part of a cloud-based ERP implementation to promote enterprise data security in the cloud from our participants viewpoint.

#### **3.1.1.4 RQ4: To what extent can enterprise database fragmentation in the cloud improve the enterprise data security of cloud-based ERP systems?**

Fragmentation is a database server feature that enables control over where table-level data is stored (Okardi and Asagba, 2021). Fragmentation permits the definition of groups of records or index keys within a table based on an algorithm or scheme. It can occur in various ways within a database management system (DBMS), impacting both data and indexes (Gonzalez et al., 2010). Internal fragmentation occurs when data storage within database pages becomes inefficient, leading to increased storage consumption and slower data retrieval. External fragmentation occurs when there's a mismatch between the logical order of data and the physical storage order, causing disordered physical layouts (Sears and van Ingen, 2006). Index fragmentation, on the other hand, helps improve query performance by providing a quick way to locate data (Cioloca and Georgescu, 2011).

Database administrators often need to manage and mitigate fragmentation to maintain database performance (Zhang et al., 2015). Defragmentation involves rearranging data and indexes to reduce internal and external fragmentation, while reorganization involves reordering the physical layout of data and index pages to reduce



fragmentation and improve data retrieval efficiency (Valavala and Alhamdani, 2020). Rebuilding can eliminate fragmentation by recreating the index structure from scratch, and vacuuming can help reduce internal fragmentation by reclaiming unused space within data files (Valavala and Alhamdani, 2020). Managing fragmentation is essential for maintaining optimal database performance and minimizing storage overhead (Hauglid et al., 2010). Regular monitoring, analysis, and appropriate maintenance actions can help keep fragmentation under control and ensure efficient data access and storage. Enterprise databases are crucial for supporting organizational operations and supporting various critical applications and services. Key factors contributing to enterprise database fragmentation include data volume, concurrent users and applications, index management, data distribution, data lifecycle, and complex queries (Bender et al., 2022). To address enterprise database fragmentation, organizations need to implement comprehensive strategies such as regular maintenance, monitoring and analysis, automated tools, data archiving, indexing strategies, and partitioning techniques. Addressing fragmentation is vital for maintaining high performance, scalability, and reliability in enterprise databases (Bhuyar et al., 2012).

Enterprise database fragmentation offers various advantages and disadvantages, such as scalability, performance optimization, fault tolerance, geographical distribution, data isolation, customization, and security (Bhuyar et al., 2012). However, it also introduces complexities, data consistency challenges, maintenance overhead, query complexity, resource allocation, data movement costs, security and compliance challenges, and vendor dependencies (Hudic et al., 2013). Advantages of enterprise database fragmentation include isolation of data, reduced attack surface, enhanced access control, data masking, and regulatory compliance (Bhuyar et al., 2012). It can help isolate sensitive data, minimize attack surface, and enable finer-grained access control. Fragmentation can also facilitate data masking strategies, allowing certain users access to non-sensitive data while protecting critical information. However, there are also disadvantages to enterprise database fragmentation, such as complexity in data distribution, synchronization, and maintenance (Hudic et al., 2013). This complexity can impact the overall security posture if not managed properly. Ensuring data consistency across fragmented portions of the database can be challenging, especially

for cloud-based systems where data movement and synchronization may involve network latency and potential data discrepancies Hudic et al., 2013). Vendor and infrastructure dependencies can also influence how fragmentation is implemented, and organizations need to align their fragmentation strategies with the capabilities and security features provided by their chosen cloud provider. Additionally, fragmentation can complicate backup and disaster recovery processes, requiring careful planning to ensure data availability and resilience (Sengupta and Annervaz, 2014). Overall, enterprise database fragmentation offers both advantages and disadvantages, and organizations must carefully evaluate and implement appropriate strategies to harness its advantages while mitigating its disadvantages.

To enhance data security in cloud-based ERP systems, it is crucial to implement best practices for database fragmentation. These include threat modelling, access controls, encryption, regular audits, data synchronization, vendor collaboration, and testing and monitoring (Sengupta et al., 2011). Threat modelling helps identify potential security risks and vulnerabilities, while access controls ensure authorized users have access to specific fragments. Encryption protects data both at rest and in transit. Regular audits evaluate the effectiveness of fragmentation strategies, while data synchronization maintains consistency across fragmented data. Collaborating with cloud providers and testing and monitoring the security of the fragmented database environment can help detect and mitigate potential security issues promptly. Therefore, our research seeks to understand to what extent can enterprise database fragmentation in the cloud improve the enterprise data security of cloud-based ERP systems from our research participants viewpoint.

#### **3.1.1.5 RQ5: To what extent can cloud computing have an impact on enterprise system data security?**

Cloud computing can significantly impact enterprise system data security, both positively and negatively, depending on how it is implemented and managed (Ahn and Ahn, 2020). The benefits of cloud computing include centralized security expertise, advanced physical security measures, automated security updates, economies of scale,

redundant storage and backup solutions, and disaster recovery (Avram, 2014). However, there are also negative impacts on data security, such as data breaches, data handling and compliance challenges, shared responsibility models, vendor lock-in, downtime and service availability, and compliance and regulations compliance (Haddara et al., 2022). To ensure a successful and secure cloud implementation, enterprises must carefully consider the chosen cloud provider, data protection measures, compliance requirements, and ongoing security monitoring and management (Kuranga et al., 2021). It is important for enterprises to assess their specific security needs, conduct thorough risk assessments, and implement appropriate security controls to mitigate potential risks (Al-Johani and Youssef, 2013).

Key areas where cloud computing can affect enterprise system data security include access control and authentication, data encryption, data loss prevention (DLP), network security, compliance and regulations, vendor management, incident response and recovery plans, data transfer and migration, data residency and sovereignty, and training and awareness (Das and Dayal, 2016; Ahn and Ahn, 2020). Enterprises need to use secure methods for data migration and consider how data may be exposed during transit. Data residency and sovereignty are crucial aspects of cloud services, as they might store data in multiple geographic locations (Lukings and Habibi Lashkari, 2022; Gondree and Peterson, 2013). In conclusion, cloud computing has a substantial impact on enterprise system data security, affecting various aspects of security practices and outcomes. To maximize the benefits of cloud computing while mitigating potential risks, enterprises must carefully assess their security requirements, select appropriate cloud services, and implement comprehensive security measures. By doing so, they can enhance their overall data resilience and protect sensitive information from potential threats.

Therefore, our research seeks to understand to what extent can cloud computing have an impact on enterprise system data security from our research participants viewpoint. The above section 1.6 in Chapter 1 looked at our eight research assumptions which

was adopted in a bid to answer our research questions and understand the viewpoint of our research participants.

### 3.1.2 Research Assumptions

The guiding beliefs that researchers employ to organise and carry out a study are known as research assumptions, and they influence the design, data gathering, and analysis. Theoretical, epistemological, ontological, methodological, sampling, statistical, ethical, cultural, and resource assumptions are examples of common categories of research assumptions. These assumptions ought to be made clear in the study documentation that researchers provide. Following the literature review that was presented in the chapters before this one, a theoretical framework was constructed to guide the research and identify additional fieldwork that would be conducted for this project. The research assumptions proposed by the researcher to investigate the links between the important of adopter end-user security responsibility in ensuring enterprise data security in public cloud. The assumptions are based on literature in this research and listed in Table 3.2 below. The aim is for the proposed approach to improve enterprise data security in the public cloud. It evaluates the numerous characteristics of the suggested model and assumes the advantages of these characteristics. If each of the preceding assumptions holds true for an ideal cloud-based ERP system, we have created sub-questions to examine these assumptions.

*Table 3.2: Initial Research Assumptions (Eya, 2023)*

<b>A1</b>	<b>Participants who have worked with a cloud-based ERP system are more likely to provide a valid response to our research survey.</b>
<b>A2</b>	Ideally, any upgrade in technology should have an impact on the previous technology, although this impact can either be positive or negative. Therefore, Cloud computing would have an impact on Enterprise system data security in Cloud.
<b>A3</b>	When the Cloud Service Provider and the Cloud Service End-users share the security responsibility of the cloud system, it will result in more secured enterprise data in the cloud.

<b>A4</b>	A proper Access Management within the Cloud Service End-user enterprise would positively improve their enterprise data security in Cloud.
<b>A5</b>	The proposed CSP Access Directory when implemented, would improve Access Control Management in the Cloud.
<b>A6</b>	Enterprise data set classification when carried out as an integral process of moving enterprise data set to the Cloud would help in creating the Enterprise Access Directory and improve Enterprise data security in Cloud, since only classified data are moved.
<b>A7</b>	System notification to the Enterprise System Administrator when there is an unsuccessful login attempt is more likely to promote Enterprise data security in the Cloud.
<b>A8</b>	Enterprise Database Fragmentation in the Cloud would improve Enterprise data security of a Cloud-based ERP system.

After establishing the primary and secondary research questions and research assumptions, it is critical to gain an understanding of the philosophical concerns underlying the research in order to form an informed opinion about how the study's findings can be most effectively applied to real-world occurrences.

### **3.2 Research Design and Strategy**

A research design is an inquiry within the qualitative, quantitative, and mixed methods approaches that provides precise guidance for processes in a research plan. The study design's objective is to assist the researcher through the process of collecting, analysing, and interpreting data. They are also known as inquiry strategies (Denzin & Lincoln, 2011). The nature of the research challenge and the manner in which it seeks solutions might influence research design. Saunders and Tosey (2013) categorise research methods based on the approaches employed to answer research questions.

This study is the first of its kind to examine end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the

formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria and aims to investigate the existing level of knowledge on the subject. The study's goal and research assumptions guided the researcher's technique of choice, in accordance with Trost (2005), who contends that the objective and problem of the study should guide the technique selection.

This chapter introduces the major procedures utilised with the fieldwork tools to fulfil the research's principal goal and goals.

### **3.2.1. Selection of Method and Approach**

The goal of research methodology and design is to use the best way to answer the core research issue. Hayes et al. (2013); Yin (2014). Three requirements, according to Aberdeen and Yin, (2013), separate distinct research approaches:

- The nature of the study question
- The degree of control an investigator has on behavioural occurrences.
- The degree of emphasis on present rather than historical events

To achieve the study aims, the researcher used the pragmatic paradigm and used a mixed-methods technique as the vehicle for data collection. This study combines quantitative and qualitative methods to give a rich contextual foundation for evaluating and validating findings. Combining qualitative and quantitative data has three important advantages. It makes it possible to validate and confirm study results. It can aid in refining or enhancing analysis and providing additional information, as well as sparking new ideas and providing new perspectives on specific topic (Miles and Huberman, 1994).

### **3.2.2. Research Overall Process**

The research examined end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. This study goal is accomplished by analysing the present

status of cloud computing security models. It also examines the essential human factor elements that influence the adoption of a cloud-based ERP systems in such organisations. The research process outlines how the study will proceed, as well as how data will be collected, analysed, and reported.

### **The Four Phases of the Research Process.**

To adequately explain all the research activities, we have taken a four-stage approach, with each stage detailing all the research activities that occurred during that stage. The stage-by-stage approach ensures that no research activity is overlooked during the thesis writing process. The stage-by-stage approach enables definition of our research problem, objectives, and goals before applying appropriate research techniques to close the gap identified. A mixed-methods approach to research, combining quantitative and qualitative techniques. The two methods were chosen because our objective was to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. The aim is to either support or oppose the proposed implementation approach viewpoints. We discovered that using mixed methods will enable us to gain a better understanding of the perspectives of the research participants. Because our primary data collection occurred following the initial study, we ensured that our questions were more focused on the outcomes highlighted in the initial study. Goddard and Melville (2004) argue that a mixed-method approach is preferable for gaining a better understanding of any research problem, as it combines the strengths of both research methods while eliminating their weaknesses and allowing each to complement the other. Our research methodology proceeded through four stages:

#### **3.2.2.1 Stage 1: Project Initiation**

This stage entailed conducting research activities such as conducting a literature review, developing a initial study, performing parametric analysis on cloud computing security models, and conducting an evaluation analysis on existing cloud computing security models. The literature review broadens the problem domain of end-user

inactivity regarding enterprise data security in the cloud. Preparing a initial study entail contacting potential participants in the research exercise.

We compiled a list of potential collaborators and visited some; for others, we sent an e-mail. Opening conversations with potential research partners quickly made us realise that the anticipation and excitement that a researcher may feel during the planning stage of his/her research may not be the same as what an enterprise feels about the research. The majority of businesses wanted to know whether their data was secure and what they could gain from such research activity. Numerous individuals declined to participate. Some agreed to participate to support the research. Others joined out of curiosity about what it would be like for their business to be involved in such research. Additionally, at this stage, we prepared our interview materials and obtained ethical approval for the research and ethics documents can be found in Appendix 1.

Consideration of the various cloud delivery models and the attributes of cloud data security also provided a thorough understanding of the CSP's and end-user's security responsibilities. We use parametric analysis to compare the effectiveness of the various cloud computing security models under consideration. To compare the various model reviews, we used parameters such as the security technology used, the security responsibility assumed, the security effectiveness, the security porosity, the targeted cloud feature, and the practicality. This provided a thorough understanding and highlighted the fact that while all cloud computing security models share the goal of securing the cloud system, the model that is most effective at accomplishing this goal will be highly secured and have a low degree of porosity.

Additionally, the evaluating analysis revealed that the majority of cloud computing security models share a fundamental goal of protecting the cloud system, despite the fact that they target distinct aspects of the cloud system, each with its own set of strengths, weaknesses, opportunities, and treatments. The Project Initiation Phase (P.I.P.) provides an opportunity to review and comprehend all the concepts that shaped our research assumptions and problem domain.



### **3.2.2.2 Stage 2: Prioritization Phase of the Project (P.P.P)**

This is the stage referred to as the Prioritization Phase of the Project (P.P.P). Three distinct project activities occurred during this stage. Execution and analysis of the initial study's findings, prioritisation of end-user involvement in cloud computing security within the enterprise, and formulation of a cloud computing security implementation approach. The new proposed model makes use of the following attributes: Enterprise Access Directory (E.A.D), Enterprise Database Fragmentation (E.D.F), Enterprise Access Queries (E.A.Q), and CSP Access Directory (CSP A.D) to improve enterprise cloud data security and end-user experience by encouraging increased end-user involvement in enterprise cloud data security. Finally, based on the findings of the initial study and literature review, it is necessary to prioritise end-user involvement in cloud computing security, as this has the potential to eliminate blame games and issues of lack of trust in CSPs, both of which have impacted the adoption rate of cloud-based ERP solutions. Our new cloud computing security implementation approach was proposed as a result of a parametric analysis of existing cloud computing security models. The goal was to create a model that was highly secure and had a low level of porosity, which would encourage increased end-user participation. At this stage, we drew the implementation approach sketch and considered the various attributes the model should have.

### **3.2.2.3 Stage 3: Project Analysis Phase (P.A.P)**

This stage is identified as the Project Analysis Phase (P.A.P). Three research activities were conducted during this phase. The initial research activity was to design and conduct a survey. A series of questions were developed to probe various facets of the research and our proposed CCS implementation approach. The initial draft questions were further narrowed to fifteen core questions because we believed it was more important to have concise, quantifiable questions than it was to have lengthy questions that might discourage research participation. Our goal was to reduce the average response time to the survey to ten minutes. The fifteen questions were developed based on various project assumptions, each of which addresses an aspect of our proposed

implementation approach. We wanted to use these sets of questions to elicit an opinion from our participants about our proposed implementation approach, which could be to oppose or support the model's viewpoints. We began identifying and recruiting potential research participants after developing and revising our research questions. At this point, we recognised that the quality of the opinions gathered trumped quantity. Our desire to use the best professionals in the field to conduct our research grew out of the belief that an experienced professional's opinion would carry more weight. We recruited participants in two ways: first, by directly contacting identified and well-known IT professionals via email, secondly, by recruiting participants on LinkedIn, considering their job profiles; and finally, by sharing our survey invitations via professional LinkedIn groups. This strategy worked well, albeit not as quickly as we anticipated, but gradually we recruited high-quality research participants for our study. We created the questionnaire using Qualtrics Software. This was a straightforward decision, as the university already had a paid account and the software-enabled easy distribution of the questionnaire across multiple platforms.

We distributed the questionnaire directly to participants via email, WhatsApp messages, and through LinkedIn cloud computing research groups such as Virtualization & Cloud Computing Solutions, which has 25,024 members; Cloud Computing, Cyber-security, SaaS, & Virtualization, which has 555,875 members; Enterprise Mobility: Mobile Cloud Computing & Enterprise Applications, which has 3918 members; and Cloud Computing, Virtualization, and Disaster Recovery in Nigeria, which has 555,875 members. The initial sample size is approximately 80 participants via direct email and six shares on various cloud computing LinkedIn groups. The response rate was approximately 23 responses during the first two weeks. Fortunately, we emailed reminders to research participants and reshared survey links on the six LinkedIn groups in which we conducted our research. We chose to extend the research period in order to recruit a larger sample size. By the end of the eight weeks, we'd received 43 responses. We knew it was safe to proceed to the next stage of the research at this point. 43 professional-quality opinions on the proposed implementation approach's viewpoints provided a solid foundation for proceeding to data analysis.

This stage's second research activity was the qualitative and quantitative data analysis of survey responses. Because our questionnaire included both multiple-choice and open-ended responses, we gathered two distinct sets of data. The quantitative analysis was carried out by creating crosstabs from the default report generated by the Qualtrics software and also exporting the data to Excel and SPSS to perform data cleaning and analysis. The qualitative component of our survey was also reviewed in order to determine similarities and outcomes.

This stage's third research activity was goal-directed reviewing. We identified the attributes of our model that received the least support from research participants based on the results of our survey exercise. We then re-examined our proposed model to determine whether any of the attributes needed to be changed to accommodate the contributions from our research findings. Although the data we obtained supported many of the attributes, we chose to review how the CSPA.D. and E.A.D. may be similar or dissimilar. If they are comparable, does this increase the security of enterprise data stored in the cloud? If they are different, does this have any effect on the cloud system's security effectiveness? This brought us to the next stage of our investigation.

#### **3.2.2.4 Stage 4: Project Evaluation**

This stage is divided into three distinct research activities. As the concluding phase of our research, it proceeded much more quickly than the previous phase, owing to our ability to draw on the experience gained during the previous stages of research activities. The first research activity was the analysis of our initial interview's qualitative data. This included the transcription of the interview and the reviewing the responses. The second research activity should be the development of a prototype for the CSP A.D. and E.A.D, although we discussed what a likely prototype should be due to financial and time constraints an actual prototype was not designed. Following that, we began the final research activity of documenting our findings in a thesis and presenting our findings, recommendations, and future

research proposals. The figure 3.1 below shows the visualization of research overall process as describe in the above paragraph.

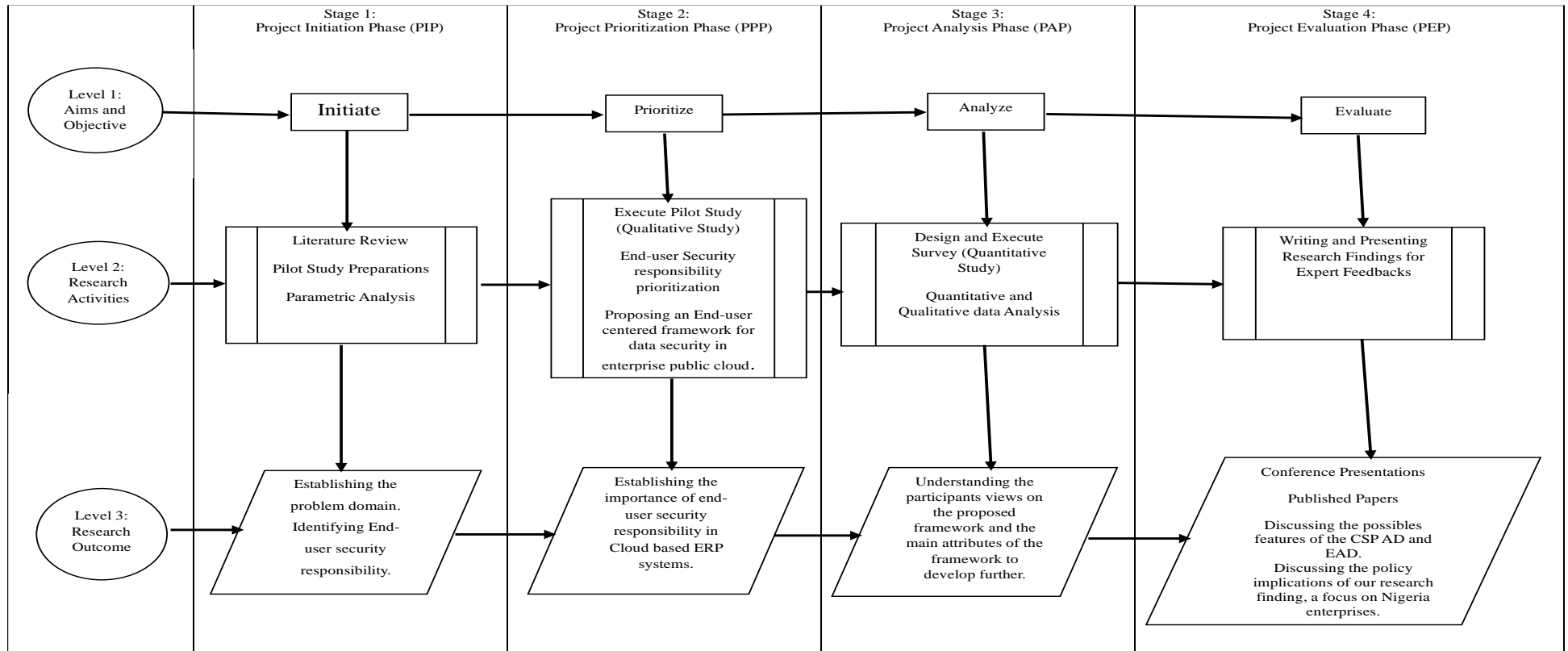


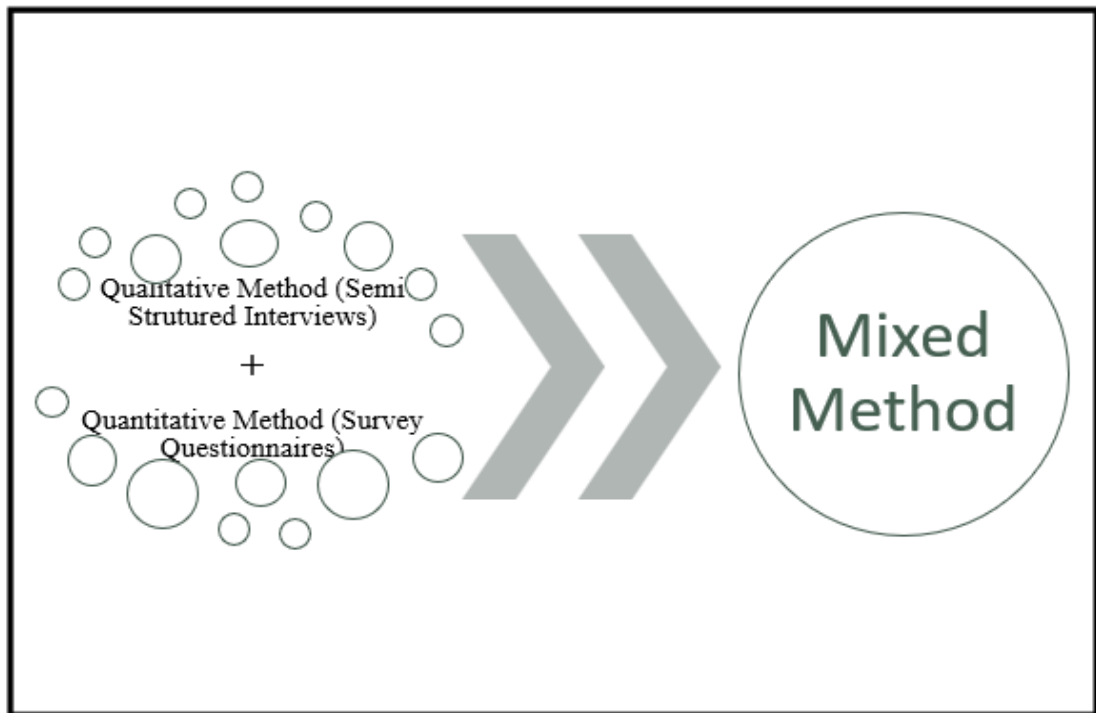
Figure 3.1: Visualization of Research Overall Process

### **3.2.3 The Mixed-Methods Approach**

Considering the nature of the research questions in section 2.8 of Chapter 2 and the scope of the study, we determined after extensive reading that the best research methodology is the mixed method. Section 3.2.3.1 provides justification for this decision. Mixed-methodologies research is a research strategy that combines philosophical assumptions with empirical processes. Combining qualitative and quantitative data in a single or series of research as shown in Figure 3.2 below. The combination of quantitative and qualitative methods yields a deeper comprehension than each method alone. In social research, triangulation is the combination of data or methods in such a manner that many perspectives shed light on the issue. (Olson, 2004). When a researcher combines quantitative and qualitative data and methods within a single study, this is known as a mixed methodological approach. According to Jacobsen (2002), this combination mitigates the limitations of each technique. Using partially mixed methods, quantitative and qualitative research may be conducted concurrently and then integrated during data interpretation. Blended techniques are advantageous when quantitative or qualitative approaches alone cannot adequately address the research concerns (Creswell, 2003). Finally, the mixed-methods approach is a research design that combines elements of both qualitative and quantitative research methods within a single study. This approach seeks to leverage the strengths of both methodologies to provide a more comprehensive understanding of a research problem or question. By integrating qualitative and quantitative data collection and analysis techniques, researchers aim to gain richer insights, validate findings, and offer a more complete view of the phenomenon under investigation.

Summarily, the mixed-method research approach was determined as the most suitable methodology considering the research questions and study scope, as discussed in Section 3.2.3.1. Mixed-method research combines qualitative and quantitative approaches, providing a deeper understanding of the phenomenon being studied, as depicted in Figure 3.2 below. This approach, endorsed by Olson (2004) and Jacobsen (2002), mitigates the limitations of individual methods and allows for concurrent data

collection and integration, addressing research concerns comprehensively, as advocated by Creswell (2003).



*Figure 3.2: Components of Mixed Method*

A mixed-methods methodology was used to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria and examine the attributes of the proposed implementation approach for cloud-based ERP systems with an enterprise. According to the techniques approach, quantitative analysis generates generalizability through statistical comparisons of volumes of data. But qualitative data adds richness through individual lived experiences. Greene (2014), identify one of the goals of mixed method research as "expanding the breadth and range of inquiry". Johnson and Onwuegbuzie (2004) propose a mixed-methods research strategy. The goal of mixed methods is not to replace either quantitative or qualitative approaches, but to profit from their strengths while minimising their limitations. Johnson & Onwuegbuzie, (2004) mentioned a mixed-methods approach allows researchers to get a more comprehensive and complementary understanding of the subject under

investigation. As a result, research is becoming more "interdisciplinary, complicated, and dynamic".

Table 3.3: *Mixed Method Designs. By Creswell et. al., 2009*

<b>Design Type</b>	<b>Description</b>
<b>Concurrent Transformative</b>	It involves gathering both quantitative and qualitative information at the same time. It is driven by a theoretical perspective on the research issue or the purpose of the study. This perspective is used to guide all the decisions about the methodology, and the objective is to evaluate that perspective.
<b>Concurrent Nested</b>	This design comprises one data collection phase in which emphasis is given to one method that guides the project, while the second approach is incorporated or nested inside the project and serves a supporting role. The embedded method frequently addresses a question other than the primary study topic.
<b>Concurrent Triangulation</b>	This design collects qualitative and quantitative data in two stages. Each data set is separately analysed, and then the results are compared and/or combined. This procedure is used to confirm, cross-validate, or support previously discovered information. It can also be used to collect qualitative data with an open-ended format that can be added to quantitative data.
<b>Sequential Transformative</b>	This design also has two stages, but it lets the researcher's theoretical point of view guide the investigation and decide the order in which data is collected. At the end of the study, during the interpretation phase, the results from both approaches are put together.
<b>Sequential Exploratory</b>	This is a two-phase design in which qualitative data is acquired first, followed by quantitative data gathering and analysis. This design's goal is to provide an instrument (such as a survey), a classification for testing, or to discover factors. This sort of design might include using information from journals or other sources to create relevant surveys to distribute to a bigger sample.
<b>Sequential Explanatory</b>	A two-phase approach in which quantitative data collecting occurs first, followed by qualitative data collection. The objective is to employ qualitative discoveries to further explain and interpret quantitative data. A survey, for instance, may be used to collect quantitative data from individuals, and then a bunch members of this group may subsequently be chosen for interviews in which they may explain and provide insight on their survey answers.

The mixed-methods approach design is one of the most commonly used in computing research and has been developed by Fraenkel and Wallen (2008) and Creswell (2009) as well as others. It comprises of six key design categories: sequential explanatory design, sequential exploratory design, sequential transformational design, concurrent design, concurrent embedded design, and concurrent transformative design as shown in the table 3.3 above.

Table 3.4: Mixed Method Designs Comparison

Design Type	Stages	Purpose	Strength	Weakness
<b>Concurrent Transformative</b>	Research is based on a certain theory (critical theory, advocacy, participatory research, or a conceptual or theoretical framework, for example).	All methodological decisions are influenced by the theoretical approach (problem definition, design, data source identification, analysis, interpretation, and reporting of results throughout the process).	Transformational framework; faster data collection; both quantitative and qualitative data; get different views from different types of data or research levels	Before being used in the analysis phase, data must be changed. There aren't many written instructions, and it's not clear how to deal with differences in results from different methods. When one method is given more importance than another, it is difficult to determine what the results indicate.
<b>Concurrent Nested</b>	Main method that guides the project (embedded or nested methods are less common and can answer a different question or look for information at a different level). During the analysis phase, data was mixed up.	A broader view than one method (embedded quantitative might give a more detailed description of sample members; embedded qualitative might explain an unquantifiable part of quantitative); one	The strengths are shorter data collection, both quantitative and qualitative data, and multiple perspectives from different types of data or different levels within the study.	Data must be changed in order to be used in the analysis phase; there isn't much written guidance; it's not clear how to deal with differences in results from different methods.



		inside the framework of the other (e.g., conduct experiment as case study of different treatments)		When there isn't equal evidence before combining the priority of two methods, it's hard to figure out what the results mean.
<b>Concurrent Triangulation</b>	Two methods are used to confirm, cross-validate, or check the results of a single study. - Methods make up for what other methods don't do well. Priority should be the same for everyone, but this isn't always possible. - Connects results to the rest of the interpretation phase: Knowledge claims are either made better or clearer by convergence.	Choosing a model triangulation allows you to view the broader picture more clearly	It's easy to understand, the conclusions are well-supported and well-validated, and it's faster to collect data than in a two-stage study.	Looking at a phenomenon in two ways takes a lot of work and knowledge. It's hard to compare results before combining different methods, and it's not clear how to settle differences in results from different methods.
<b>Sequential Transformative</b>	Either strategy is used first, is prioritized, or is given equal weight. The findings are pooled at the interpretation stage. Research is driven by theory rather than methods.	The goal is to adopt ways that best support the theoretical point of view (give voice to different points of view, speak up for participants, and learn more about a phenomenon or process that is changing because of the study).	Design, description, and reporting are done in stages.	The temporal span between two different stages (especially if they have the same amount of emphasis).

<b>Sequential Exploratory</b>	<ul style="list-style-type: none"> <li>- Priority in the first stage - Collect and analyse qualitative data</li> <li>- Gather and analyse quantitative data</li> <li>- Integrated during the interpretation phase</li> <li>- Theoretical viewpoint may or may not exist</li> <li>- Quantitative data aids in the comprehension of qualitative data.</li> </ul>	Look into a phenomenon (find out how often it happens in a certain population); grounded theory is the process of putting parts of an emerging theory to the test so that it can be used more widely; making and trying out a new tool.	distinct stages in design, description, and reporting	How long it takes to combine two separate processes; it might be hard to switch from qualitative analysis to quantitative data collection.
<b>Sequential Explanatory</b>	<ul style="list-style-type: none"> <li>- Gather and analyse qualitative data</li> <li>- Gather and analyse quantitative data</li> <li>- Integrated during the interpretation phase</li> <li>- Theoretical viewpoint may or may not exist</li> </ul>	Qualitative data may be used to assist explain and interpret quantitative data. Useful when unexpected quantitative results are achieved - qualitative analyses are exhaustive	Various steps in design, description, reporting	How long it takes for two separate stages to come together (especially if they have equal emphasis)

The table 3.4 above shows there are no perfect method, but there is one that is best for looking at a certain research topic. Quantitative methods give researchers an objective way to measure reality, while qualitative methods let them study and understand a phenomenon's subtle elements. Each quantitative and qualitative research technique is made to answer a certain type of research question and looks at, and explores, different kinds of information. The best way to look into the current research problem was to use an sequential exploratory mixed methods design. With this approach, different methods can work well together. The survey is used to determine which concerns are significant to the study's broad population. The interviews are utilised to provide further information on the identified gaps.

### **3.2.3.1 Justification for Adoption of Mixed Methods**

We are tasked with testing the attributes behind our suggested implementation approach with the assistance of our study participants. We might confirm this using a range of techniques, such as case study, comparative case study, qualitative research, quantitative study, and mixed-method approaches.

*A case study approach:* Case studies will be used to identify an enterprise that is currently deploying a cloud-based ERP solution. This technique enables us to collaborate closely with the implementation team and corporate staff to guarantee that the suggested model's attributes are included and executed. For example, "business data set categorization based on data sensitivity and enterprise role classification; enterprise data set fragmentation inside the corporate database." After the implementation exercises, we would be able to observe first-hand how the model increased enterprises' end-user involvement in cloud data security, how the model approach can increase enterprise employees' awareness of their cloud security responsibilities, and how CSP trust will be enhanced. Our model concepts will be validated through the reviews of the participating enterprise in this manner. We were unable to adopt this strategy, even though it would have been preferable because we were unable to obtain a participating enterprise during our research time. Enterprises that worked with us during the initial study were unable to continue in the latter stages of the research since they were not yet using a cloud-based ERP system.

*A comparative case study:* This approach will involve two enterprises, ideally one that is already using a cloud-based ERP solution and another that will implement cloud-based ERP solutions based on our model attributes and methodology. This will be a type of longevity study, in which we will examine data security incidents from both enterprises over time and using comparable parameters, such as similar size, nature of business, and location of business. Our objective is to determine whether any of the proposed model's attributes reduced the number of data security incidents in a cloud-based ERP system. Additionally, we will be able to observe how end-user security

accountability improves enterprise data security in a public cloud environment. This study would have been excellent because it would have compared the proposed model to a real-world model. Enterprises that collaborated with us during the initial study were unable to continue in the later stages of the research because they were not yet implementing a cloud-based ERP system.

***A quantitative study:*** This study design will be ideal for quantifying the extent to which our research participants agree on the model's attributes. However, quantity alone may not be sufficient to validate the concepts underlying our proposed model. For example, just because all of our research participants agreed that data security is a significant challenge in the cloud does not mean it is true. Thus, while a quantitative study alone will not suffice to validate the concepts of our proposed model, it will suffice to demonstrate the proportion of participants who agree or disagree with the model's concepts.

***A qualitative study:*** A qualitative study will allow our research participants to provide us with detailed feedback on their perceptions of our proposed model. A qualitative study involving interviews will enable us to conduct a more in-depth examination of the model's attributes. Although qualitative research is excellent at reviewing models, we face the constraint of not being able to reach a sufficiently large sample size of research participants given the pandemic situation at the time of the research. As a result, we chose a mixed method that combines the best features of both research methods, even when the sample size of research participants is small.

***Mixed method study:*** This research design requires us to simultaneously undertake quantitative and qualitative research. Because this methodology integrates quantitative and qualitative research methodologies, it was selected. Consequently, mixed methods will allow us to comprehend our research question numerically (how many of our research participants agree with us) and subjectively (how many of our research participants disagree with us) (the in-depth understanding of the reasons and justification for the responses they provide). For analysing the concepts in our

suggested model for this study, the mixed technique was the most suitable approach. We will be able to identify the number of study participants who agreed with the model concepts and their justifications for agreeing with the model's recommended features. This will strengthen our study data and the trustworthiness of the proposed model. In order to make the most of the sample number of study participants we had, it was also crucial that we employ a mixed methodology. As a result of our mixed-method approach, we selected survey questions with a Likert Scale option, allowing respondents to pick an answer and then provide an explanation for their choice. This allowed us to concurrently gather quantitative and qualitative data.

One of the numerous incentives for selecting a mixed-methods approach is the researcher's desire to address the issue comprehensively within a single piece of research. This desire is only one of many possible justifications. When doing research using a mixed methodology, additional information on the subject of the study is acquired, and the combined strengths of each research approach produce results that are trustworthy and valid. In order to have a full understanding of the findings of the current research, it is necessary to provide extensive explanations for some aspects of the study, particularly those that deal with enterprise end-user security responsibility, cloud computing security, management support, training, and awareness programs. As a direct consequence of this, it was decided to conduct semi-structured interviews with some of the experienced IT and IS personnel.

Even though Creswell and Clark (2007) say that research is easier to do when there is only one type of data to collect and analyse at a time, mixed methods are thought to have the following benefits:

- Assist in improving the validity and reliability of study findings and ensuring that they are scientifically sound (Pearson et al., 2015).
- Be able to combine the strengths of qualitative and quantitative methodologies (Pearson et al., 2015).

- When compared to a single method approach, mixed-methods research allows researchers to examine and investigate complicated topics in a more thorough and broad-based manner (Lockyer, 2006).
- Qualitative approaches, for example, are more interested in how something works at a deeper level, whereas quantitative methods are more interested in how something works at a high level (Merriam and Grenier, 2019).
- Mixed-methods research allows researchers to reach a broader variety of results, leading to additional study (Pearson et al., 2015).

### **3.2.3.2. Pragmatic Approach**

This study used a pragmatic approach with a mixed method. This pragmatic method puts the focus on the results of the research and has a pluralistic nature. Pragmatists want to learn more about the structures and mechanisms that make up a phenomenon. They ask questions that can be answered using both positivist and interpretivist methods.

Peirce's method of inquiry is based on abduction, deduction, and induction, which are all types of reasoning that can be used over and over again. This way of thinking is unique to Peirce's philosophy because it combines the three steps into a single unit of methodological inference, which is a complete way to clear up doubt (i.e. solve a problem). The pragmatic approach accepts deduction as a way to figure out what the results of assumptions are and to test and prove research assumptions. (Peirce, 1986).

According to Creswell (2009), the predominant paradigm with a strong philosophical relationship for a mixed-methods approach is a pragmatic research strategy. In mixed-methods research, pragmatism or a pragmatic approach is therefore frequently employed as a philosophical concept. Onwuegbuzie and Johnson (2004) mentioned in mixed-methods studies, for instance, researchers frequently develop knowledge for pragmatic reasons. Philosophically, pragmatism considers knowledge as a necessary

reality or direct experience. Consequently, knowledge can be converted, updated, or altered throughout time, whether or not it is studied.

A pragmatic approach provides a firmer basis than a single-method approach for examining complicated phenomena in greater depth and responding to what, why, and how research questions is desirable (Saunders et al., 2009). Taking into account the particular characteristics of this pragmatic perspective and deducing critically from the foregoing, the most appropriate strategy for this research is a pragmatic approach.

### **3.2.3.3. Justification for the Adopted Pragmatic Approach**

A pragmatic strategy, according to researchers such as Creswell (2009) and Rossman and Wilson (1985), focuses on the research topic rather than the methodology and employs a range of methodologies to comprehend the problem. Creswell (2009) summarises the key philosophical assumptions of pragmatic research, on which this thesis is built.

- Each researcher is allowed to select the methodologies, methods, and processes that are most suited to their requirements and objectives.
- Pragmatists do not see the world as a whole.
- Whatever works at the time is the truth. Pragmatist researchers are concerned with the "what" and "how" of research in light of what they aim to discover (i.e. where they want to go with it).
- Pragmatists believe that research takes place in a variety of settings, including social, historical, political, and other factors.
- Pragmatists think that there is a world beyond the mind as well as a world within the mind.
- Pragmatism provides for a variety of methodologies, worldviews, and assumptions, as well as varied approaches to data collection and analysis.

The aforementioned arguments, particularly those relating to subjectivity and unpredictability, support the choice to take a pragmatic approach in the current study.

When analysing participant viewpoints, the pragmatic research philosophy's combination of diverse data gathering techniques offers the chance to be both objective and subjective. (Saunders et. al. 2009)

The following sections shed light on the two research methods for data collection.

### 3.3 Data Collection Techniques

Data is defined as "the facts offered to the researcher by the study environment, which are subsequently turned into valuable information." Bryman and Bell (2007) advocates mixing quantitative and qualitative approaches for data collection in the same research to improve decision-making. After examining and analysing all available information using both qualitative and quantitative methodologies, decisions are made. According to Bryman and Bell (2007), the use of triangulation is made possible by combining quantitative and qualitative data. To collect data for this study, survey questionnaires with Likert scale choices and semi-structured interviews with open-ended questions were used as shown in Figure 3.3 below. The purpose of this strategy is to gain a better knowledge of the study topic by allowing the researcher to ask semi-structured questions to which respondents must respond in their own words.

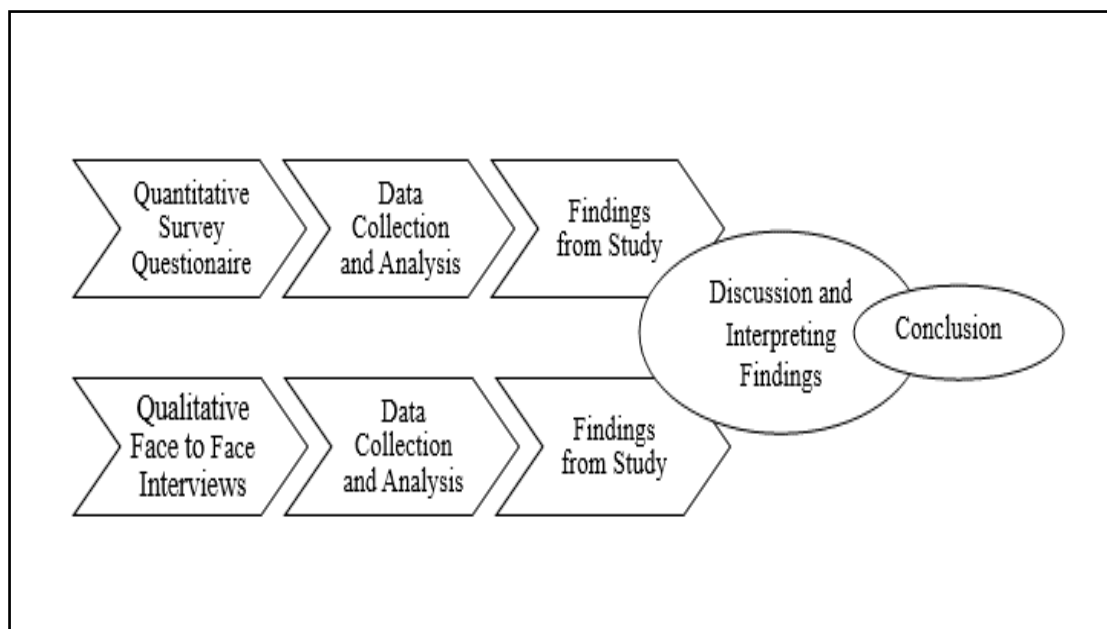


Figure 3.3: Data Collected Technique for Mixed Method Approach. (Eya, 2023)



The complementary quantitative and qualitative methodologies utilised to develop good reports are driven by the research question and study aim. The most successful approach of combining components of both methodologies in a single study is the mixed-methods research plan. The next section goes over the quantitative technique, which is part of the data collection procedure.

### **3.3.1 Quantitative Techniques**

The quantitative research approach differs depending on the investigation's goals. It is a great tool for gathering data from a range of sources and conditions. It is well-known and commonly used in social science research to examine intercultural and organisational challenges. Bond (1988), Cameron and Quinn (2005), Hofstede (2005), Schein (1992).

Survey research is "the process of getting information from a sample of people by asking them questions" (Hofstede (2005)). The questionnaire is a well-known way to find out what people think. It also helps researchers find and describe differences in events and investigate and explain relationships between variables. (Saunders et al. (1997)). It is a "successful way to get information from a lot of different people and social situations. Also, Saunders et al. (1997) say that questionnaire-based survey research is usually the only way to get a good picture of the attitudes and traits of a large group of people. In quantitative research, data from many people is collected, grouped together, and used to draw conclusions. Its main goal is to show a phenomenon and how common it is in a population. Academic psychologists like to use quantitative methods, such as measuring and analysing important variables.

Positivists believe that there is a single, measurable, and known reality, and they want to use quantitative methods to measure this reality. (Shuttleworth (2008)). A quantitative perspective is based on the positivist paradigm and is hypothesised and co-deductive in that it often starts with a research assumptions or research questions based on a review of the literature. Quantitative research is done with the help of

questionnaires, experiments, and mathematical modelling. Myers and Avison (2002) use math and statistics to find facts and connections between ideas in a certain field.

Shuttleworth (2008) says that quantitative methods have been used for thousands of years to finalise data and prove or disprove theories. After the data has been analysed statistically, a thorough answer is made, and the results can be argued and published in a good way. It gives proven data with less uncertainty, which leads to a clear conclusion and fewer possible directions for more research. Quantitative research, in contrast to qualitative research, examines quantitative phenomena using quantitative methodologies (methods that measure and examine the relationship between numbers, weights, quantities, volumes, and strengths to support specific questions or hypotheses). (Carr, 1994). In the form of a research question, quantitative research must first come up with a specific assumption about a given issue. Creswell (2003) says that researchers use research questions and assumptions to describe the purpose and goals of quantitative studies more accurately. (Creswell, 2003). Denzin (2000) says that quantitative research looks at how variables cause each other, not how processes cause each other. Investigations and epidemiological studies are examples of quantitative research methods (e.g., incidence, prevalence, and risk studies). Creswell (2003) say that quantitative methods give results that are scientifically sound and can be used to make changes or take action.

There are three types of quantitative research: descriptive, experimental, and comparing causes. Leedy and Ormrod (2001) say that the descriptive research method looks at how things are right now. In descriptive research, you try to figure out what something is like by observing it or looking at the connections between two or more events. Quantitative statistics don't tell us much about attitudes, behaviours, or what drives people, but they can be used to make generalisations because they are based on sample sizes (Williams, (2000).

Quantitative research usually looks through a limited lens because it usually only looks at one or a few causes. A questionnaire, which is a common tool in quantitative research, was used to get the results of this study. In this study, a questionnaire was

used to find out what the research participants believe about the attributes of the proposed approach for the implementation of a cloud-based ERP systems within an enterprise, putting into consideration the security responsibility of the enterprise end-users.

#### **3.3.1.1. Design of the Quantitative Method**

A questionnaire is a great way to find out how two or more variables that are based on positivist assumptions are related to each other. In quantitative research, a survey questionnaire is often used to collect data and make a numerical description of trends, attitudes, and views of the target population about a certain topic. Neuman (2006, p.272), argues that questionnaires are "the most common way to gather data in the social sciences. In several ways, the survey results backed up the main idea. It was used to find out what the research participants believe about the attributes of the proposed approach for the implementation of a cloud-based ERP systems within an enterprise, putting into consideration the security responsibility of the enterprise end-users. This was done by looking at how the respondents felt about the attributes of the proposed approach.

#### **3.3.1.2. Design of a Survey**

The survey for this study was made to be as unobtrusive as possible because cloud computing security is a sensitive subject in organisations. The questionnaire was six pages long, with fifteen questions. Most of the questions were closed-ended, but the last section asked for an open-ended comment where participants were asked to write down their own thoughts, ideas, and any other information that justify the response they provided. The participants ranked the items on a 5-point Likert scale with the anchors "Definitely Agree, Probably Agree, Might or might not Agree, Probably Disagree, and Definitely Disagree." This scale was made to measure key different attributes of the proposed implementation approach. Before starting the survey, the questionnaire starts with a statement of agreement to take part, which shows that taking part is optional. The permission statement also says what the goal of the study is and how long the survey needs to be filled out.

The primary objective of this study was to validate or refute the position taken in the proposed implementation approach for the adoption of a cloud-based ERP systems in enterprises and to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. To accomplish this goal, the following research questions must be answered: To what extent is the Impact of Cloud Computing on Enterprise Data Security in the Cloud? How critical are an end user's security responsibilities when it comes to cloud data security? How critical is end-user access control in ensuring the security of enterprise data in the cloud? To what extent can cloud-based enterprise database fragmentation enhance the enterprise data security of a cloud-based ERP software system within the enterprise? Is data security a significant consideration when implementing a cloud-based ERP system?

By using the aforementioned questions as a guide for collecting data that will be used to validate or refute the views expressed in our proposed framework, we were able to generate multiple hypotheses about what an ideal situation might be. The assumptions are based on literature reviews and our conviction that, in such a situation, it would be ideal. The research assumptions are showed in the Table 3.2 above, it covers the different assumptions that arose from considering how the proposed framework will improve enterprise data security in the public cloud when implemented. It considered the various attributes of the proposed framework and assumed the benefits of these attributes. Assuming all the above assumptions apply to an ideal cloud-based ERP system, it has led us to create sub-questions to review these assumptions. When reviewing research assumptions, it can be helpful to break down the examination into sub-questions that target different aspects of the assumptions. These sub-questions aim to prompt a thorough examination of research assumptions across various dimensions, ensuring that researchers critically evaluate the foundational principles guiding their study.

*Table 3.5: Research survey questions and the research assumption it is addressing, and the type of data response collected*

<b>No</b>	<b>Survey Questions</b>	<b>Research Assumption Addressed</b>	<b>Type of Response Option</b>
<b>SQ1</b>	How many years have you worked in your current role?	A1	Demographic Multiple Choice
<b>SQ2</b>	Do you currently work with a Cloud-based ERP system in your enterprise?	A1	Demographic Multiple Choice
<b>SQ3</b>	Cloud Computing has an impact on Enterprise system data security. To what extent do you agree with the above statement?	A2	Likert Scales and Open-Ended
<b>SQ4</b>	The security responsibility for a Cloud system within an enterprise; should be a shared responsibility between the Cloud Service Provider [CSP] and the Cloud Service End-users. (Cloud Service End-user is the enterprise employees who use the enterprise system to work.) To what extent do you agree with the above statement?	A3	Likert Scales and Open-Ended
<b>SQ5</b>	In your opinion, is it okay to ensure that no single system end-user (including the CEO and the System Administrator) has access to all the Enterprise data set in the Cloud storage?	A4	Likert Scales and Open-Ended

<b>SQ6</b>	How important is your job description and responsibility, in determining the level or type of system access given to you in your enterprise system?	A4	Likert Scales and Open-Ended
<b>SQ7</b>	Do you agree that, when a single system end-user has access to all the Enterprise data set in the Cloud, this may increase the Enterprise's chances of suffering a successful cyber-attack?	A4	Likert Scales and Open-Ended
<b>SQ8</b>	End-users of a Cloud-based ERP software system should hold some security responsibilities to ensure the security of their Enterprise Data in the Cloud. Do you agree with this statement?	A3	Likert Scales and Open-Ended
<b>SQ9</b>	How important is End-user Access Control in ensuring Enterprise data security in the Cloud?	A4	Likert Scales and Open-Ended
<b>SQ10</b>	To manage Access Control, Cloud service providers keep a directory known as "CSP Access Directory"; this is a database of all the Cloud end-users and their passwords which is used in authentication each time an end-user accesses data in the Cloud. Do you agree that the "CSP Access Directory" would improve access control management in the Cloud?	A4, A5	Likert Scales and Open-Ended

<b>SQ11</b>	Enterprise data set classification is a process of classifying enterprise data sets against key roles and responsibilities of their end-user, which will determine the level of access each end-user will have and the data that they can access in the Cloud. Enterprise data set classification: should happen as an integral process of the enterprise preparations to move the enterprise data to the Cloud. Do you agree with the above statement?	A6	Likert Scales and Open-Ended
<b>SQ12</b>	Enterprise Database Fragmentation is a feature of a Cloud security model that suggests that Cloud service providers should store the enterprise data set in fragments and implement access control for each fragment of the database. Do you agree that Enterprise Database Fragmentation in the Cloud would improve enterprise data security of a Cloud-based ERP software system?	A8	Likert Scales and Open-Ended
<b>SQ13</b>	An Enterprise system that prompts the Enterprise System Administrator when there is an unsuccessful login attempt, is more likely to promote Enterprise data security in the Cloud. Do you agree with the above statement?	A1, A7	Likert Scales and Open-Ended

<b>SQ14</b>	The set of policies, procedures, technology and controls that functions jointly to safeguard the Cloud-based system, infrastructure and data are known as Cloud + Model. Based on the above definition, Does the current Cloud Security Model available in your Enterprise meet all your Enterprise needs for data security in the Cloud?	A1	Likert Scales and Open-Ended
<b>SQ15</b>	From your experience, do you consider data security a major concern when your enterprise is adopting a cloud-based ERP software system?	A1	Likert Scales and Open-Ended

The relationship between the different research assumptions and the research survey questions is shown in Table 3.5 above. It also shows what kinds of answers were given for each of the research questions. For example, the SQ10 will answer the research assumptions A4 and A5 and will be a Likert scale and open-ended question. In the paragraphs that follow, we explain why each of the research questions we used in our initial study to get secondary research data are important. It starts with the question, and then it explains why that question is being used.

### **3.3.1.3 The Quantitative Approach**

Qualitative research is defined as an activity designed to collect non-numerical data. The data collected may take the form of audio recordings, video clips, or written text, among other formats. This type of data enables the researcher to gain a thorough understanding of the researched concept through the participants' opinions or experiences (Sofaer 1999). By contrast, a quantitative research method entails the collection of numerical data or any other quantifiable data set. It is primarily concerned



with analysing data sets to discover patterns and always quantifies its findings of the larger research sample size. Quantitative research is most effective when making predictions and examining relationships between variables. (Osborne (2008) According to Saks and Allsop (2012), combining qualitative and quantitative research methods results in a better understanding of concepts, particularly when human subjects are involved, as demonstrated by research in the health sciences. This bore a striking resemblance to our research, as we sought to understand our participants' perspectives on our proposed implementation framework, which was developed to address concerns about a lack of end-user participation in their enterprises' cloud data security. We reasoned that combining qualitative and quantitative methods, dubbed "mixed methods," would enable us to gain a better understanding of our participants' perspectives on the proposed implementation framework. With the end goal of obtaining participant feedback on the attributes of our proposed implementation framework, we recruited research participants by visiting the companies listed below. The following paragraphs discuss the benefits and limitations of a quantitative research methods.

#### **3.3.1.4 The Quantitative Approach's Advantages and Limitations**

Some of the quantitative method's advantages and disadvantages are listed below.

##### **Advantages of the Quantitative Method:**

- The quantitative approach allows for the collection of information from a reasonably large number of individuals.
- Because a large, semi-randomly selected sample is used, the quantitative findings can be generalised to a whole population or a subpopulation.
- Data analysis takes less time since statistical tools such as SPSS is used.
- Analysis of multiple groups enables comparison.
- The use of standardised questions enables easy comparison of respondents and groups of respondents.
- Results with greater impartiality and precision. In general, quantitative approaches produce data summaries that support generalisations about the topic under investigation.

- Conducted remotely, which lowers or eliminates geographical constraints. Quantitative approaches are useful for data collection since surveys may be sent to participants in several ways, such as e-mail or WhatsApp, or over the Internet. The online survey approach is becoming the most common means to collect data from target participants. Researchers can collect data from people across the world.
- Statistical tools are used to determine associations between variables. Advanced statistical approaches may be used with quantitative methods to analyse survey data, determining validity, reliability, and statistical significance.
- Personal prejudice or opinion is avoided. Quantitative approaches offer all participants with a uniform stimulus, allowing huge groups of individuals to submit information free of the researcher's opinion.

### **Limitations of the Quantitative Approach**

Beside the benefits that the quantitative method provides, there also some limitations as listed below:

- Difficulty recognising new and unexplored phenomena.
- The quantitative method overlooks respondents' experiences and perspectives in highly controlled settings. (Silverman (2010))
- The lack of a direct connection between researchers and the participants when collecting data, results in a degree of objectivity in collecting data.
- Improper representation of the target population might hinder the researcher. Despite attempts at rigorous sampling, the representation of the subjects is dependent on the probability distribution of observed data. This may lead to miscalculation of probability distribution and lead to false propositions.
- Quantitative research methods use structured questionnaires with close-ended questions. This can limit outcomes outlined in the research proposal. Results may not always represent the actuality in generalised terms. In addition, response options are limited to the question selection made by the researcher.

- Inability to control the environment. Sometimes researchers face problems controlling the environment in which respondents provide answers. Silverman (2010). Responses often depend on particular time and the conditions occurring during that particular period.

### **3.3.1.5 Sample of the survey**

Bell et al. (2018). said that the information gathered from employees of different organisations of different sizes was a good mix. The study's survey was meant for people who work in the IT sectors of various enterprises. As the sampling was targeted at IT professional, majority of the people who filled out the survey worked in the IT sector with at least a minimum of few months experience. There was a good mix of small, medium and large enterprises from our respondents.

The study's target or ideal research participants have experienced information technology professionals with some experience working with both traditional and cloud-based ERP systems. To reach the targeted population, we recruited participants in two ways: first, by directly contacting identified and well-known IT professionals via email; second, by recruiting participants on LinkedIn, considering their job profiles; and third, by sharing our survey invitations via professional LinkedIn groups. This strategy worked well, albeit not as quickly as we anticipated, but gradually we recruited high-quality research participants for our study.

The initial sample size is approximately 80 participants via direct email and six shares on various cloud computing LinkedIn groups. The response rate was approximately 23 responses per week during the first two weeks. This was an inadequate sample size in light of our initial sample size. We emailed reminders to research participants and reshared survey links on the six LinkedIn groups in which we conducted our research. We chose to extend the research period in order to recruit a larger sample size. By the end of the eight weeks, we'd received 43 responses. It was safe to proceed to the next stage of the research at this point.

To ensure that research participants met the criteria, a demographic question was included, which helped screen out responses from participants who lacked IT work experience and had limited familiarity with cloud-based ERP systems. During data cleaning, priority was given to responses from experienced IT professionals. This is because they are on the ground and are therefore more likely to provide useful feedback on the proposed implementation framework's attributes. 43 professional-quality opinions on the proposed implementation framework's viewpoints provided a solid foundation for proceeding to data analysis. The decision to contact participants directly via email and to share on LinkedIn groups may have increased the rate of no responses by more than 50%. This can be attributed to a variety of factors, including outright disregarding emails, or neglecting to check one's email or LinkedIn profile during the research period. It would have been preferable if the researcher had been able to meet the research participants or participating enterprises physically, but this was not feasible at the time of the research due to the global pandemic.

### **3.3.1.6 Survey Distribution**

After sampling, the survey was sent out to everyone. The "Qualtrics" online survey design tool was used to make the questionnaire and collect data for the independent and dependent variables used in the research assumptions. Qualtrics is a free online tool for making surveys and collecting data. It lets researchers make surveys and get answers from specific samples. Qualtrics uses encryption to keep data safe and keep information private. The data is protected by a password. The person who owns the survey must enter a security code to get into it. The information is stored in encrypted internet files that only the researcher can see. All electronic research data is kept in an online survey tool that is connected to the internet through a secure connection. This information is erased from all discs after a certain amount of time. For data security, all hard copies of data will be thrown away.

Most participant got an email encouraging them to fill out the survey, and Qualtrics sends a thank-you note to each participant after the survey is done. Qualtrics told the

researcher that a new questionnaire had been filled out. Qualtrics made it possible for everyone to access the survey at the same time, no matter where they were in the world. It also cut costs and led to a higher response rate. Before the data were collected and looked at, the online survey was open for eight weeks.

### **3.3.1.7 Survey Data Collection and Coding**

Qualtrics's data was transferred and encoded in Excel, therefore it had to be quantified. The researcher cleansed and checked for missing data before uploading it to SPSS v22. SPSS can efficiently code, retrieve, and store survey data. It categorises, organises, and analyses data. The data was double-checked by humans to ensure SPSS accuracy. Before analyzation, the researcher checked the amount of valid and missing occurrences and variable labels.

Data cleansing eliminated surveys with too many unresolved questions. To improve survey reliability, the researcher replaced unanswered questions with zeros. No questionnaires were deleted in this study since most data fields were completed. The cleaning procedure replaced a few missing replies with zeros. SPSS provided fast, accurate results.

All survey questions were answered using a 5-point Likert scale: "Definitely Agree, Probably Agree, Might or might not Agree, Probably Disagree, and Definitely Disagree." This scale was made to measure key different attributes of the proposed implementation approach. Response coding was done using reverse-scoring before statistical testing and analyses. The first thing we did was to map the research questions against the research assumptions they are addressing, and also, we coded our Likert scale responses using 1, 2, 3, 4, and 5, as shown in Table 5.17 in section 5.2 of chapter 5, where 1 represents a negative not agreeing with the view, 3 is neutral, and 5 is a positive strong agreeing with the view. In many questions, the wording is different, but the coded number always carries the same meaning. This strategy increases research credibility and follows best practises.

### **3.3.1.8 Survey Data Analysis**

Data was analysed using the Excel and SPSS program. Descriptive research data understanding, and it contains a summary of each of the research questions as well as the data collected. We used a bar chart to virtualize the responses received for each research question. The statistical data analysis of our research assumptions is the second part where the researcher used SPSS to analyse the data gathered to see if the attribute of the proposed implementation's framework is supported or not. The tests of normality, ordinal regression, the test of parallel lines, and non-parametric correlations were performed and represented here by tables and more details with charts can be found in the Appendix 5.

The data was analysed using the SPSS programme. Table 5.16 in chapter 5 shows the research assumption variables and how they are related to the research SQs variables. Here, the primary variables are the SQs variables, while the secondary variables are the assumption variables. Under the assumption variables, A1 is the dependent variable, while A2 to A8 are the covariant variables. A1 is the dependent variable because this is the variable that addresses the assumption that participants who have worked with a cloud-based ERP system are more likely to provide a valid response to our research survey.

### **3.3.2 Qualitative Techniques**

Qualitative research is concerned with "the study of things in their natural environments, to try to understand or interpret [an event or experience] based on the senses that people give" (Denzin 2000 pp. 256-265). Qualitative methods are characterised by their interpretive practices and their focus on meaning-making and building concepts. Interviews are the most widely employed method in qualitative research, as they allow participants to give their personal experiences rather than relying on numbers. There are three main categories of Interviews: the structured,

semi-structured and unstructured. A structured interview consists of fixed questions and all respondents receive the same interview stimulus.

An unstructured interview is guided only by a list of topics or issues to be discussed and there is no specific sequencing of questions. Qualitative methods are appropriate for social science research, particularly when studying individual and group behaviour in an organisation (Yin, 2014). Qualitative research is interpretive in nature and focuses on words, not numbers; it analyses the data to search for themes, patterns, and holistic features. Since it is dependent on the context, reliability is limited since this is a single case study. Glesne and Peshkin (1992) note that multiple methods need to be used by researchers in qualitative studies to understand, describe, and make sense of the research.

#### **3.3.2.1. Design of an Interview Guide**

The interview, according to Lee and Fielding (1991), is one of the most essential sources of qualitative data collecting. Interviewing is a data collection technique in which selected individuals are asked questions to learn what they do, think, or feel. According to Denzin and Lincoln (2011), interviews are regarded as the major data gathering technique in qualitative research. During the data collecting process, an interview guide or questions for this initial study was created based on the associated work review, the researcher's understanding of the issue, and her work experience. It offered some structure throughout the semi-structured participant interviews, as well as a link between the interview questions and their associated research topics.

The interview guide included 30 questions initially but was redesign to a more focus 15 questions. Each set of questions was centred on a certain topic title. The majority of the questions were designed to help participants understand the state of end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security in their enterprise, and the extent of employee

compliance with cloud computing information security best practises. The questions are also designed to extract the motivations for various data management security behaviours and data security policies adherence. However, as is typical of such flexible semi-structured interviews, the topics were merely used as a jumping off point, and participants were invited to express themselves freely.

The interview guide was made up of extensive and well-organized semi-structured open-ended questions that encouraged participants to provide thorough replies. Semi-structured interviews are defined as "a qualitative data gathering approach in which the researcher poses a sequence of planned but open-ended questions to informants." (Ary, et al. 2013, p. 811). The ability to add and edit questions, as well as offer supplemental prompts, is a significant aspect of semi-structured interviews. Furthermore, this sort of interview may be readily controlled to get the necessary information from interviewees within a certain time frame.

The interview guide included questions regarding the organization's present status of Cloud-based ERP system impact on enterprise data security, Data Management Security Policies, DMS policies and senior management end-user involvement in DMS policies, DMS policies and enterprise incentive policies, End-user skills and end-user roles, Employees' actions and security risks, Number of staff in your enterprise, Organization data security culture, Training programs and organization EIS regulations, EIS awareness programs and its effectiveness and End-user knowledge of cloud-based ERP systems.

The study information page, which offered information about the research in general and the interview in detail, was handed to each participant at the start of each interview. A consent form was also supplied to the participant to sign, acknowledging that he/she had read and understood the information page and accepted to participate. The interviews were then conducted with the participants' agreement for further study of processing the data collected.



### **3.3.2.2. Qualitative Approach Advantages and Limitations**

When sensitive themes are being discussed, qualitative research is ideal for gathering data on persons, their histories, viewpoints, and experiences. In qualitative research, interviews are typically broad in scope, investigating problems in depth. The researcher invites people to express themselves fully. These are typical Qualitative research advantages. It did, however, come with certain drawbacks.

#### **Benefits of Qualitative Methods**

- Designed to elicit detailed information and are useful to a study of social processes.
- Qualitative methods are often face-to-face, allowing researchers to make observations beyond respondents' oral responses.
- In-depth interviews provide very rich information and offer the opportunity to ask follow-up questions, probe additional information, justify previous answers, and establish a connection between several topics.
- Statistical measures can be used to extract more meaning from a qualitative data set, as certain of these data sets will lend themselves to transformation or translation into quantitative data sets.

A researcher using this approach may delve considerably deeper into a topic than a researcher using a quantitative method. It allows participants to expound in ways that survey research does not allow, and they are allowed to share information with researchers in their own words and from their own viewpoints rather than being asked to fit those perspectives within the researcher's restricted answer possibilities.

#### **Limitations of Qualitative Methods**

- Cannot generalise to the general population. The data collected cannot be used to make assumptions beyond the current group of participants. This is because

the data collected is specific to how the current group of participants feel, think and behave.

- Silverman (2010) argues that qualitative research approaches sometimes leave out contextual sensitivities and focus more on meanings and experiences.
- The quality of research is heavily dependent on the skills of the researcher and can be easily influenced by personal idiosyncrasies and biases of researchers.
- A smaller sample size raises the issue of generalisability to the whole population of the research. A researcher faces the issue of applicability to the population as a whole when working with a small number of participants.
- Data interpretation and analysis may be more difficult/complex.

### **3.3.2.3 Justification for Using Semi Structured Interviews with Open-Ended Questions for Qualitative Data Collection**

The main advantage of the qualitative technique is that it fills holes in the questionnaire method and improves the research's validity and reliability. Tashakkori and Teddlie (2003); Creswell and Clark (2007). Furthermore, according to Brenner, Brown, and Canter (1985), the fundamental advantage of interviews as a data gathering tool is that they allow both sides to examine the meaning of the questions presented and the responses offered. Furthermore, the interactive character and immediacy of face-to-face interviewing give significant flexibility in terms of the direction of the discussion and the themes discussed. (Creswell and Clark (2007). Interviews, according to Creswell and Clark (2007), provide the researcher with rapid replies to queries. They can provide rich and detailed data as well as insights on topics that the researcher has never considered before.

Because the study employs a mixed-methods approach, the researcher had predetermined themes to discuss with participants, in addition to soliciting in-depth responses to questions. In addition, the researcher might use an investigative framework or interview guide to direct the interviews. As with numerous other information security researchers, such as (Doherty et al., 2012). While open-ended inquiries offer the benefit of allowing the respondent to react in an unfettered manner.

This style of inquiry gives the reply to the gratification of giving finer information, which might be more motivating. Semi-structured interviews with open-ended questions are a popular method for qualitative data collection, offering flexibility, depth, and a participant-centred approach. These questions allow participants to express themselves freely, providing in-depth insights. They are effective for exploratory research, understanding context, tailoring questions based on individual responses, building rapport, and providing a robust foundation for thematic analysis.

### **3.3.2.4 Organizational Selection for Interview**

The researcher should carefully consider interviewee selection and not depend on chance or opportunity (Bell et al., 2018). The emphasis should be on the human aspects of the adoption of cloud-based ERP, rather than on technology issues. This requires exploring the culture of the organisation to understand the employees in their work surroundings while collecting the data required for the study.

The interviewees were chosen based on the following criteria:

- To find people from enterprises that have recently started using cloud-based ERP systems.
- To include people from SME enterprises with a lot of employees in order to find out how human factor and enterprise culture affects how people act in these kinds of organisations.
- To find people who work for SME enterprises that are considering the adoption of a cloud- based ERP system.

These different types of organisations helped find the key human-factor and organisational drivers and barriers to adopting a cloud-based ERP system.

#### **3.3.2.4.1 The Initial Studies as a Qualitative Data Collection Technique**

A initial study is necessary to assist the researcher in discovering any problems in the research instrument. Excellent questionnaires, according to Altman et al., (2006), need a initial study. A initial study, according to Johanson and Brooks (2010), is an ideal

strategy for designing an appropriate research instrument and evaluating the dependability and validity of the research assumptions. A initial study was undertaken prior to distribution of survey to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. The researcher communicated various enterprise in Nigeria to participate in the initial test: two enterprises from the oil and gas private-sector organisations participated. The researcher sent the participating enterprises an email and visited them to seek their consent to take part in the research. More details of initial study can be found in Chapter 6 section 6.5.

Qualitative research is defined as an activity designed to collect non-numerical data. The data collected may take the form of audio recordings, video clips, or written text, among other formats. This type of data enables the researcher to gain a thorough understanding of the researched concept through the participants' opinions or experiences (Sofaer, 1999). By contrast, a quantitative research method entails the collection of numerical data or any other quantifiable data set. It is primarily concerned with analysing data sets to discover patterns and always quantifies its findings of the larger research sample size. Quantitative research is most effective when making predictions and examining relationships between variables (Osborne, 2008). According to Saks and Allsop, (2012), combining qualitative and quantitative research methods results in a better understanding of concepts, particularly when human subjects are involved, as demonstrated by research in the health sciences. This bore a striking resemblance to our research, as we sought to understand our participants' perspectives on our proposed implementation framework, which was recommended to address concerns about a lack of end-user participation in their enterprises' cloud data security. We reasoned that combining qualitative and quantitative methods, dubbed "mixed methods," would enable us to gain a better understanding of our participants' perspectives on the proposed model.

With the end goal of obtaining participant feedback on the attributes of our proposed model, we recruited research participants by visiting the companies listed below. The following paragraphs discuss the profiles of companies that the researcher visited in Nigeria during the first stage of the initial study to recruit participants. These businesses were chosen for their accessibility and size of operation. They are primarily SMEs enterprises with the financial means to implement an ERP system if they do not already have one. All the companies are based in Nigeria and have experience in oil and gas logistics. Although two enterprises participated in our initial studies, both companies declined to continue participating in the research, owing to their closure or disruption of business as a result of the pandemic at the time of data collection for the main study.

The initial study research process was divided into four distinct stages. The first phase was the investigation, which included a review of the literature, consultation with supervisor and the identification of theories. The investigation phase typically refers to the initial stage of a study where researchers explore and gather information to understand the background, context, and relevant literature related to their research topic. This phase is crucial for defining the research problem, formulating research questions or hypotheses, and establishing a solid foundation for the study.

The second phase was prioritisation, which involved classifying which aspects of the human factor are critical for cloud data security, as well as analysing the gap between current data management security models and the human factor's impact on cloud data security. This phase began the process of proposing an ERP implementation framework for a cloud-based ERP in the public cloud, based on literature reviews and gap analysis, but we needed to conduct the initial study to have a clear understanding of the concepts. The proposed implementation framework, which considers the trust relationships between cloud service providers and cloud service end-users, shaping the deployment of cloud services to ensure reliability and security. By addressing trust relationships, it aims to establish a foundation for effective collaboration and risk management in the cloud computing ecosystem. The proposed framework will then be

evaluated in the following stage of the research exercise using a qualitative and quantitative data collection method.

The final stage the initial study will be to examine how the finding from the study can shape the design of the main study and how the information gathered will be analysed to convey its useful information. The final stage of an initial study is crucial for shaping the design of the main study and planning the analysis of gathered information.

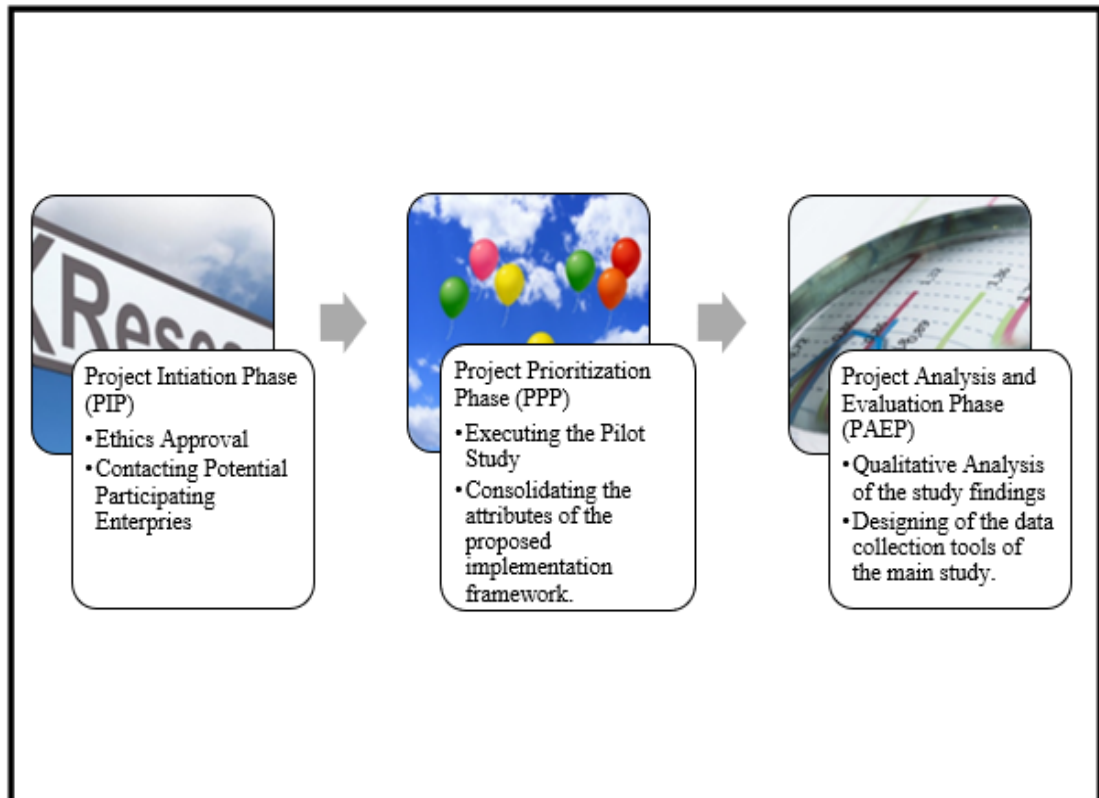


Figure 3.4: Phases of the Initial study research activities (Eya, 2023)

Figure 3.4 illustrates the various phases of initial study, as well as the research components and activities used at each phase. It is acceptable to note that our research was viewed from the start as a project with a timeline for completing each phase. Although the timeline was not rigid, we discovered that due to unforeseen circumstances, some of which are beyond our control, each phase of the research exceeded the initially planned timeline, although this did not affect the quality of our research findings.

### 3.3.2.5 Interview Sampling

In qualitative research, selecting appropriate respondents is a critical and challenging topic. The researcher purposefully chose persons considered to have a supervisory role at the organisational level within the targeted organisations to gain a better knowledge of the present status of end-user security responsibility in ensuring enterprise data security in public cloud. It was intended to elicit their perspectives through semi-structured qualitative interviews using open-ended questions. Purposive sampling is used by researchers to pick research participants who match defined criteria and are assumed to be representative of the study community. Although educational level also played a role in participants selection.

*Table 3.6: Interview Sample for participating enterprises*

Category (Respondents)	Number and Respondent
Total Number	20
Respondent Number Analysed	9
First Enterprise	5
Second Enterprise	5
Specialization	Various
Nationality	Nigerians
Experience	Various

Enterprise supervisors and IT managers who had experience and knowledge in their fields were chosen to be interviewed. Before doing interviews, the researcher knew that few supervisors and managers might be willing to talk about human factor and cloud computing security issues in their companies, even though the researcher had promised not to tell anyone. The table 3.6 above shows the interview sample for participating enterprises.

### 3.3.2.6 Interview Data Collection

Each participant had a face-to-face, semi-structured, open-ended interview. The researcher was able to communicate with respondents, allowing them to elaborate on their responses in order to gain more relevant insights into the study topics.

Respondents might also discuss the subject in their own words. They were each supposed to openly answer the interview guide's questions. The semi-structured interview was used to grasp the world from the participants' perspectives. The semi-structured interview also allowed participants to convey a thorough comprehension of the subject (Carr, L. T. (1994)

The respondents were mostly supervisors and managers from two enterprises. They were questioned in order to obtain their impressions of the end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. Respondents were asked to provide facts as well as their perspectives on occurrences. An interviewee's function in the research might fluctuate between respondent and informant depending on the conditions. According to Rubin and Rubin (2005), each conversation in qualitative interviews is unique, since researchers adjust their questions to what each respondent knows and is ready to offer. Notably, this study is concerned not only in the views of participants toward the issue at hand, but also in the organisational reality in which these people function.

As a key component in qualitative data collecting, the researcher's primary method was to employ open-ended questions to create credibility and trust with participants. To find an appropriate interview time and location, all ten participants were contacted. All interviews took place at the interviewee's workplace. Conducting research in participants' natural environs is vital... since the richness of human interaction is available only in the settings of ordinary life (Rubin & Rubin (2011). The interviews were done over a two-week period, with each session lasting between 30 and 45 minutes. Five interviews were conducted in each of the participating enterprise. While listening to the recorded voice, the recorded talks were manually transcribed. During the interview, the researcher first told the participants about the aim of the interview, the study subject, and the length of the interview. Before beginning, the researcher acquired permission to take notes and voice record each interview. The researcher also



advised the participants that they might terminate the interview at any time. Following that, participants were requested to sign a consent form promising confidentiality.

Except for one participant, everyone consented to have their interview digitally recorded to guarantee minimal inference reception, which aided the transcribing process later on. In one unique situation, the researcher documented the interview by taking thorough notes focusing on capturing the meaning expressed by the subject rather than a word-for-word transcription. (Stake, 1994). Voice recordings of interviews, according to Ali and Yusof (2011) are more dependable and accurate than written records. Writing notes can disrupt the interviewing process, and notes prepared later are likely to leave out certain facts.

In addition to audio recordings, field notes were utilised to capture major themes, noteworthy points, researcher perspectives, and ideas for future interviews. Immediately following each interview, the researcher completed the interview guide with a description of essential points on each topic asked, noting any items skipped or overlap. During the interviews, each participant was given a list of the same pre-prepared set of questions (interview guide), and the researcher asked the same set of questions to each participant to keep the session on course. (Doyle et al. (2009). Although the themes frequently overlap, the inquiry topics that prompted the interviews are later used as theme headers in the analysis portion.

During the interviews, the researcher effectively employed a variety of tactics and strategies, including probing, direct, and interpretative questions, to ensure a deep dive into the respondents' experiences. These interview strategies yielded rich and thorough data, as well as encouraged participants to participate more and contribute higher-quality information. (Anderson and Jack (2015). The researcher employed a neutral tone of voice and let the respondents use their own words and phrasing while answering questions to maximise the usefulness of the interviews. By not displaying any evident emotional reactions to comments, the researcher avoided changing interviewees' responses. To ensure a more trustworthy relationship to the study themes,

the researcher framed questions to retain an open-ended interviewee answer and asked related questions that promoted further responses. (Mayoral et al. (2022).

The researcher would say the following about the interview: For most of the participants, the interview was a friendly way to collect data and an easy way to draw conclusions from the answers. (Mayoral et al. (2022). The researcher also found that the interview data were very specific. there were some clear similarities in their experiences and views. all participants, as well as uniqueness. Even though each person's own experiences or thoughts about the concept or event was subjective, there were some things that everyone agreed on. showed that a lot of people had similar experiences and interpretations. After the interviews, the researcher added the information to what was already known about the state of end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria.

### **3.3.2.7 Interview Data Analysis**

Data analysis is critical because it combines the researcher's interpretation of her findings with what the participants reports. The data was analysed by the researcher to find links, patterns, ideas, themes, and meanings using thematic analysis method. Initially, the researcher concentrated on the data, then examined each component in detail and tried a more meaningful restructure. The researcher was able to compare and contrast patterns using NVivo software to collect themes in codes, as well as think carefully on specific patterns, after grouping the data in this manner. According to Denscombe (2014), there are several ways for doing qualitative data analysis based on interpretations, including thematic analysis, content analysis, grounded theory, discourse analysis, conversation analysis, and story analysis. Yin (2014) advises the researcher to address three aspects of interview analysis in order to gain strong evidence from in-depth interviews: Sort interview data into different headings and subheadings based on the goals of the interview, giving each interview a unique code that can be used for reference and summarize each category and add up the totals. This

method of analysing qualitative data makes it possible to gather a lot of information about the thing being studied.

#### **3.3.2.7.1 Thematic Analysis of Interview Data**

"Thematic analysis" is widely accepted and used in cloud computing security research. The thematic analysis method looks for patterns in data, interprets them, and groups them in a way that makes sense (Bryman et al. (2008). The researcher conducted a manual examination of the nine-interview data on various perspectives about the end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. Miles and Huberman (1994) advocate three steps for data analysis: data reduction, data display, and conclusion.

The pieces of interview text data were first thoroughly read, highlighted, and then placed in the categories to which they belonged, based on the interview guide's thematic categorisation using NVivo. The interview guide utilised in this study included questions designed to elicit respondents' ideas and understanding of the "reality" of implementing a cloud-based ERP systems and the end-user security responsibility in ensuring enterprise data security in public cloud. Each respondent was assigned a code number to assist the researcher in disseminating the discovered data from the interviewees' responses. Thematic content analysis enabled contextualization and the formulation of theoretical interpretations that might support and illuminate the study results. Quotations have been chosen to provide the reader with a better understanding.

#### **3.4 Validity, Reliability, Repeatability**

The validity of the research findings is related to the extent to which the data can be generalised and how relevant and applicable it is in other frameworks (Onwuegbuzie and Johnson, 2006). The greater the expected validity, the more objective and

consistent the data analysis. This is dependent on the methodology chosen, which handles greater reliability when retained systematically and accurately. Furthermore, it is critical that the data analysis and research findings are logical and distinct, and that they are accurately presented with a rational relationship to all concepts. This level of data analysis quality ensures not only reliability but also repeatability (Hardwicke et al., 2018). In other words, given a similar setting with homogeneous team members, the outcome and research findings would be very similar. This study believes that using a mixed methodology ensured validity, reliability, objectivity, and credibility while also ensuring repeatability.

### **3.5 Ethical Consideration**

At all times during any research exercise, ethical standards must be considered and adhered to. This is because research ethics ensures that all research participants are protected and not exploited at any point during the research process. It always ensures the confidentiality of research participants. These were conducted with consideration for the potential impact of the research findings on the participants or even the businesses in which they worked. Throughout the research exercise, the most critical ethical consideration was the confidentiality of collected data. All processing will be conducted by the Data Protection Act, and no personally identifiable information will be published. The research activities were conducted following the University of Strathclyde's ethical policies. A consent letter and an introductory letter to the research were provided to research participants, outlining the types of data we will collect and how they will be processed and stored throughout the research. Participants were assured that their personal information would be protected and would be deleted after the research.

### **3.6 Summary of Chapter 3**

This section of the thesis summarised the research methodology. Numerous uncertainties were raised throughout the research exercises, beginning with the initial study and ending with the main study. These uncertainties came from a variety of sources, including the participants, their enterprises, the enterprises' expectations of

the research, and the pandemic, all of which introduced some level of risk that needed to be managed. As a result, the study took a vigorous research approach, utilising a variety of techniques to collect both qualitative and quantitative data to answer the research questions and examine the proposed implementation framework's viewpoints. The research exercises included a literature review, initial study interviews, gap analysis using parametric comparisons of cloud computing security models, and the proposing of an end-user centred implementation framework for a cloud-based ERP system based on the public cloud. Following that, the research exercises incorporate concepts from well-established methods, such as sequential exploratory mixed methods design. The mixed-method approach bolstered the credibility, reliability, and validity of the research findings. We described in this section how both qualitative and quantitative data will be generated for the subsequent sections' data analysis. Additionally, we discussed how the final research questions were developed and justified, as well as the research question or assumption addressed by each question. We began by breaking down the research questions and the proposed implementation framework's various attributes into smaller questions that will be included in the questionnaire used to collect data. Following that, we discussed the various data collection tools we used and justified our sampling method selection. Finally, the ethical consideration, the validity, reliability, and repeatability of the research method used was also discussed in this section of the thesis.

## Chapter 4. End-user Centric Access Control Framework

This chapter of the thesis presents a novel End-user Centric Access Management Implementation Framework for enterprise systems running on public cloud infrastructures in section 4.3. The proposed framework discussed in this chapter is a significant contribution to knowledge made by our research. Additionally, this chapter compares the various cloud security models to our proposed framework in section 4.1. This chapter also discussed the strengths and weaknesses of cloud security models in section 4.2.

Numerous Cloud Computing Security Models are evaluated using parameters, with a particular emphasis on the model that addresses the data security challenges associated with cloud-based ERP systems. While all CCSMs share the goal of securing the cloud system, the Multi-Cloud Database Model (MCDM) is more focused on data protection in the cloud (Eya and Weir, 2021). The MCDM was reviewed to determine a method for incorporating end-user experience into the design and development stages. This thesis proposes a cloud computing security framework that incorporates Enterprise Access Directory (EAD), Enterprise Data Fragmentation (EDF), and End-User Access Quires (EAQ). Table 4.1 below gives a summary of the definitions of these attributes. This proposed approach is an updated version of the original MCDM, but the new framework takes the end-user role and responsibility into account when determining the level of access and data set to access in the cloud. Securing enterprise data requires that no single end-user has access to the entire enterprise cloud database in a single instance. The Table 4.1 below gives the definitions of the Enterprise Access Directory (EAD), Enterprise Data Fragmentation (EDF), End-User Access Quires (EAQ) and CSP Access Directory (CSP AD), where it is hoped that the table will give more clarity to the meaning of the attributes of the proposed framework dumped the end-user centric access control framework.

Table 4.1: Summary of Framework Attributes Definitions

Framework Attributes	Definitions
<b>Enterprise Access Directory (EAD)</b>	Enterprise Access Directory (EAD) is a database listing key roles, responsibilities, and data access levels for enterprise roles, serving as the primary end-user portal for cloud data access.(Eya and Weir, 2021).
<b>Enterprise Data Fragmentation (EDF)</b>	Fragmentation is a database server feature that controls data storage at the table level by defining groups of rows or index keys (Eisa et. al., 2017). It is proposed that after data classification, the CSP should provide enterprise database fragmentation for each set of enterprise data being moved to the cloud. (Eya and Weir, 2021).
<b>CSP Access Directory (CSP AD)</b>	This is simply a directory of cloud usernames and passwords maintained by the CSP to validate each time an end-user accesses cloud data (Kumari and Nath, 2018).
<b>End-User Access Quires (EAQ)</b>	The proposed cloud security framework uses a unique feature that enables Enterprise Cloud Administrators to trigger queries when end-users are denied access. These queries help determine the end-user's identity, which can then be used to add or update them to the Enterprise Cloud Directory. (Eya and Weir, 2021).

#### 4.1 Parametric Comparison of the various Cloud Security Models

A parametric comparison of various cloud security models involves evaluating different models based on specific parameters or criteria. To compare the cloud security models, we considered certain parameters. We intend to identify the unique characteristics and objectives of cloud security models and to compare them to the security technology used, the security responsibility, the security effectiveness, the security porosity, the targeted cloud feature, and the practicality. This parametric comparison should be tailored to the specific requirements and priorities of our research for instance the elements of CSM and the underlying technology it employs to deliver on its cloud security promises are described as the "technology used." Virtualization, layer dependencies, algorithm sharing mechanisms, and even something as basic as encryption are examples of security technology. The summary of the definitions of these parameters can be found below in Table 4.2 below.

Table 4.2: Summary of Parameters Definitions

<b>Parameters</b>	<b>Definitions</b>
<b>Technology used</b>	The “technology used” is describing the CSM features along the underlining technology it uses to achieve its cloud security promises. Security technology can range from virtualization, layer dependency, algorithm sharing mechanism, to something as simple as encryption (Eya and Weir, 2021); (Zarger and Chaturvedi, 2015).
<b>Security responsibility</b>	The "security responsibility" refers to the security sharing responsibility between end-users and CSPs in different Cloud Service Models (CSMs). In some CSMs, the end-user holds more security responsibility, such as IaaS (infrastructure as a service), while in SaaS (software as a service), the CSP holds more. The security responsibility of a CSM depends on the cloud delivery model it targets (Eya and Weir, 2021) ;(Chou, 2010).
<b>Security effectiveness</b>	The "security effectiveness" yardstick measures the effectiveness of Cloud Service Model (CSM) in securing cloud systems. "Averagely secured" indicates medium security, while "highly secured" indicates high security (Eya and Weir, 2021).
<b>Security porosity</b>	Security porosity refers to a CSM's vulnerability to attackers, indicating that malicious insiders can easily bypass security modalities, making it more likely for an attacker to gain access (Eya and Weir, 2021).
<b>Targeted cloud feature</b>	The "targeted cloud feature" identifies the specific aspects a CSM focuses on protecting in a cloud system. Some CSMs target data at rest or transit, while others protect network infrastructures and end-users. This feature helps identify which aspect of the cloud system a CSM is focusing on (Eya and Weir, 2021).
<b>Security practicality</b>	The "Practicality" yardstick helps identify different cloud security models (CSMs) based on their system-centred or user-centred approach. All models aim to secure cloud systems but differ in mechanism and preferred approach. Table 4.3 compares CSMs against these features to identify more user-centred models (Eya and Weir 2021).

Zarger and Chaturvedi (2015). The term "technology used" refers to the CSM's features as well as the technology that enables it to deliver on its cloud security promises. Virtualization, layer dependency, algorithm sharing mechanisms, and even something as simple as encryption are all examples of security technology (Sharma and Kaur, 2014). The term "security responsibility" is used to refer to the shared security responsibilities of the various CSM (Chou, 2010). It simply states who is more responsible for security in the various CSMs between the end-user and CSP. For some of the CSM, the end-user bears additional security responsibilities, as is the case with



cloud delivery models such as IaaS. (Infrastructure as a service). The need for adopting enterprise end-user to share a greater security responsibility in the SaaS delivery model of cloud computing have been identified by previous authors such as: Saa, Moscoso-Zea et. al., (2017); Ahmed and Kommos, (2012); Weli. 2021; Feuerlicht and Govardhan, (2010); Orosz, Selmeci et.al., (2019) and Al-Okaily, Alkhwalidi, et. al., (2022).

Saa, Moscoso-Zea et. al., (2017) reported that cloud computing has become the new trend in how businesses conduct themselves, allowing them to innovate and compete in a dynamic environment. Cloud-based ERP raises concerns about the security and integrity of data stored in the cloud. Small and medium-sized enterprises (SMEs) benefit the most because data security concerns do not apply a lot to them. Due to data security concerns, large organizations are more hesitant to move mission critical enterprise applications to the cloud. A hybrid solution is proposed, in which organizations can keep sensitive applications on-premises while reaping the benefits of the cloud.

According to Ahmed and Kommos (2012), cloud computing is quickly developing and expanding to encompass all internet services until it can incorporate business services like ERP systems offered via the cloud. Most businesses lack the analysis and understanding necessary to transfer their systems to the cloud; as a result, a comparative case study examining the advantages of adopting cloud-based ERP solutions was carried out. In cloud ERP solutions influence numerous areas of a firm, including cost and time savings, according to the comparative case study. Additionally, the cloud-based system is more interactive and user-friendly than the on-premises system, which motivates users or workers to perform more productively. In conclusion, Bring Your Own Device (BYOD) is best suited for businesses with a high level of cost and time sensitivity, indicating that in-house ERP implementation will be more expensive and time-consuming. Weli. 2021 stated that end-user computing satisfaction model (EUCS) has been extensively utilized in past research in Enterprise Resource Planning. Consequently, the Enterprise Resource Planning (ERP) system must be

created in accordance with cloud computing, which currently dominates information technology devices. His research goal was to re-examine the validity and reliability of the computer application satisfaction model and its association with user performance in cloud-based ERP systems. The author noted that majority of users are unfamiliar with cloud-based ERP systems, but they give the content, accuracy, timeliness, and format high marks. The low score for usability is due to the system's complexity especially around the clarity of their security responsibility. The author suggested that adopting enterprise end-user satisfaction component should be supplemented with measures of comfort, adaptability, and efficacy through additional research.

According to Feuerlicht and Govardhan, (2010) cloud-based ERP system adopting enterprise that do not worry about data security, service continuity, and being locked into one provider are likely to push for Cloud Computing. The rate of adoption is likely to be very different for different types of applications and industries. Small and medium-sized enterprises (SMEs) and start-ups will use cloud computing in many ways. The author stated that as IT industry grows up, vendors, end-user enterprises, adopting enterprise end-users and third parties will have to specialize more and change how they do things. The traditional enterprise computing model is no longer useful because of how fast and easy it is to connect to the Internet and how flexible computing platforms are. The author argue that Cloud Computing represents a continuation of existing trend towards centralization of IT resources resulting in increased specialization and ultimately leading to most end user organizations abandoning IT ownership, the authors believe that adopting enterprise end-uses should consider specializing on the security of their enterprise data in cloud.

According to Orosz, Selmeçi et.al., (2019) cloud computing has reinvented how organizations conduct business and enabled them to compete in a dynamic environment through new and innovative business models. This paper discusses the data security issues and concerns that are prevalent when organizations are moving their Enterprise Resource Planning (ERP) systems to the cloud particularly the relationship of trust between the cloud provider and client enterprise, where assuring

the integrity of data is mainly the responsibility of the provider. Therefore, clients must trust the providers to comply with the agreed-on security measures and protocols to achieve integrity of data. The relationship of trust is based not only on the provider's reputation but also on the specifications of the SLAs between them and client enterprise end-users are to share in the responsibility to adherence of the SLAs. The author stated small to medium enterprises gain the maximum benefits from cloud-based ERP as many of the concerns around data security are not relevant to them. A hybrid solution where organizations can choose to keep their sensitive applications on-premises while leveraging the benefits of the cloud is proposed in this paper.

Al-Okaily, Alkhwalidi, et. al., (2022) in their research finding stated that 71% of the variance in behavioural intention (BI) to use cloud-based ERP- accounting information systems (AIS) was explained by performance expectations, social incentive, COVID-19 risk (COV-19 PR), and trust (TR). Contrary to assumptions, effort expectations and perceived security risk have no impact on business intelligence (BI). In addition, it was discovered that BI influenced how individuals actually utilized the system and accounted for 74% of its variation. The deployment of cloud-based AIS has a significant impact on communication quality (CQ) and decision quality (DQ) as outcome factors (DQ). The authors mentioned that small- and medium-sized enterprise officials and policymakers could use the current research to illustrate the relatively low rates of cloud-based AIS and to develop strategies to increase the acceptance and use of cloud-based AIS by Jordanian users, where cloud-based services are still considered an innovation.

However, in the case of SaaS (software as a service), the CSP bears a greater share of the security burden. For each CSM, one would discover that the security responsibility of the CSM is determined by the cloud delivery model that the CSM is targeting. The classification of the various security responsibilities between end-users and CSPs in the various cloud security models is depicted in figure 4.1. As illustrated in the figure 4.1 below, the CSP is entirely responsible for security in a Software as a Service (SaaS) delivery model, which is where a typical cloud-based ERP will fall. Our review

identified two cloud security models that are particularly well-suited for SaaS delivery: the Multi-Cloud Database Model (MCDM) and the Multiple Tenancy Model (MTM).

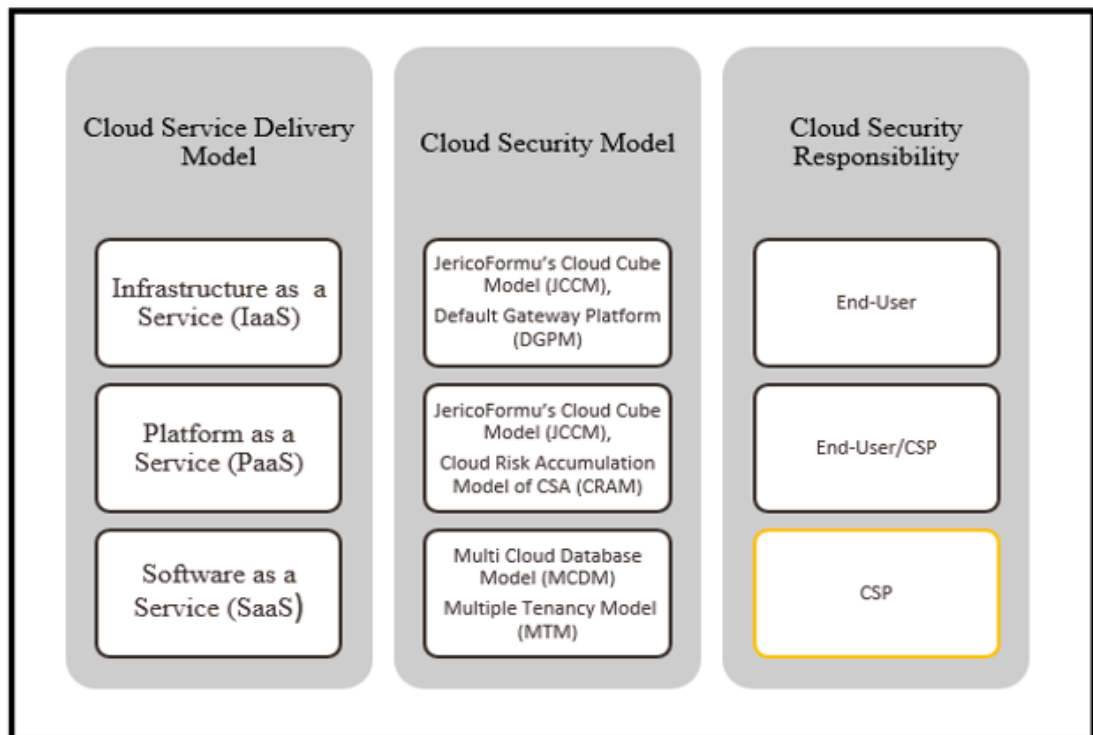


Figure 4.1: Classification of the Different Security Responsibilities between the End-Users and the CSP in the various Cloud Security Models (Eya, 2023)

Chou (2010), as illustrated in figure 4.2 below, also attempted to classify the responsibilities sharing structure between end-users and CSPs. As illustrated in his diagram, data responsibilities are not the end user's responsibility in a SaaS cloud deployment model; however, in all other deployment models, the end-user shares or holds data responsibilities. In his model, the allocation of data responsibilities differs across various cloud deployment models, with Software as a Service (SaaS) relieving end-users of data management tasks, contrasting with other models where end-users either share or hold these responsibilities. Furthermore, the critical components of cloud infrastructure—servers, storage, and networking—are integral to ensuring robust security measures, suggesting that if CSPs oversee these components, they likely bear responsibility for overall cloud security. Servers, storage, and networking are all critical computing features of cloud security; therefore, wherever the CSP is responsible for these features, it is reasonable to assume they are also responsible for

cloud security. This does not apply to On-Premises or Private Cloud environments, where the end-user assumes complete responsibility for the cloud system.

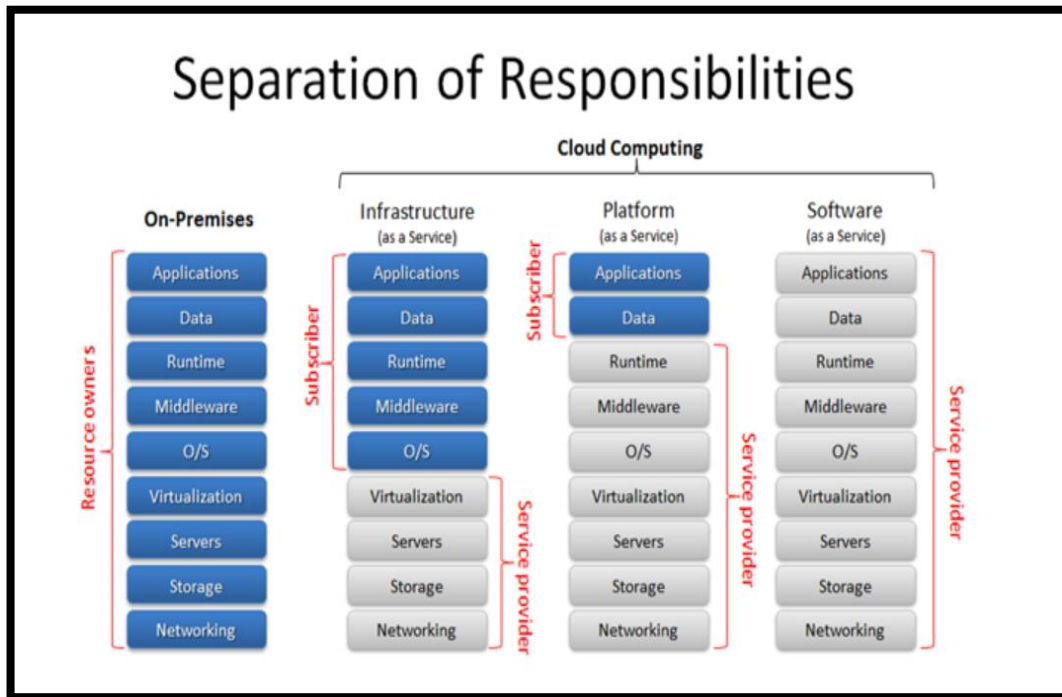


Figure 4.2: Separation of responsibility between the end-user and CSP using different cloud deployment models (Chou, 2010)

The "security effectiveness" metric is the yardstick we've chosen to describe how effective CSM are at securing the cloud-based infrastructure (Eya and Weir (2021); Sharma and Kaur (2014)). We use the term "averagely secured" to denote when a cloud system's CSM provides medium security; on the other hand, we use the term "highly secured" to denote when a cloud system's CSM provides an effective high level of protection. The "security porosity" is the yardstick we used to describe the CSM, which is a measure of how likely it is to be porous to an attacker (Eya and Weir (2021); Sharma and Kaur (2014)), for example, classifying the CSM as having a high likelihood of being porous to an attacker because a malicious insider can easily bypass the security modalities of such a model. The term "targeted cloud feature" is used to describe what the cloud security model (CSM) is aiming to secure more in the cloud system (Eya and Weir, 2021). Some CSM is aiming to secure cloud data, whether it is data at rest or data in transit, while others are aiming to secure cloud network infrastructures, and still, others are aiming to secure the end-user. The feature is used

to identify which aspect of a cloud system a CSM is primarily concerned with safeguarding. The "Practicality" criterion has been adopted to distinguish between the different CSMs in terms of whether they are system-centred or user-centred (Eya and Weir, 2021). All cloud security models have the same overall goal of attempting to secure the cloud system, though they differ in the mechanisms and approaches they employ to accomplish this goal. This feature will assist us in identifying the CSM that is more user-centric in their approach. The CSM was itemised and compared against these characteristics in the first column of table 4.3 below.

*Table 4.3: Table representation of the cloud security model and its analysing features*

	The Cloud Multiple-Tenancy Model of NIST	The Cloud Risk Accumulation Model of CSA	Jericho Forum's Cloud Cube Model	Default Gateway Platform	Multiple Cloud Database Model	End-user Centric Access Control Framework for implementation of ERP systems in Public Cloud.
Technology Used	Virtualization	Layer Dependency	Cloud Formation	Three Level Defence	Multi CSP and Secret Sharing Algorithm	EAD, EDF, CSP AD, EAQ.
Security Responsibility	Cloud Service Provider	Cloud Service Provider	End-user and Cloud Service Provider	End-user	Cloud Service Provider	End-user and Cloud Service Provider
Security Effectiveness	Averagely Secured	Averagely Secured	Highly Secured	Highly Secured	Highly Secured	Highly Secured
Security Porosity	Less Likely	More Likely	More Likely	More Likely	Less Likely	Less Likely
Targeted Cloud Feature	Cloud Network Infrastructure (CNI)	Cloud Network Infrastructure (CNI)	Cloud Network Infrastructure (CNI)	Cloud Database	Cloud Database	Cloud Enterprise Dataset and Cloud Database
Security Practicality	System Centred	System Centred	System Centred	System and End-user Centred	System Centred	System and End-user Centred

## **4.2 Strengths and Weaknesses of the Cloud Security Models.**

Using the information in the preceding table 4.3 above, we can now carefully examine the strengths and weaknesses of the various CSM in an effort to identify similarities, differences, and gaps that can be further investigated. The obvious similarity shared by all of the CSMs is that they all share the same goal of securing the cloud computing system. Although some of the CSM are more focused on securing user data/databases,

such as the Multi-Cloud Database Model (MCDM), others, such as the Cloud Risk Accumulation Model of the Cloud Security Alliance (CSA), are more focused on securing the cloud infrastructure level. Because providing cloud system security is their primary responsibility, the CSM with the "highly secured" security effectiveness and "less" security porosity would be the most preferred in terms of achieving the primary goal of the CSM: which is cloud system availability. According to the data in table 4.3, the multi-clouds database model appears to be the CSM that best meets the CSM objective, even though Kaur and Sharma (2014) believe it to be more expensive and time-consuming than the other cloud security models. However, in the MCDM, the risk associated with the failure of cloud services is minimal, and the risk associated with a malicious end-user is also minimal. In MCDM, the end-user of the cloud system does not bear any significant security responsibilities; this CSM is compatible with the vast majority of SaaS cloud platforms.

It is important to note that cloud ERP (Enterprise Resource Planning) applications modules can be accessed via the internet via the SaaS delivery model, which stands for Software as a Service. As a result, MCDM is the CSM that is most closely associated with cloud ERP systems. As a result, given that most businesses, particularly SMEs, are interested in moving to Cloud ERP but are concerned about the security concerns associated with cloud computing, The question is whether it is possible to have an MCDM updated to encourage more end-user involvement/responsibility in securing the cloud system. A more in-depth examination of MCDM and cloud ERPs may be required to determine how this improvement can be used to increase cloud security and cloud ERP adoption by an enterprise.

The NIST cloud multiple tenancy model's strength lies in its ability to separate virus, intrusion, and malfunctioning features from the different virtual machines and cloud hardware, allowing for more effective virus protection. It also helps to reduce the risk of a malicious application being deployed in the cloud environment. But its disadvantages are found in technological difficulties such as performance customization, data isolation, and architecture extension that must be overcome. The

Cloud Cube model developed by the Jericho Forum is distinguished by the ability of end-users to select cloud formations for a collaborative effort in securing the cloud system. However, there is a risk of data leakage when using this CSM, particularly if the backup with the CSP was not deleted at the end of the service agreement. This is managed by ensuring that data is properly transferred, managed, and deleted from all CSP backups at the end of the service agreement, as advised by the service provider. Because of the model's layer dependency, the Cloud Risk Accumulation model of the Cloud Security Alliance (CSA) makes it simple to assess the security of a cloud system. The most noticeable challenge here is that the CSP's security responsibility remains in the IaaS, which is the lower service level; this assumes that the greater the amount of end-user security responsibility, the greater the risk of a security breach in the environment. In addition to being more end-user oriented than other CSMs, the Default Gateway Platform has the advantage of providing the end-user with the ability to encrypt sensitive data using TrueCrypt prior to processing. The challenge, as well, is that the greater the level of end-user security responsibility, the greater the likelihood of security porosity, because of the human factor challenges an end user will present. The table 4.4 below shows the concise summary of the strengths and weaknesses of the different cloud security models.

*Table 4.4: Summary of the strength and weakness of the different CSM*

<b>Cloud Security Models</b>	<b>Strengths</b>	<b>Weakness</b>
<b>The Cloud Multiple-Tenancy Model of NIST</b>	Ability to minimise malicious application damage in cloud environment, isolate errors, viruses, and intrusions from other virtual machines and hardware.	Data isolation, architecture extension, configuration self-definition, and performance customization are all technological challenges of this CSM.
<b>The Cloud Risk Accumulation Model of CSA</b>	The layer dependency of this cloud service models facilitates the analysis of security risks in cloud computing.	The lower a cloud service provider's service layer, the more tasks and security features a customer is responsible for and the greater the likelihood of a security breach.
<b>Jericho Forum's Cloud Cube Model</b>	Ability of end-user to choose the optimal cloud configurations for confidential sharing.	Terminating an agreement with a cloud service provider requires proper data wiping from the CSP's infrastructure,



		including backups, to prevent potential data leaks.
<b>Default Gateway Platform</b>	This CSM enables the end user to encrypt sensitive data using TrueCrypt before the data is processed.	The greater the end-user's security responsibilities, the higher the probability of security vulnerabilities.
<b>Multiple Cloud Database Model</b>	Minimizes malicious insider risk in cloud, preventing service failure and enhancing security.	This expensive and time-consuming cloud security model lacks significant security responsibility for end-users, making it less efficient than other models.
<b>End-user Centric Access Control Framework</b>	Encourage shared security responsibility between the End-user and Cloud Service Provider which increases security awareness and effectiveness.	Establishing security effectiveness requires ongoing research and case studies.

#### **4.3 End-user Data Access Management Implementation Framework for Enterprise ERP Software based in the Public Cloud.**

Some of the most common types of cloud security issues have been identified. These include embedded security issues, application issues, trust and conviction problems, client management problems, cloud data storage problems, clustering computing problems, forensic problems and operating system-related problems (Singh, 2016); (Khan, 2016). Cloud security, as previously mentioned, can be either system- or user-centred or it can be a combination of the two (Eya and Weir, 2021). A new cloud security framework will be proposed in this project, with a particular emphasis on incorporating the various components of end-user management issues into the framework, with the goal of improving enterprise cloud data security and end-user experience in general. It can be categorised as a user-centred cloud security framework that is both system and user-friendly in its design and implementation. The following issues pertain to end-user management: end-user experience issues, end-user authentication issues, end-user centric confidentiality, service level management, human factor, forensic value, reputation, governance and security, trusted third party and a lack of trust on the part of the end-user (Pollini, 2022); (Tabrizchi, 2020). Almost all of the issues related to end-user management that have been identified can be summed up as "the role of the human factor." This is because the system end-users are humans, and if all of the human factor influences are positive, then these issues can be

managed, if not eliminated. If human factors do not influence the situation, there may be no problems at all. In the following stages, the proposed framework will consider the following factors: the various cloud delivery models (IaaS, PaaS, SaaS, and AaaS), as depicted in figure 4.3 below. The security responsibilities of the cloud service provider (CSP) and the end-user, cloud data security (which includes data integrity, data confidentiality, and data availability), and the various available technologies are all discussed.

This cloud computing security framework, which uses Enterprise Access Directory (EAD), Enterprise Database Fragmentation (EDF) in the cloud, and End-user Access Quires (EAQ), to control who has access to enterprise data in the cloud, is known as the End-user Data Access Management Framework (EDAF). To run ERP software in a cloud environment, a cloud authentication control framework must be implemented.

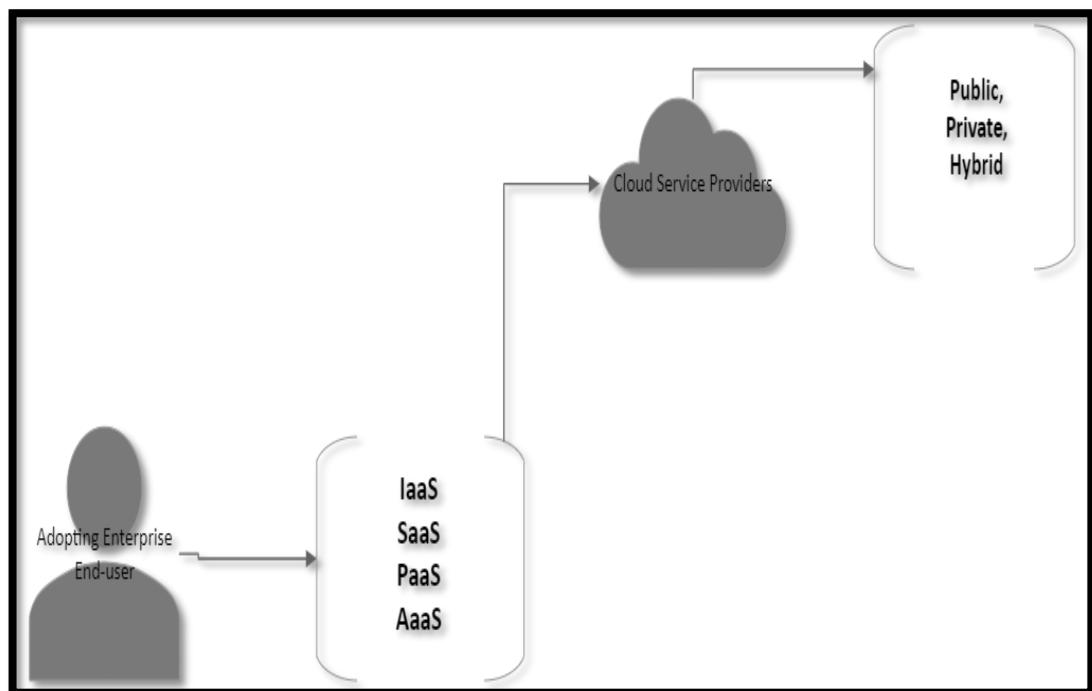


Figure 4.3: Summary of cloud computing delivery model and services (Eya, 2023)

To encourage end-user participation in enterprise cloud data security while also reducing the impact of malicious insiders on enterprise cloud data, the proposed framework is designed to do two things: The following characteristics distinguish the proposed framework from others: in a cloud environment, the EAD, EDF, and EAQ.

The proposed data security frameworks can be classified as a SaaS data security framework. In most SaaS, the cloud service provider (CSP) is responsible for the security of the cloud system; however, this issue is addressed in this framework, which will encourage the involvement of end-users in the SaaS cloud data security system, according to the new framework. The elements of the proposed framework discussed in the below following paragraphs can be found in the Figure 4.4 below.

***Enterprise Access Directory:*** This is one of the framework's distinguishing characteristics. This is the directory that is created after the enterprise's initial data classification. The Enterprise Access Directory (EAD) is a list of key roles and responsibilities for various roles within the enterprise, as well as the level of data access for each role. This is the enterprise's roles and responsibilities database, which should be the first port of call when an end-user wants to access data in the cloud. The key benefit of the EAD is that no single role will have simultaneous access to the entire enterprise dataset. This feature of the framework will mitigate the impact of a malicious insider incident on the organisation.

***Enterprise Database Fragmentation:*** This feature of the framework proposes that after an enterprise has gone through data classification as part of the procedures for moving data to private, public, or hybrid cloud, the CSP should provide enterprise database fragmentation for each set of enterprise data being moved to the cloud. A fragmented enterprise database in the cloud means that enterprise authorised end-users only have access to the information they need to perform their job at the company.

***CSP Access Directory:*** Although a feature of the framework, it is not a distinguishing feature because authors such as Kumari and Nath (2018) proposed this feature in their

paper "Data Security Model in Cloud Computing Environment." This is simply a directory of cloud usernames and passwords maintained by the CSP to validate each time an end-user accesses cloud data.

***End-user Access Queries:*** When the end-user role is not classified in the EAD or the end-user username/password is not determined by the CSP Access Directory, this is a unique feature of the cloud security framework that triggers a set of queries. The Enterprise Cloud Administrator will be notified, and the end-user will be denied access. The end-user will be asked to answer a series of generic questions that will aid the Enterprise Cloud Administrator in determining the end-user identity. The determined identity can then be used to add or update the new end-user to the Enterprise Cloud Directory.

In cloud security frameworks, particularly when utilizing End-User Access Directories (EAD), instances may arise where the end-user role isn't clearly defined within the directory, or their username and password details aren't readily available from the Cloud Service Provider's (CSP) Access Directory. This scenario triggers a distinctive protocol within the security framework, initiating a series of specific inquiries. Upon detection of such an event, the Enterprise Cloud Administrator is promptly alerted, and access for the end-user in question is promptly denied as a precautionary measure. Subsequently, the end-user is guided through a structured series of generic questions designed to facilitate the identification process by the Enterprise Cloud Administrator. These inquiries aim to extract pertinent information that assists in verifying the end-user's identity accurately. Once the end-user's identity is determined through this process, the verified details can then be utilized to either incorporate or update the end-user's information within the Enterprise Cloud Directory, ensuring accurate and secure access management within the cloud environment. In conclusion, the complex landscape of cloud security frameworks may lead to instances of ambiguity in end-user roles or inaccessible login credentials. In such situations, a specific protocol is activated, prompting immediate notification to the Enterprise Cloud Administrator, who takes proactive measures to restrict access for the affected end-user.

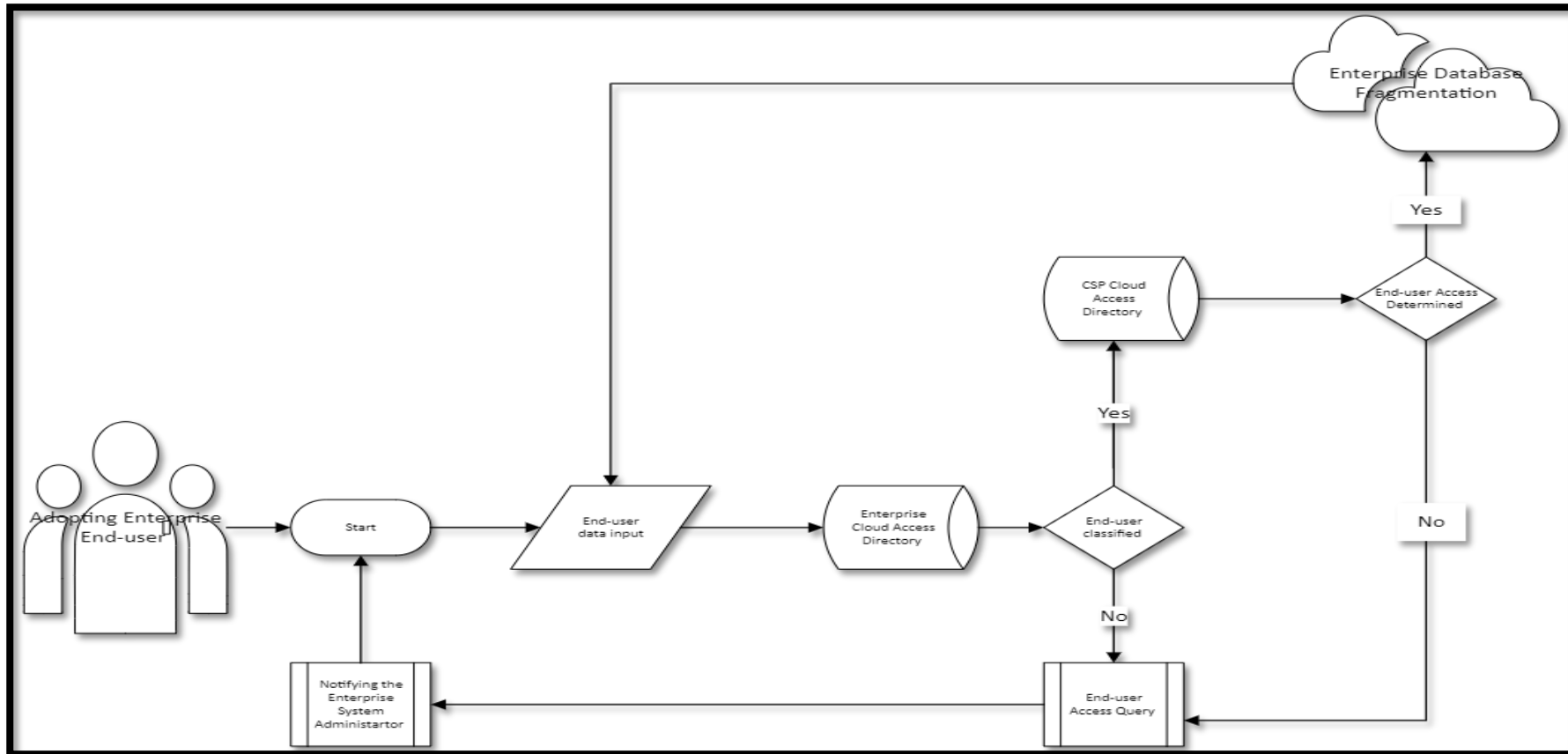


Figure 4.4: End-user Data Access Management Implementation Framework for Enterprise ERP software based in the Public Cloud (Eya, 2023)

As illustrated in Figure 4.4, an End-user Data Access Management Implementation Framework in public ERP software based in the cloud is proposed. The proposed framework is divided into two distinct phases; the first phase is dedicated to end user security responsibility and is

managed by the end-user enterprise, while the second phase is managed by the CSP enterprise. The first security responsibility phase involves classifying the enterprise's data set according to its security importance and populating the Enterprise Cloud Directory with the enterprise's distinct roles and responsibilities. The end-user enterprise is responsible for this phase's security. The second phase begins when a classified end user logs in to a cloud-based enterprise database using the correct username and password. The second phase consists of three components: a CSP Access Directory, enterprise database fragmentation, and end-user access queries. The three features are managed by the Cloud Service Provider (CSP), and the CSP is solely responsible for security. When compared to other existing models, the proposed framework will encourage greater end-user participation in their enterprise's cloud data security. Additionally, the framework mitigates the impact of a malicious insider on the enterprise cloud data set in the cloud, as no single user has concurrent access to the entire enterprise database in the cloud.

#### **4.4 Summary of Chapter 4**

Numerous cloud security issues have been identified, including embedded security issues, application security issues, trust and conviction issues, client management issues, cloud data storage issues, clustering computing issues, and operating system-related issues. The purpose of this chapter of the thesis is to propose a new cloud security framework that focuses on incorporating the various components of end-user management issues. As illustrated in figure 4.3 above, End-user Data Access Management Implementation Framework in public ERP software based in the cloud, is a cloud computing security framework that utilizes Enterprise Access Directory (EAD), Enterprise Database Fragmentation (EDF) in the cloud, and End-user Access Queries (EAQ) to manage who has access to enterprise data in the cloud. The framework's objective is to increase end-user engagement in enterprise cloud data security and to mitigate the impact of malicious insider attacks on cloud data.

The framework can be classified as a cloud-based SaaS data security framework. The CSP Access Directory is a simple database of cloud usernames, passwords, and other

generic classifications that the CSP maintains for the purpose of validating each time an end-user accesses data in the cloud. End-user Access Quires will prompt the user to respond to a series of generic questions designed to assist the Enterprise Cloud Administrator in determining the user's identity in the event an end user is not already classified. The determined identity can then be used to configure or update the Enterprise Cloud Directory to include the new individual. The proposed framework is divided into two distinct phases, the first of which is end user security responsibility. The end-user enterprise manages the first phase, while the CSP enterprise manages the second phase. The framework reduces the impact of a malicious insider on the enterprise cloud data set stored in the cloud. No single user has concurrent access to the entire enterprise database. The subsequent chapters will attempt to validate the views of this proposed framework.

# Chapter 5. Quantitative Data Analysis

This chapter 5 delves into the details of our quantitative data analysis to better understand how the views of our research participants in the survey supports end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. This chapter is divided into two sections. The first section 5.1 is called “Quantitative Data Visualization Using Tables and Bar Charts”, and it contains a summary of each of the survey questions as well as the data collected. We used tables and bar charts to virtualize the responses received for each survey question. The section 5.2 called “statistical analysis of our research assumptions” is the second part of this chapter. This section aims to use SPSS to analyse the data we gathered. The tests of normality, ordinal regression, the test of parallel lines, and non-parametric correlations were performed and represented here by tables.

## 5.1 Quantitative Data Visualization Using Tables and Bar Charts.

Quantitative data visualization using tables and bar charts involves representing numerical information in a visual format to aid understanding and analysis. Tables present data in rows and columns and Bar charts, display data using rectangular bars.

Table 5.1: Data representation of SQ1

<b>Q1 - How many years have you worked in your current role?</b>			
#	Answer	%	Count
1	Few months up to 1 year	30.23%	13
2	2 years up to 4 years	32.56%	14
3	5 years up to 7 years	25.58%	11
4	8 years up to 10 years	6.98%	3
5	11 years and above	4.65%	2
	Total	100%	43



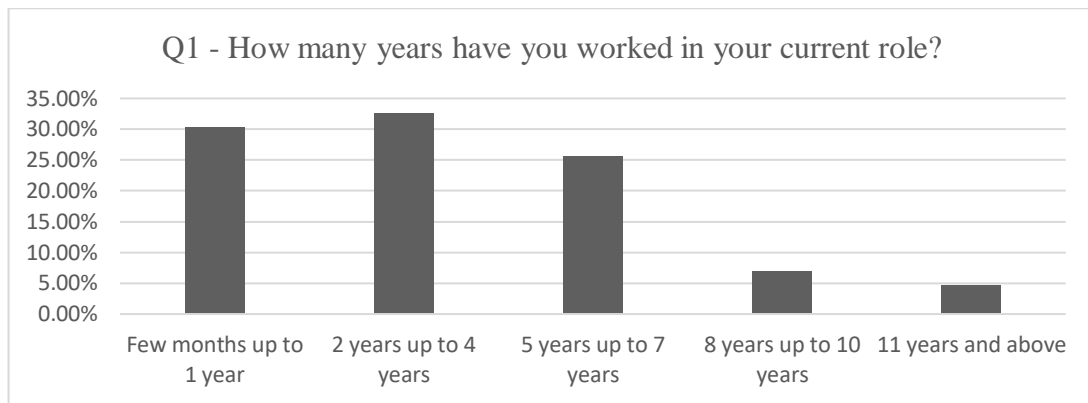


Figure 5.1: Bar Chart representation of collected data for SQ1

This ordinal question was created to address research assumption 1, which states that participants who have worked with a cloud-based ERP system are more likely to respond to our research questions correctly. This question will tell us how experienced our participant is; more experienced participants may provide more useful responses. Although authors such as Sveiby (1997) argue that knowledge cannot be measured solely by experience, but also by other intangible assets such as staff competency, internal structure, and external structures that influence those experiences, the longevity of the experience is being measured. We agree with Davenport and Prusak (1998) that the more a person does something, the more likely they are to be good at it; we live in a society where one's knowledge of the field is thought to be influenced by experience. As a result, our question about the number of years of IT experience our research participants have is reasonable, as it will increase confidence in the reviews and responses we gathered. Because this is an ordinal question, the summary of our responses is represented in bar charts plotted against the percentage of responses for each choice answer.

Table 5.1 and Figure 5.1 show that 43 of the 44 people who took part in our survey answered this question, one participant did not respond to this SQ1. According to their responses, 30.23 % had only a few months to a year of experience in their current IT position. 32.56 % had two to four years of experience, while 25.58 % had five to seven years. A total of 11.63 % of the participants are more experienced professionals with at least 8 years of experience. Because the results show that all of our participants work in IT roles for various companies, we didn't feel the need to include "No Experience"

as an option in our response to this question. We can proceed safely because all of our participants have at least one month of experience in an enterprise IT role, even if the majority of that experience is less than five years, but we will try to analyse the responses of the more experienced professionals to see if there is any discernible difference in opinion. Because all of these questions focus on addressing research assumption 1, this SQ1 is closely related to SQ2, SQ14, and SQ15.

Table 5.2: Data representation of SQ2

<b>Q2 - Do you currently work with a Cloud-based ERP system in your enterprise?</b>			
#	Answer	%	Count
1	Yes, we are using a Cloud-based ERP system	47.73%	21
2	No, we are not using a Cloud-based ERP system	52.27%	23
	Total	100%	44

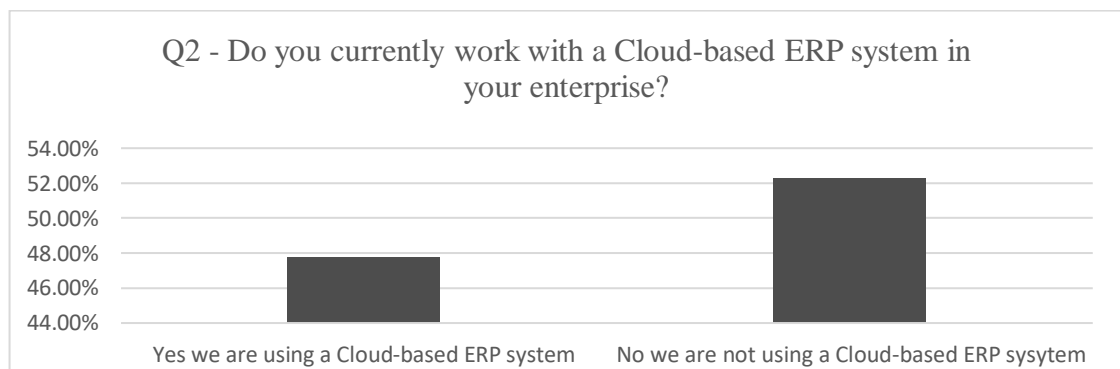


Figure 5.2: Bar Chart representation of collected data for SQ2

This demographic question was created to learn more about the IT experience of our study participants. We wanted to see how many of our participants had used a cloud-based ERP system with this question. This is significant because the framework we propose for validating its attributes is geared toward cloud-based ERP systems. This isn't to say that the opinions of professionals who haven't used a cloud-based ERP system aren't valid; rather, knowing that our participants have used one gives us more confidence. This question relates to research assumption A1, which states that participants who have used a cloud-based ERP system are more likely to provide a valid response to our survey.

Table 5.2 and Figure 5.2 show that 44 of the 44 people who took part in our study answered this question. 47.73% of the participants said they use a cloud-based ERP system in their business, while 52.27% said they don't. Understandably, slightly more than half of our survey respondents have yet to implement a cloud-based ERP system in their company. This could be due to several factors already discussed in the literature, but the two most notable ones are the security concerns businesses have with cloud-based ERPs and the fact that cloud-based ERPs are still a new IT solution that will take time for more businesses to adopt. It's important to note that, while our research participants may not be using a cloud-based ERP solution, they are familiar with the fundamentals of cloud computing security as IT professionals, and thus feel comfortable participating in the study. A comparison of the responses from SQ2 and SQ15 reveals two things: 52.27% of our respondents do not use a cloud-based ERP system in their company, and 66.67% believe data security is a major concern when their company adopts a cloud-based ERP software system. This demonstrates that data security is still a concern when adopting cloud solutions, and this could be due to a lack of CSP trust or a lack of end-user involvement in data security in cloud-based ERP systems. This highlights the persistent concern surrounding data security during the adoption of cloud solutions, potentially stemming from either a deficit in trust towards Cloud Service Providers (CSPs) or insufficient engagement from end-users in safeguarding data within cloud-based Enterprise Resource Planning (ERP) systems. Such observations underscore the importance of fostering trust relationships with CSPs and promoting active participation from end-users.

Table 5.3: Data representation of SQ3

<b>Q3 - Cloud Computing has an impact on Enterprise system data security. To what extent do you agree with the above statement?</b>			
#	Answer	%	Count
1	Definitely has an impact	53.49%	23
2	Probably has an impact	27.91%	12
3	Might or might not have an impact	11.63%	5
4	Probably has no impact	4.65%	2
5	Definitely has no impact	2.33%	1
	Total	100%	43

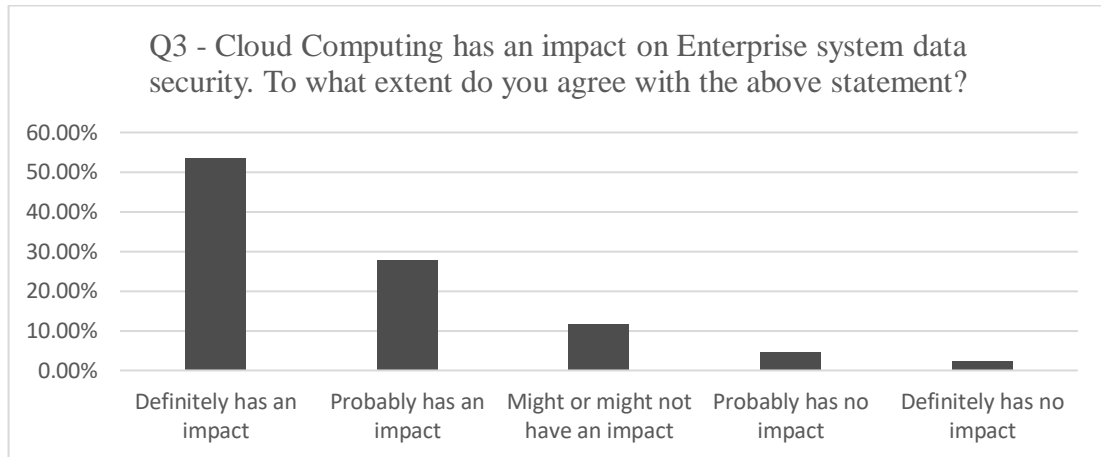


Figure 5.3: Bar Chart representation of collected data for SQ3

This question was created to address one of the research goals: determining whether enterprises' adoption of a cloud-based ERP system has an impact on enterprise data security. This question has two response options: a Likert scale and an open-ended question that allows participants to justify their choice if they wish. This question directly addresses research assumption A2, which states that any upgrade in technology should, in theory, have some impact on previous technology, which can be positive or negative. Cloud computing would have an impact on enterprise system data security in the cloud, according to authors like Cheng and Lai (2012) and Sharma, et al. (2017), but the extent of this impact was unknown. Authors such as Saripalli and Walters (2010) and Subramanian and Jeyaraj (2018), on the other hand, believed that the impact would be negative because data security would become more porous as a third party is now involved.

According to Table 5.3 and Figure 5.3, 43 of the 44 participants responded to this question. 53.49% of respondents strongly agree cloud computing has an impact on enterprise data security, 27.49% agree that it probably has an impact, and 11.6% are undecided, believing it might or might not have an impact. Approximately 6.98% believe that cloud computing has little or no impact on enterprise data security in the cloud. The meaning of "impact" to each participant can be an influencing factor in why they choose a particular answer in this case. Although it is not safe to assume that our

participants who stated that cloud computing has no impact on enterprise data security are looking at the word "impact" in a negative light. This leads us to define the term "Impact," which means "to have a strong effect on someone or something, or a marked effect or influence," according to the Oxford Dictionary. The impact can have a positive or negative effect on enterprise data security, according to this definition. So, based on our findings, cloud computing has a significant impact on enterprise data security (Mather, et al. (2009); Al Noor et al. (2010); Gupta, et al. (2013); Sharma, et al. (2013), and Sharma, et al (2017).

Table 5.4: Data representation of SQ4

<b>Q4 - The security responsibility for a Cloud system within an enterprise; should be a shared responsibility between the Cloud Service Provider (CSP) and the Cloud Service End-users. (Cloud Service End-user is the enterprise employees who use the enterprise system to work.) To what extent do you agree with the above statement?</b>			
#	Answer	%	Count
1	Definitely Agree	56.82%	25
2	Probably Agree	20.45%	9
3	Might or might not Agree	13.64%	6
4	Probably Disagree	4.55%	2
5	Definitely Disagree	4.55%	2
	Total	100%	44

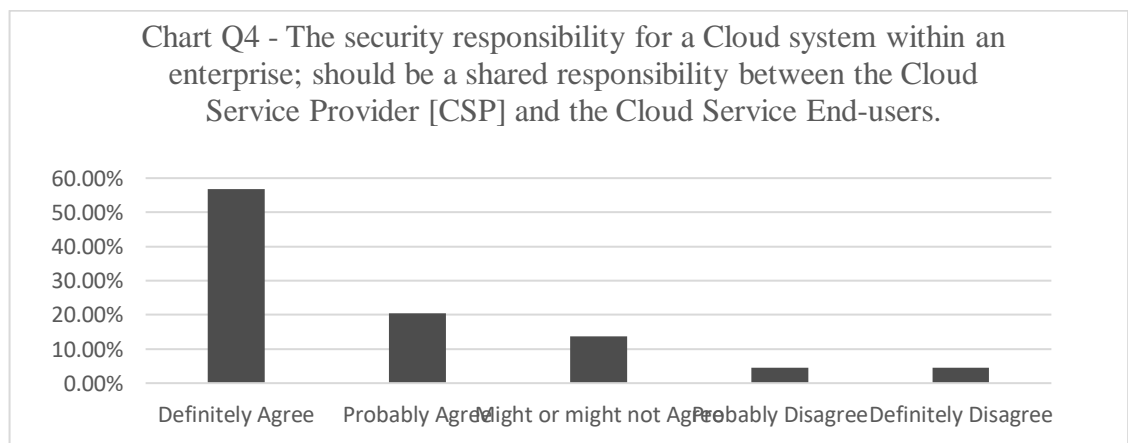


Figure 5.4: Bar Chart representation of collected data for SQ4

This multiple-choice question was designed to allow our participants to express how they agree or disagree with the statement that security responsibility for cloud systems within an enterprise should be shared by cloud service providers (CSP) and cloud service end-users. The framework proposed that the End-User Enterprise and the Cloud Service Provider share security responsibility (CSP). This question will help us determine whether or not our participants agree with such a division of security responsibilities. This question addresses our research assumption A3, which states that when the cloud service provider and cloud service end-users share security responsibility for the cloud system, the enterprise data in the cloud will be more secure. Because both questions are focused on the research assumption A3, this question is closely related to SQ8.

According to the data gathered from our research activity (see Table 5.4 and Figure 5.4 above), 56.82 % of participants strongly agreed that security responsibility for cloud systems within an enterprise should be shared by the cloud service provider (CSP) and the cloud service end-users. They chose because 20.45 % are likely to agree, and 13.64 % "Might or Might not agree" hence are undecided. The remaining 9.10 %, on the other hand, may not have seen the need for a shared security responsibility between the CSP and the system's end-users. As a result, we are confident that a shared security responsibility between the end-users of the system and the CSP will improve trust in cloud ERP systems and allow the end-user to be a part of the entire data security process, as over 70 % of our participants agree. Second, it will encourage CSPs to think about their type of end-user when developing cloud-based ERP solutions. A shared security responsibility is bound to improve communications between CSPs and end-users, allowing both parties to easily document and escalate security incidents, as well as provide a shared solution to security incidents that are tailored to the end-users needs. The End-user Data Access Management Implementation Framework in public ERP software based in the cloud, emphasised the importance of shared security responsibility, as well as a framework that integrates both CSPs and end-users into the data security responsibility of enterprise data in cloud-based ERP systems. This will ensure that the end-user know their responsibilities in ensuring their enterprise data security.

Table 5.5: Data representation of SQ5

<b>Q5 - In your opinion, is it okay to ensure that no single system end-user (including the CEO and the System Administrator) has access to all the Enterprise data set in the Cloud storage?</b>			
#	Answer	%	Count
1	Definitely Okay	45.45%	20
2	Probably Okay	15.91%	7
3	Might or might not be Okay	25.00%	11
4	Probably not Okay	13.64%	6
5	Definitely not Okay	0.00%	0
	Total	100%	44

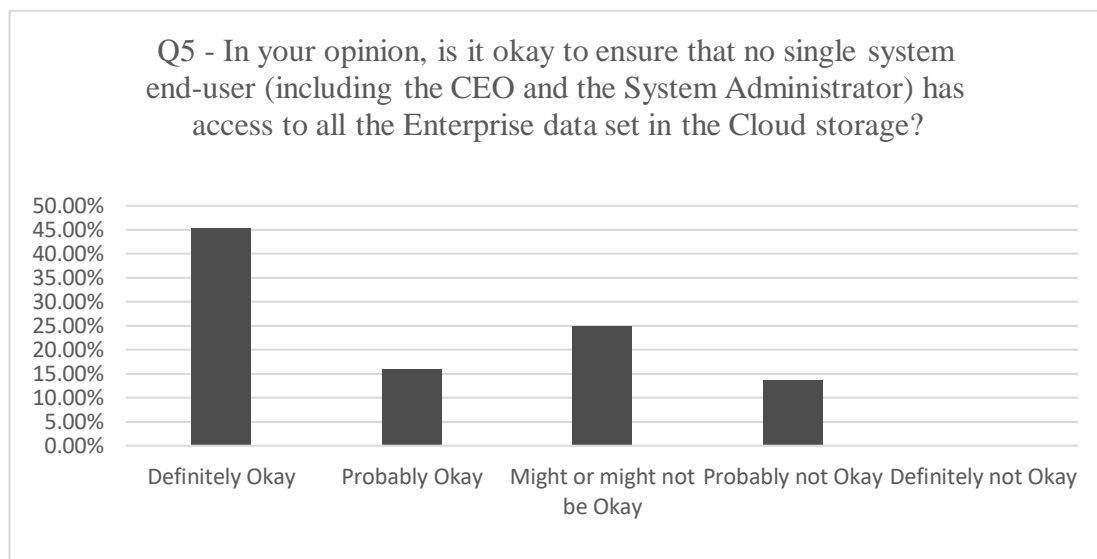


Figure 5.5: Bar Chart representation of collected data for SQ5

To better understand our participants' opinions on the research assumption A4, we created this multiple-choice question. We assumed that proper access management within the cloud service end-user enterprise would positively improve their enterprise data security in the cloud. The SQ5 is related to the SQ6, SQ7, SQ9, and SQ10, which are all questions that are focused on addressing the research A4 in one way or another. According to the results shown in Table 5.5 and Figure 5.5 above, 45.45% of respondents agreed that it is acceptable to ensure that no single system end-user has access to an enterprise data set stored in cloud storage, 15.91 % agreed that it is

probably acceptable, and 25.00% said it might or might not be acceptable. According to 45.45 % of respondents, it is acceptable to ensure that no single system end-user has access to an enterprise's data set stored in cloud storage, according to 45.45% of respondents, whereas 13.64% responded that it is most likely not acceptable. According to our assumptions, limiting complete access to the enterprise network and systems by any single system end-user in the cloud would benefit the enterprise. The End-user Data Access Management Implementation Framework for public cloud-based ERP software underscores the significance of preventing any single system end-user from accessing all of the enterprise's data in the cloud through enterprise dataset classification and database fragmentation.

Table 5.6: Data representation of SQ6

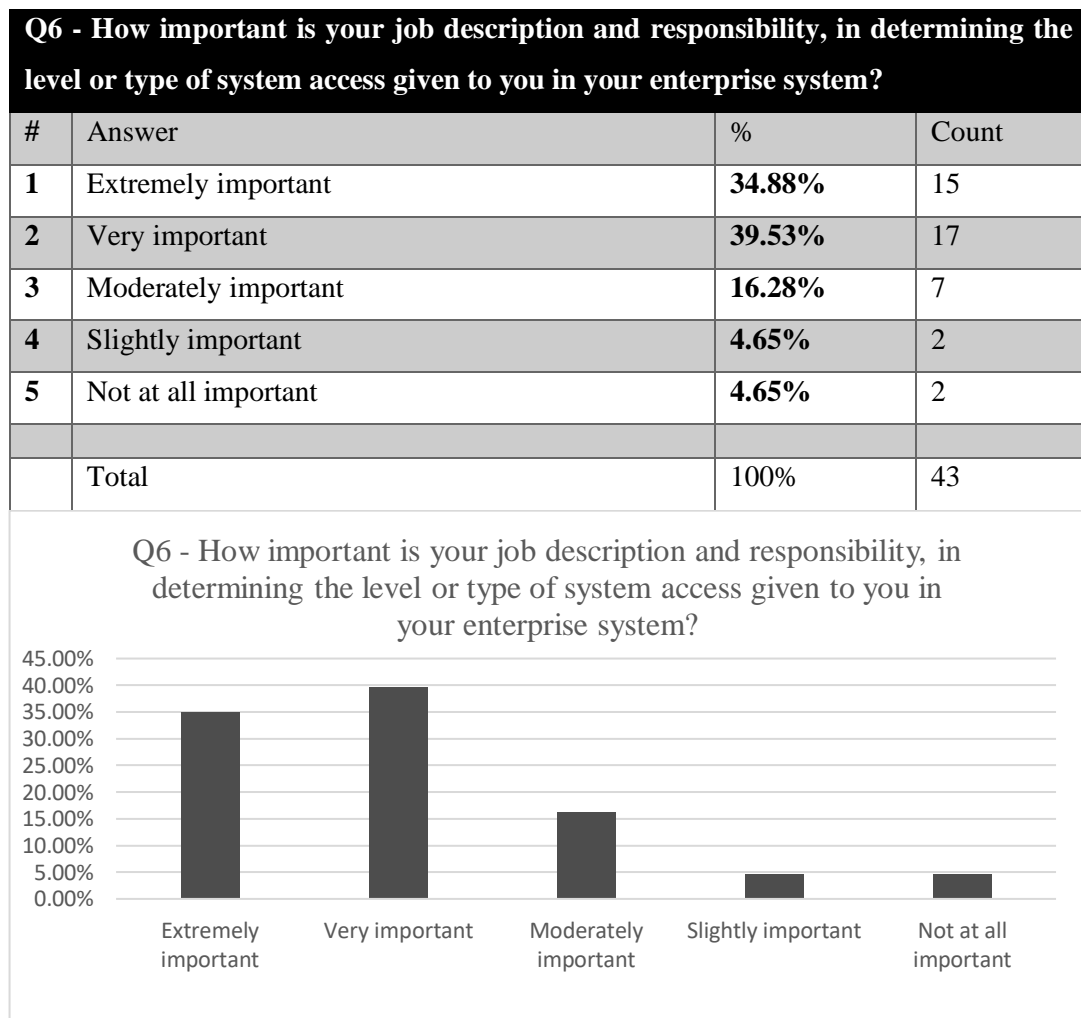


Figure 5.6: Bar Chart representation of collected data for SQ6



This Likert scale question was created to address our research assumption A4, where we assumed that proper access management within the cloud service end-user enterprise would positively improve their enterprise data security in the cloud. Access management is crucial for enhancing cloud security in enterprises. Key strategies include identity verification, role-based access control, least privilege principle, dynamic access policies, centralized control, audit trails, automated provisioning, encryption, tokenization, API security, regular security training, vendor access management, compliance with regulations, incident response planning, and continuous monitoring. We wanted to understand how our participants believed their job roles in their enterprises should be considered when determining what type of data, they could access on the cloud. The SQ6 is related to SQ5, SQ7, SQ9, and SQ10 where all the questions focus on addressing the research A4.

Table 5.6 and Figure 5.6 showed above that 34.88% of participants answered that our job description is extremely important in determining the type of system access given to us in our enterprise system, whereas 39.53% thought it was very important. This means that the Enterprise Access Directory is a welcome structure, and even employees will be satisfied with a directory that keeps track of what access each role within the enterprise has. 16.28% of participants thought it was moderately important to determine the type of system access given to us in our enterprise system, whereas 4.65% of participants thought it was slightly important and unimportant.

*Table 5.7: Data representation of SQ7*

<b>Q7 - Do you agree that, when a single system end-user has access to all the Enterprise data set in the Cloud, this may increase the Enterprise's chances of suffering a successful cyber-attack?</b>			
#	Answer	%	Count
<b>1</b>	Definitely Agree	<b>50.00%</b>	21
<b>2</b>	Probably Agree	<b>35.71%</b>	15
<b>3</b>	Might or might not Agree	<b>11.90%</b>	5
<b>4</b>	Probably Disagree	<b>2.38%</b>	1
<b>5</b>	Definitely Disagree	<b>0.00%</b>	0
	Total	100%	42

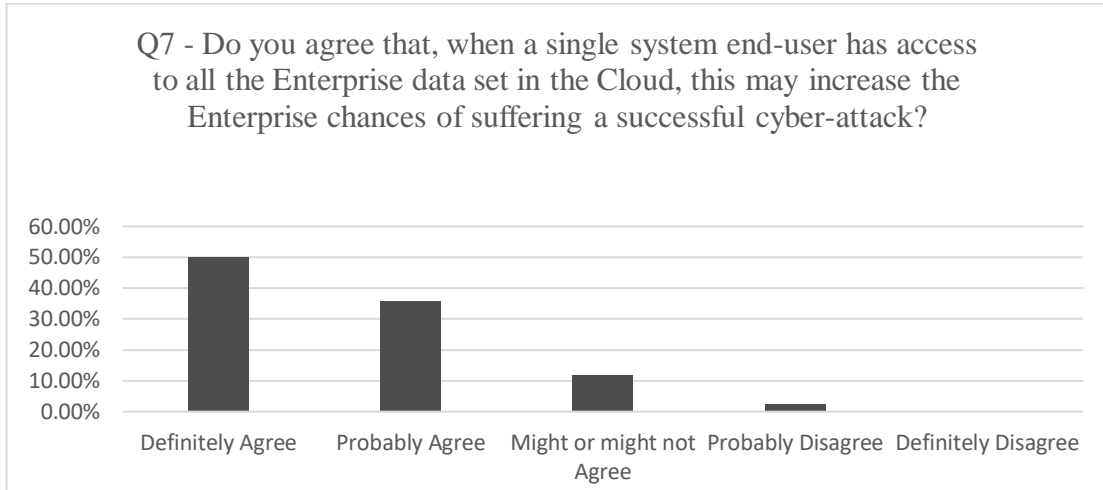


Figure 5.7: Bar Chart representation of collected data for SQ7

This Likert scale question was created to address our research assumption A4, where we assumed that proper access management within the cloud service end-user enterprise would positively improve their enterprise data security in the cloud. We wanted to understand how our participants believed that when a single system end-user has access to all the enterprise datasets in the cloud, it will increase their enterprise's chances of having a successful cyber-attack. The SQ7 is related to SQ5, SQ6, SQ9, and SQ10, where all the questions focus on addressing the research A4.

In Table 5.7 and Figure 5.7 above, 50.00% of participants definitely agree with the suffering of a cyber-attack when a single system end-user has access to all the enterprise data set in the cloud, whereas 35.71% of respondents answered that they probably agree with this. 11.90% of participants answered that it might increase the chances of a successful cyber-attack. Among the participants surveyed, a mere 2.38% expressed a probable disagreement with the notion that granting a single system end-user access to the entire enterprise dataset in the cloud could elevate the risk of a successful cyber-attack. This suggests a widespread recognition among respondents regarding the potential security implications associated with such unrestricted access privileges within cloud environments. This indicates that the overwhelming majority of surveyed participants, accounting for 97.62%, acknowledged the risk posed by

providing a single system end-user with access to the entire enterprise dataset in the cloud.

Table 5.8: Data representation of SQ8

<b>Q8 - End-users of a Cloud-based ERP software system, should hold some security responsibilities to ensure the security of their Enterprise Data in the Cloud. Do you agree with this statement?</b>			
#	Answer	%	Count
1	Definitely Agree	<b>61.90%</b>	26
2	Probably Agree	<b>30.95%</b>	13
3	Might or might not Agree	<b>7.14%</b>	3
4	Probably Disagree	<b>0.00%</b>	0
5	Definitely Disagree	<b>0.00%</b>	0
	Total	100%	42

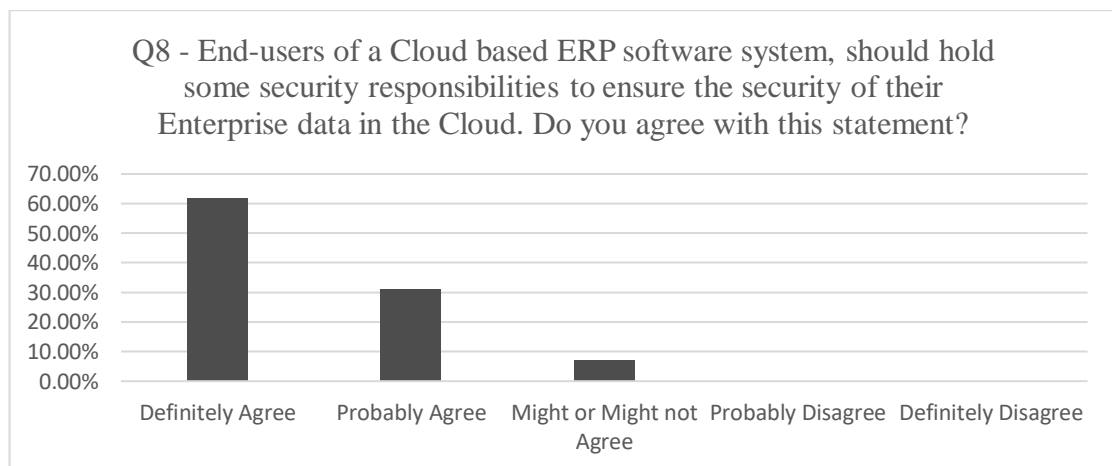


Figure 5.8: Bar Chart representation of collected data for SQ8

The Likert scale question was created to address our research assumption A3, where we assumed that when the cloud service provider and the cloud service end-user share security responsibility of the cloud system, it will result in a more secured enterprise in the cloud. We wanted to understand if our participants believed that the end-user of a cloud-based ERP software system should hold some security responsibility to ensure the security of their enterprise data in the cloud. The SQ8 and SQ4 are related as both questions are targeted at determining the research assumption A3. Table 5.8 and Figure 5.8 above, show that 61.90% of participants definitely agree that End-users of a cloud-

based ERP software system should hold some security responsibilities to ensure the security of their Enterprise Data in the Cloud, this goes to answer our research question; how important is an end-user security responsibility in ensuring enterprise data security in Cloud? this figure shows our participants believed it is very important. Whereas 30.95% answered that they probably agree with the statement. Only 7.14% of participants answered that they might or might not agree with the statement.

Table 5.9: Data representation of SQ9

<b>Q9 - How important is End-user Access Control in ensuring Enterprise data security in the Cloud?</b>			
#	Answer	%	Count
1	Extremely important	42.86%	18
2	Very important	47.62%	20
3	Moderately important	7.14%	3
4	Slightly important	0.00%	0
5	Not at all important	2.38%	1
	Total	100%	42

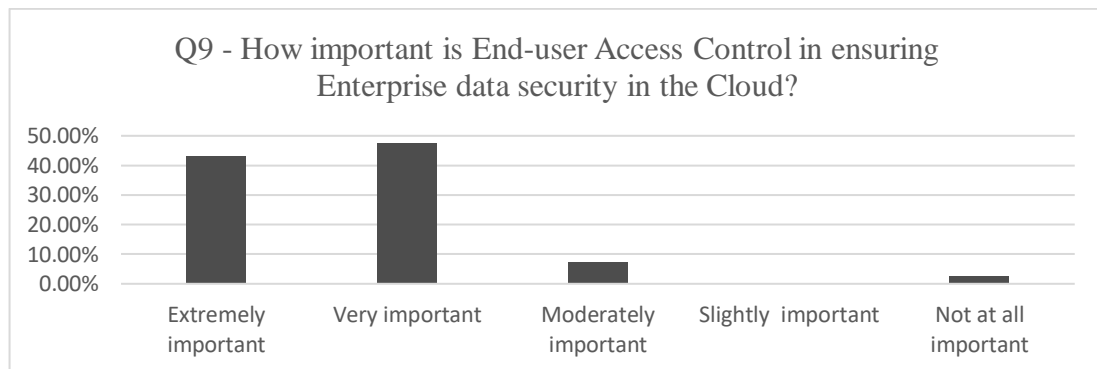


Figure 5.9: Bar Chart representation of collected data for SQ9

This Likert scale question was created to address our research assumption A4, where we assumed that proper access management within the cloud service end-user enterprise would positively improve their enterprise data security in the cloud. We wanted to understand how our participants believed that when a single system end-user has access to all the enterprise datasets in the cloud, it will increase their enterprise's chances of having a successful cyber-attack. This directly answers our

research question: "How important is end-user access control in ensuring enterprise data security in the cloud?" The QS9 is related to the QS5, QS6, QS7, and QS10, with all of the questions focusing on the research area of A4. Table 5.9 and Figure 5.9 show that 42.86% of participants answered that end-user access control is extremely important in ensuring data security in the cloud, whereas 47.62% answered that it is very important when ensuring enterprise data security in the cloud. 7.14% of participants thought it was moderately important and 2.38% thought it was not important.

Table 5.10: Data representation of SQ10

<b>Q10 - To manage Access Control, Cloud service providers keep a directory known as "CSP Access Directory"; this is a database of all the Cloud end-users and their passwords which is used in authentication each time an end-user accesses data in the Cloud. Do you agree that the "CSP Access Directory" would improve access control management in the Cloud?</b>			
#	Answer	%	Count
1	Definitely Agree	47.62%	20
2	Probably Agree	28.57%	12
3	Might or might not Agree	21.43%	9
4	Probably Disagree	2.38%	1
5	Definitely Disagree	0.00%	0
	Total	100%	42

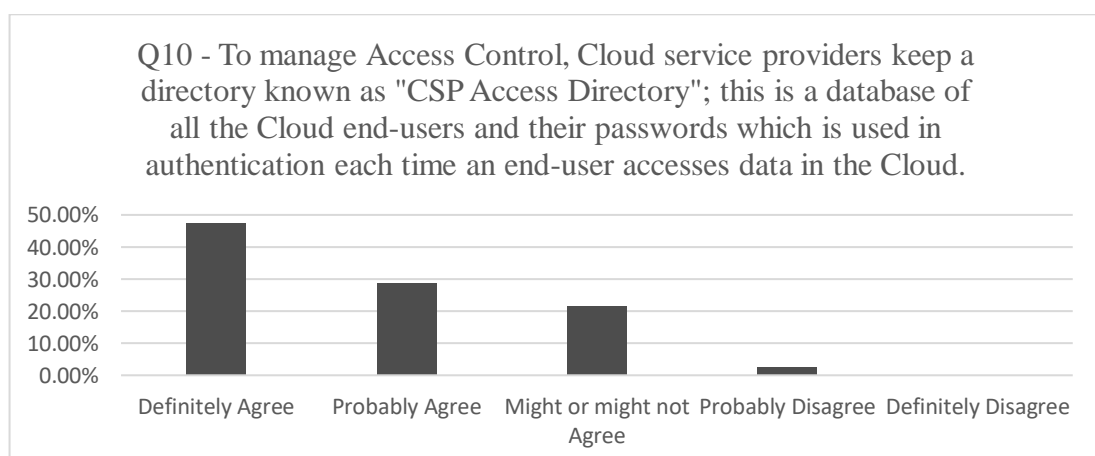


Figure 5.10: Bar Chart representation of collected data for SQ10

This question was created to address the research assumptions A4 and A5, where for A4 we assumed that proper access management within the cloud service end-user enterprise would positively improve their enterprise data security in the cloud; and for A5, we assumed that a feature of our proposed framework, which is the CSP Access Directory, when implemented, would improve access control management in the cloud. By leveraging a well-designed CSP Access Directory, organizations can establish a robust and flexible access control framework in the cloud, promoting security, compliance, and efficient management of user access. Regularly updating and optimizing access policies within the Access Directory ensures ongoing alignment with organizational needs and evolving security landscapes.

We wanted to use this question to know if our research participants agreed that the CSP Access Directory would improve access control management in the cloud. Table 5.10 and Figure 5.10 show that 47.62% of participants answered that they agree that managing access control using CSP Access Directory would improve access control management in the cloud, whereas 28.57% of participants answered that they probably agree with this statement. 21.43% of participants answered that they might or might not agree with the statement, whereas 2.38% answered that they probably disagree with the statement that access control management in the cloud can be improved. According to Gartner cited by Lin, Wu, and He (2019), server workloads in hybrid data centres spanning private and public clouds require a different protection strategy than end-user-facing devices. This is because cloud applications can be very flexible, and execution agents for local servers don't work with them.

As per Gartner's insights, as referenced by Lin, Wu, and He (2019), hybrid data centers integrating both private and public clouds necessitate distinct protection strategies compared to those employed for end-user-facing devices. This distinction arises from the inherent flexibility of cloud applications, which renders traditional execution agents for local servers incompatible with them. Therefore, safeguarding server workloads in hybrid environments mandates tailored security approaches that account for the unique characteristics and dynamics of cloud-based applications.

Table 5.11: Data representation of SQ11

**Q11 - Enterprise data set classification is a process of classifying enterprise data set against key roles and responsibilities of their end-user, which will determine the level of access each end-user will have and the data that they can access in the Cloud.**

**Enterprise data set classification: should happen as an integral process of the enterprise preparations to move the enterprise data to the Cloud.**

**Do you agree with the above statement?**

#	Answer	%	Count
1	Definitely Agree	61.90%	26
2	Probably Agree	23.81%	10
3	Might or might not Agree	11.90%	5
4	Probably Disagree	2.38%	1
5	Definitely Disagree	0.00%	0
	Total	100%	42

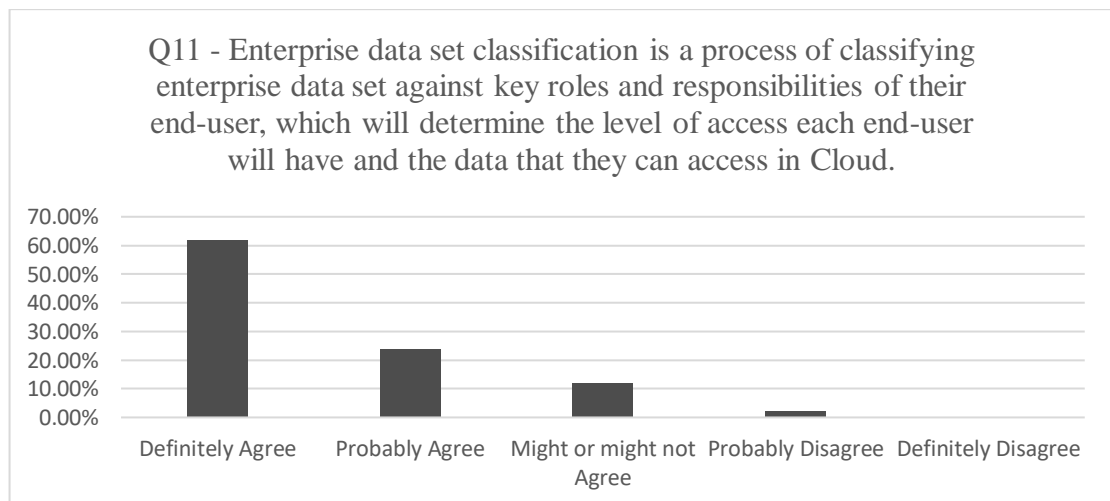


Figure 5.11: Bar Chart representation of collected data for SQ11

Table 5.11 and Figure 5.11, above, show that out of the 44 participants, 42 answered this question. 61.90% believed that enterprise data set classification should happen as an integral process of a cloud-based ERP implementation. 23.81% probably agreed with the importance of enterprise data set classification, while 11.90% remained undecided. They believed it might or might not have an impact. About 2.38% think that enterprise data set classification is of no importance to enterprise data security in the cloud. Here, considering something as an integral part of processing in an

enterprise can have multiple meanings for the study participants. But this notion cannot be denied that more than half of the study participants agreed that this classification system is important for the security of data and, in turn, for the positive progress of the enterprise.

Table 5.12: Data representation of SQ12

<b>Q12 - Enterprise Database Fragmentation is a feature of a Cloud security model that suggests that Cloud service providers should store the enterprise data set in fragments and implement access control for each fragment of the database. Do you agree that Enterprise Database Fragmentation in the Cloud would improve enterprise data security of a Cloud-based ERP software system?</b>			
#	Answer	%	Count
1	Definitely Agree	40.48%	17
2	Probably Agree	33.33%	14
3	Might or might not Agree	21.43%	9
4	Probably Disagree	4.76%	2
5	Definitely Disagree	0.00%	0
	Total	100%	42

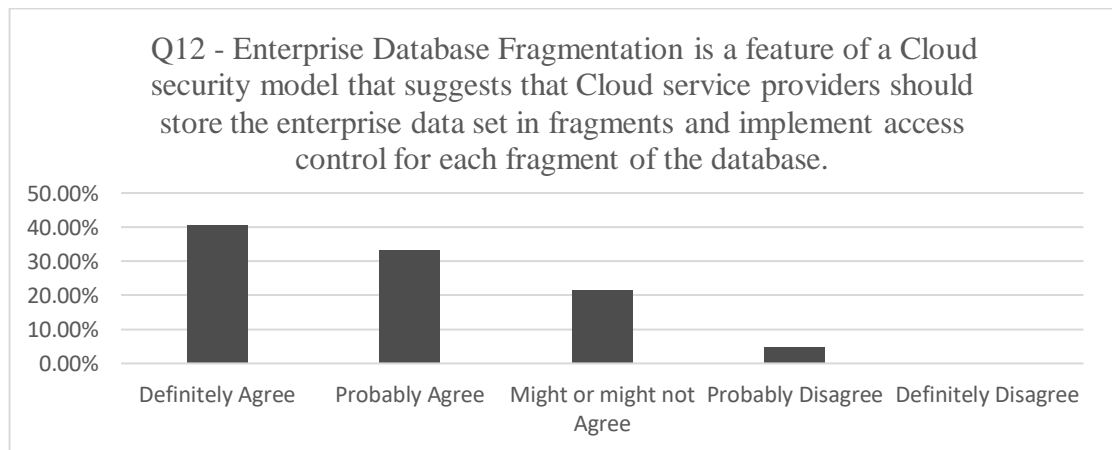


Figure 5.12: Bar Chart representation of collected data for SQ12

Table 5.12 and Figure 5.12 above show that out of the 44 participants, 42 answered this question. 40.48% believed that cloud service providers should store the enterprise data set in fragments and implement access control for each fragment of the database. 33.33% probably agreed with the importance of fragmentation of the data and access



control processing, while 21.43% remained undecided. They believed it might or might not have been useful. About 4.76% think that enterprise data set classification is of no importance for enterprise data security in the cloud. For this question, it can be stated that a mixed kind of response is received. One possible reason could be the individual differences or the different personality traits of each individual. Yet another reason could be making things easier. It is important that the employee can easily approach fragmented data. It could be possible for the study participants to select this option as important. Ensuring that employees can readily access fragmented data is crucial for operational efficiency.

Table 5.13: Data representation of SQ13

<b>Q13 - An Enterprise system that prompts the Enterprise System Administrator when there is an unsuccessful login attempt, is more likely to promote Enterprise data security in the Cloud. Do you agree with the above statement?</b>			
#	Answer	%	Count
1	Definitely Agree	<b>64.29%</b>	27
2	Probably Agree	<b>23.81%</b>	10
3	Might or might not Agree	<b>11.90%</b>	5
4	Probably Disagree	<b>0.00%</b>	0
5	Definitely Disagree	<b>0.00%</b>	0
	Total	100%	42

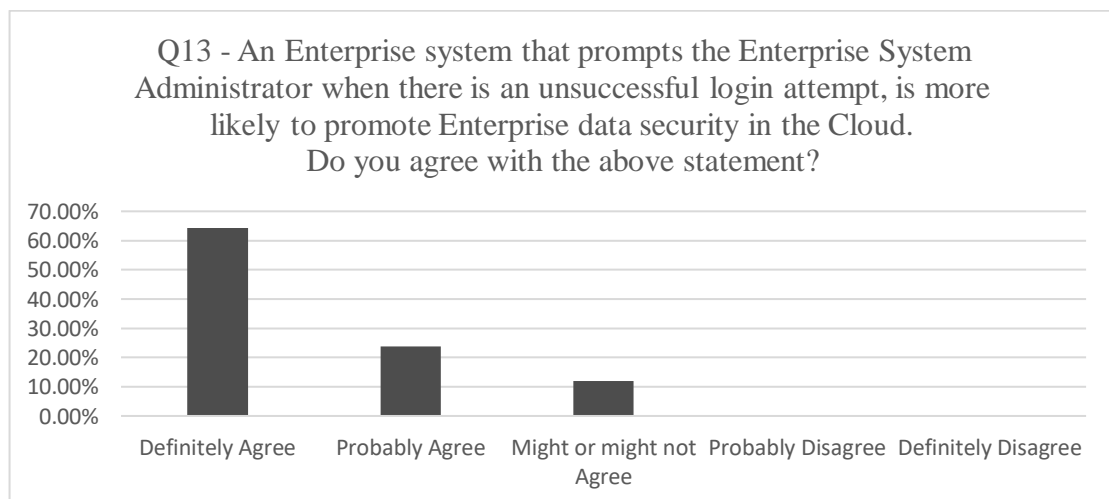


Figure 5.13: Bar Chart representation of collected data for SQ13

Table 5.13 and Figure 5.13, above, show that out of the 44 participants, 42 answered this question. 64.29% believed that an enterprise system that prompts the Enterprise System Administrator when there is an unsuccessful login attempt is more likely to promote enterprise data security in the cloud, 23.81% probably agreed that the Enterprise System Administrator is more likely to promote enterprise data security in the cloud-based on-going issues, and 11.90% remained undecided. They believed it might or might not have been useful. None of the study participants thought that unsuccessful logins prompts could not promote enterprise data security in the cloud. For this question, it can be stated that only positive responses are received.

Table 5.14: Data representation of SQ14

<b>Q14 - Does the current Cloud Security Model available in your Enterprise meet all your Enterprise needs for data security in the Cloud?</b>			
#	Answer	%	Count
1	Definitely Yes	23.81%	10
2	Probably Yes	33.33%	14
3	Neutral	33.33%	14
4	Probably No	4.76%	2
5	Definitely No	4.76%	2
	Total	100%	42

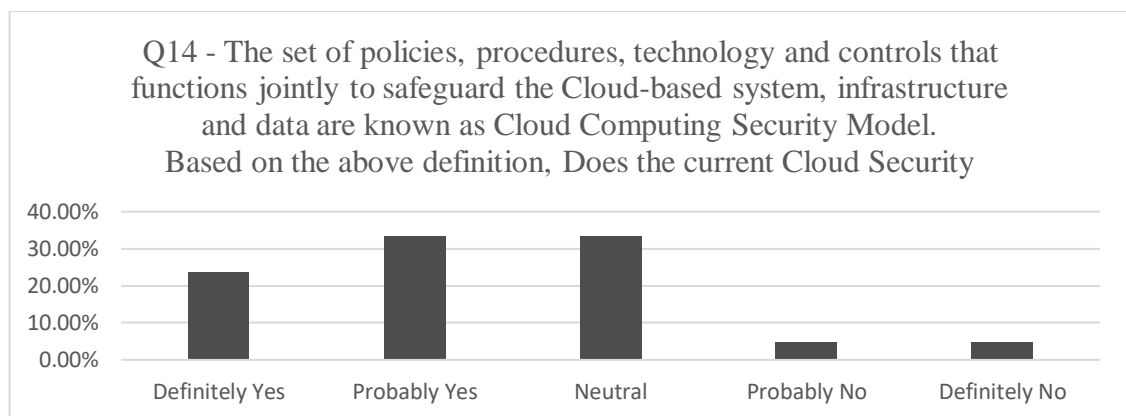


Figure 5.14: Bar Chart representation of collected data for SQ14

Table 5.14 and Figure 5.14, above, show that out of the 44 participants, 42 answered this question. 23.81% believed that the current Cloud Security Model available in their enterprise meets all their enterprise's needs for data security in the Cloud, while 33.33%

agreed with the efficiency of the current data security system in their enterprise. 33.33% remained undecided. About 4.76% think the current cloud security system is probably not efficient enough, and a similar percentage of study participants indicated that the current system is not good. Even though the majority thought the current system was good enough for data security, 33% of study participants and about 9% thought the system was not good enough. This shows that businesses should pay attention when they choose an adequate security system.

Table 5.15: Data representation of SQ15

<b>Q15 - From your experience, do you consider data security a major concern when your enterprise is adopting a cloud-based ERP software system?</b>			
#	Answer	%	Count
1	Definitely a major concern	<b>66.67%</b>	28
2	Probably a major concern	<b>14.29%</b>	6
3	Might or might not be a major concern	<b>11.90%</b>	5
4	Probably not a major concern	<b>7.14%</b>	3
5	Definitely not a major concern	<b>0.00%</b>	0
	Total	100%	42

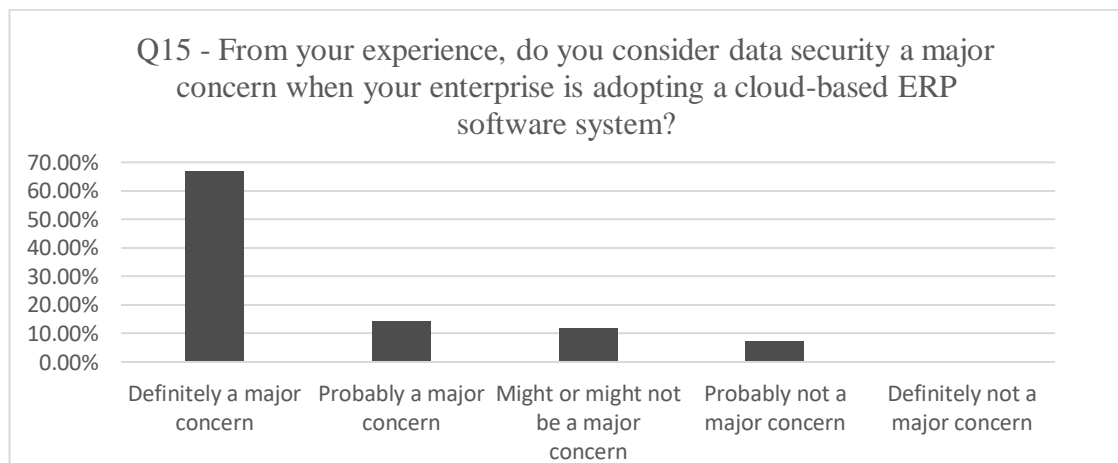


Figure.5.15: Bar Chart representation of collected data for SQ15

Table 5.15 and Figure 5.15 above show that 42 participants answered this question; 66.67% considered adopting an ERP software system a major concern, whereas 14.29% thought it was probably a major concern. 11.90% answered that it might or might not

be a major concern to adopt an ERP software system, whereas 7.14% thought it was probably not a major concern.

## 5.2 Statistical Analysis of our Research Assumptions

A Likert scale questionnaire is a common survey method used to measure attitudes, perceptions, opinions, or behaviors of individuals towards a particular topic. In analysing our Likert scale questionnaire, we followed a few steps. First was the descriptive data analysis above, using the bar charts to show a virtual percentage representation of what our data set looks like. The second step now is the statistical analysis of our research data set against our research assumptions or hypothesis, which formed the foundation of the views in our proposed framework. The first thing we did was to map the research questions against the research assumptions they are addressing, and also, we coded our Likert scale responses using 1, 2, 3, 4, and 5, as shown in Table 5.17 below, where 1 represents a negative not agreeing with the view, 3 is neutral, and 5 is a positive strong agreeing with the view. In many of the research questions, the wording for each response to each SQ varies, but the coded numbers always carry the same meaning: 1 = Strongly Disagree (SD), 2 = Disagree (D), 3 = Undecided (U), 4 = Agree (A), and 5 = Strongly Agree (SA). For example, for SQ1 and SQ14, the coded response 1 is Strongly Disagree even though the wording response for 1 is "Definitely a major concern" for SQ1 and "Definitely yes" for SQ14.

Table 5.16: The Assumption variables and the SQs Variables

Assumption Variables	SQs Variables
A1	SQ1, SQ2, SQ13, SQ14, SQ15
A2	SQ3
A3	SQ4, SQ8
A4	SQ5, SQ6, SQ7, SQ9, SQ10
A5	SQ10
A6	SQ11
A7	SQ13
A8	SQ12

Table 5.17: The Agreement Scale (Eya, 2023)

Likert Scale Coding	If our data set is up to or greater than 0.5 (Sig $\geq 0.05$ )	If our data set is less than 0.5 (Sig $< 0.05$ )
1 = Strongly Disagree (SD) 2 = Disagree (D) 3 = Undecided (U) 4 = Agree (A) 5 = Strongly Agree (SA)	Normally distribute Likert Scale data. (Parametric Method)	Not-Normally distributed Likert Scale data (Non-parametric Method)
	1. Linear Regression	1. Ordinal Regression
	2. Pearson Correlation	2. Spearman Rank Correlation

Table 5.16 above shows the research assumption variables and how they are related to the research SQs variables. Here, the primary variables are the SQs variables, while the secondary variables are the assumption variables. Under the assumption variables, A1 is the dependent variable, while A2 to A8 are the covariant variables. A1 is the dependent variable because this is the variable that addresses the assumption that participants who have worked with a cloud-based ERP system are more likely to provide a valid response to our research survey. Table 5.17 shows some options of statistical test we can conduct based on our research questions, but various statistical tests can be used to derive meaningful conclusions and insights from Likert scale survey data. The choice of statistical test depends on the objectives of the research, the nature of the data, and the specific hypotheses being examined. T-tests, ANOVA (Analysis of Variance), chi-square tests, Kruskal-Wallis tests, Mann-Whitney U tests, Wilcoxon Signed-Rank tests, and correlation analysis are common tests used with Likert scale data (Verma and Abdel-Salam, 2019).

These tests are selected based on the level of data measurement and research questions. The data on a Likert scale are ordinal, meaning they have a specific order but inconsistent intervals between response options (Verma and Abdel-Salam, 2019). This restricts the applicability of particular parametric tests that presume a normal distribution and equal intervals (Verma and Abdel-Salam, 2019). When parametric test

assumptions are not met, non-parametric tests are frequently preferred. To ensure we choose the appropriate test for our data we consulted a statistician or data analyst when selecting the appropriate statistical test to ensure the selected test correlates with the research objectives and data characteristics.

The reason for choosing Ordinal regression analysis, also known as ordinal logistic regression or proportional odds regression, is because it is utilised when dealing with an ordinal outcome variable with ordered categories that are separated by meaningful distance (Harrell et al., 2015). It is appropriate for ordinal data because it preserves the natural ordering of categories and takes into consideration the rank ordering of responses. Ordinal regression makes more effective use of available data, resulting in more accurate and reliable parameter estimates. It prevents the collapse of categories, which can lead to information loss when using linear regression on ordinal data (Kumar and Sankar, 2008). Ordinal regression is appropriate for analysing data with three or more response options because it can handle multiple categories which in our case, our SQs had mainly five responses (Harrell et al., 2015). It presupposes proportional odds, which means that predictor effects are constant across all levels of the outcome variable (Kumar and Sankar, 2008). This simplifies the model and makes its validity testable. Ordinal regression also provides results that are interpretable in terms of odds ratios, allowing one to comprehend the impact of predictors on the probability of belonging to a higher category (Harrell et al., 2015). It is adaptable and can accommodate various ordinal models, such as the proportional odds model, partial proportional odds model, and continuation ratio model.

The reason for choosing the Spearman rank correlation is because, it is a non-parametric measure of association between two variables, used when the assumptions of parametric correlation methods such as Pearson correlation cannot be satisfied (Prasad, 2023). It is appropriate for ordinal data and monotonic relationships (Puth et al., 2015). This is suitable for our collected data since a monotonic relationship is a relationship that does one of the following: (1) as the value of one variable increases,

so does the value of the other variable; or (2) as the value of one variable increases, the other variable value decreases. Spearman rank correlation is sensitive to changes in the ranks of the data as opposed to the actual values, which is advantageous when comparing data measured on various scales or units (Stephanou and Varughese, 2021). Spearman rank correlation is straightforward to calculate and does not assume a particular data distribution (Prasad, 2023). It makes no assertions regarding the distribution of the underlying data or the nature of the relationship between variables (Hung, et al., 2017). It does not detect certain types of relationships, such as curvilinear associations, and it may be excessively sensitive for large sample sizes (Hung, et al., 2017). It is crucial to interpret the results in light of the research questions and the nature of the data being analysed. In our case from the “test of normality” below, it shows we have “Not-Normally Distributed Likert Scale Data”; hence we will be using non-parametric method tests which includes “Ordinal Regression and Spearman Rank Correlation” which the reasons for choosing and benefits of these tests have been examined in the above paragraphs.

### **5.2.1. Test of Normality**

We wanted to see if our assumption variables were normally distributed after mapping our research variables and entering our data into SPSS. We first transformed our SQ variables into the assumption variables they are addressing by creating the assumptions variable, which is the mean of all the SQs addressing that particular research assumption. Some of the assumption variables have only one SQ addressing them. In that case, the resulting assumption variable will be a replica of the initial SQ that addresses them. It is important to check if our assumption variables are normally distributed because this will inform the type of analysis we will perform on our data. As shown in Table 5.17 above, if our assumption variables are normally distributed, we will be using the parametric method of research analysis, which is Linear Regression and Pearson Correlation. But when our assumption variables are not normally distributed, we will be using non-parametric research analysis tools, which are ordinal regression and spearman rank correlation. In our case, when our assumption variable has a significant statistic that is less than 0.05, we consider it not normally

distributed, but when our assumption variable has a significant statistic greater or equal to 0.05, we consider it normally distributed.

Table 5.18: Test of Normality of our Assumption Variables

<b>Tests of Normality</b>						
	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
A1	.188	43	.001	.808	43	.000
A2	.325	43	.000	.704	43	.000
A3	.246	43	.000	.704	43	.000
A4	.159	43	.008	.756	43	.000
A5	.306	43	.000	.737	43	.000
A6	.354	43	.000	.653	43	.000
A7	.336	43	.000	.644	43	.000
A8	.248	43	.000	.783	43	.000

Here we are using the Shapiro- Wilk, since our test set or number of research participants, is below 100. If our research participants were above 100, we will use the Kolmogorov- Smirnov values to make decisions about the normality of our assumption variables. From table 5.18 above, we can see that our assumptive variables are not normally distributed since we do not have any of the (Sig) values under Shapiro- wilk greater or equal to 0.05. Therefore, our assumption variables are not normally distributed because they are all statistically significant. It means that the responses collected from our survey do not follow a normal distribution although ordinal data are not necessarily expected to follow a normal distribution, as they represent categorical or ordered responses rather than continuous numerical values, the implications and considerations when dealing with non-normally distributed data in



our Likert scale questionnaire is that we are going to use nonparametric statistical tests. These tests do not rely on the assumption of normality and can be more appropriate for analysing ordinal data.

*Table 5.19: Case Processing Summary for "Test of Normality "*

<b>Case Processing Summary for "Test of Normality "</b>						
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
A1	43	100.0%	0	0.0%	43	100.0%
A2	43	100.0%	0	0.0%	43	100.0%
A3	43	100.0%	0	0.0%	43	100.0%
A4	43	100.0%	0	0.0%	43	100.0%
A5	43	100.0%	0	0.0%	43	100.0%
A6	43	100.0%	0	0.0%	43	100.0%
A7	43	100.0%	0	0.0%	43	100.0%
A8	43	100.0%	0	0.0%	43	100.0%

The Case Processing Summary is a statistical output generated by statistical tests, such as tests of normality. It provides information about the number of cases included in the analysis and those that were excluded (Ho, 2013). It comprises valid cases, which are the data points for which the normality assumption was evaluated, in the tests of normality. Cases excluded from the analysis due to lacking data constitute the missing cases. The sum of valid and lacking cases constitutes the total number of cases in the dataset. The case processing summary assists researchers in comprehending the number of data points considered in the test of normality and how missing data may influence the results and interpretations of the test of normality. It also considers the impact of lacking data on their analyses' reliability and validity. In our research, the table 5.19 above shows the case processing summary when testing our assumption variables for normality; it shows there were no missing participants and that we had 43 participants. Since all our assumption variables are valid cases and there are no missing or excluded cases, it also improves the validity of the test of normality of our assumption variables.

Table 5.20: The Descriptive Statistics of the each of the Assumption Variables

<b>Descriptive for our Assumption Variables A1 to A8.</b>			
		Statistic	Std. Error
A1	Mean	3.2558	.10166
	95% Confidence Interval for Mean		
	Lower Bound	3.0506	
	Upper Bound	3.4610	
	5% Trimmed Mean	3.3085	
	Median	3.4000	
	Variance	.444	
	Std. Deviation	.66666	
	Minimum	.20	
	Maximum	4.40	
	Range	4.20	
	Interquartile Range	.60	
	Skewness	-2.323	.361
	Kurtosis	9.836	.709
A2	Mean	4.2093	.18396
	95% Confidence Interval for Mean		
	Lower Bound	3.8381	
	Upper Bound	4.5805	
	5% Trimmed Mean	4.3656	
	Median	5.0000	
	Variance	1.455	
	Std. Deviation	1.20630	
	Minimum	.00	
	Maximum	5.00	

	Range		5.00	
	Interquartile Range		1.00	
	Skewness		-1.789	.361
	Kurtosis		3.106	.709
A3	Mean		4.3256	.14778
	95% Confidence Interval for Mean	Lower Bound	4.0273	
		Upper Bound	4.6238	
	5% Trimmed Mean		4.4541	
	Median		4.5000	
	Variance		.939	
	Std. Deviation		.96907	
	Minimum		.00	
	Maximum		5.00	
	Range		5.00	
	Interquartile Range		1.00	
	Skewness		-2.525	.361
	Kurtosis		8.648	.709
A4	Mean		4.0930	.12860
	95% Confidence Interval for Mean	Lower Bound	3.8335	
		Upper Bound	4.3526	
	5% Trimmed Mean		4.1742	
	Median		4.2000	
	Variance		.711	
	Std. Deviation		.84329	
	Minimum		.00	

	Maximum		5.00	
	Range		5.00	
	Interquartile Range		1.20	
	Skewness		-2.690	.361
	Kurtosis		12.421	.709
A5	Mean		4.1860	.16724
	95% Confidence Interval for Mean	Lower Bound	3.8485	
		Upper Bound	4.5235	
	5% Trimmed Mean		4.3101	
	Median		5.0000	
	Variance		1.203	
	Std. Deviation		1.09666	
	Minimum		.00	
	Maximum		5.00	
	Range		5.00	
	Interquartile Range		2.00	
	Skewness		-1.637	.361
	Kurtosis		3.568	.709
A6	Mean		4.3721	.15968
	95% Confidence Interval for Mean	Lower Bound	4.0499	
		Upper Bound	4.6943	
	5% Trimmed Mean		4.5168	
	Median		5.0000	
	Variance		1.096	
	Std. Deviation		1.04707	

	Minimum		.00	
	Maximum		5.00	
	Range		5.00	
	Interquartile Range		1.00	
	Skewness		-2.254	.361
	Kurtosis		6.352	.709
A7	Mean		4.3953	.14934
	95% Confidence Interval for Mean	Lower Bound	4.0940	
		Upper Bound	4.6967	
	5% Trimmed Mean		4.5168	
	Median		5.0000	
	Variance		.959	
	Std. Deviation		.97930	
	Minimum		.00	
	Maximum		5.00	
	Range		5.00	
	Interquartile Range		1.00	
	Skewness		-2.484	.361
	Kurtosis		8.598	.709
A8	Mean		4.0698	.16437
	95% Confidence Interval for Mean	Lower Bound	3.7381	
		Upper Bound	4.4015	
	5% Trimmed Mean		4.1809	
	Median		4.0000	
	Variance		1.162	

Std. Deviation	1.07781	
Minimum	.00	
Maximum	5.00	
Range	5.00	
Interquartile Range	2.00	
Skewness	-1.460	.361
Kurtosis	3.287	.709

Descriptive statistics are concise measures employed to comprehend the fundamental characteristics of a dataset, especially when dealing with assumption variables (Johnson and Bhattacharyya, 2019). Statistics such as the mean, median, mode, standard deviation, range, interquartile range, skewness, kurtosis, and percentiles have been used frequently by researchers (Islam et al., 2018). The mean is the arithmetic average of the variables, whereas the median is the intermediate value. The mode is the value that occurs most frequently in a data set, whereas the standard deviation measures the spread or dispersion of the data. The range is the difference between the maximum and minimum values, while the interquartile range is the range between the first and third quartiles. The skewness statistic measures the asymmetry of the data distribution, whereas the kurtosis statistic measures the distribution's shape. Percentiles categorise the data into discrete groups (Johnson and Bhattacharyya, 2019).

Descriptive statistics are a crucial first stage in our data analysis because it enable us to comprehend the nature of your assumption variables, which inform subsequent statistical tests and analyses. Table 5.20 above is the descriptive statistics of the different assumption variables against the following Mean, 95% Confidence Interval for Mean: Lower Bound and Upper Bound, 5% Trimmed Mean, Median, Variance, Std. Deviation, Minimum, Maximum, Range, Interquartile Range, Skewness and Kurtosis as generated from the SPSS used in analysing our dataset.

The second test of normality we did, was the Log10 of A1, A3 and A4. We had to do this because these three assumption variables have more than one SQs that make them up. We wanted to ensure that these variables are not normally distributed as seen in our first test of assumption variables. Therefore, after taking the natural logarithm of the three assumption variables A1, A3, and A4 in our data, we wish to determine if the transformed data Log10 of A1, A3 and A4 adhere to a normal distribution. This log transformation is often used to make a dataset more normally distributed when the original data is positively skewed as in our case, we had more than one SQs for each of these Assumption variables.

Table 5.21: Test of Normality of the Log10 A1, A3 and A4

<b>Tests of Normality of Log A1, A3 and A4</b>						
	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	df	Sig.
log_A1	.156	42	.012	.937	42	.022
log_A3	.257	42	.000	.752	42	.000
log_A4	.128	42	.084	.932	42	.016

Even with the Log10 of A1, A3 and A4, our variables' data responses are still not normally distributed because it is just log\_A4 is 0.16 which is above 0.05, but the other two log\_A1 and log\_A3 are below 0.05 for their Sig value under the Shapiro-Wilk as shown in Table 5.21 above. Having proven that our data set for our assumption variables are not normally distributed, this suggests that the data does not exhibit the typical bell-shaped curve associated with normal distribution, which can have implications for certain statistical analyses and interpretations. It may necessitate the use of alternative analytical techniques or caution in drawing conclusions that rely on assumptions of normality. We are going to use the non-parametric method in analysing our data set. Firstly, we adopted the use of ordinal regression analysis to perform our analysis.

Table 5.22: Case Processing Summary for log\_A1, log\_A3 and log\_A4

Case Processing Summary for log_A1, log_A3 and log_A4						
Cases						
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
log_A1	42	97.7%	1	2.3%	43	100.0%
log_A3	42	97.7%	1	2.3%	43	100.0%
log_A4	42	97.7%	1	2.3%	43	100.0%

Table 5.22 above shows that for the log\_A1, log\_A3 and log\_A4, we have one missing number which amounts to the value of 2.3% of the total value. Therefore, 97.7% percent of the test set was used when executing the test of normality for this group of assumption variables.

Table 5.23: The Descriptive Statistics of the each of the Assumption Variables for log\_A1, log\_A3 and log\_A4

Descriptive for log_A1, log_A3 and log_A4			
		Statistic	Std. Error
log_A1	Mean	.5178	.00995
	95% Confidence Interval for Mean Lower Bound	.4977	
	Upper Bound	.5378	
	5% Trimmed Mean	.5209	
	Median	.5315	
	Variance	.004	
	Std. Deviation	.06448	
	Minimum	.34	
	Maximum	.64	



	Range	.30	
	Interquartile Range	.08	
	Skewness	-.793	.365
	Kurtosis	1.265	.717
log_A3	Mean	.6399	.01222
	95% Confidence Interval for Mean Lower Bound	.6152	
	Upper Bound	.6645	
	5% Trimmed Mean	.6498	
	Median	.6532	
	Variance	.006	
	Std. Deviation	.07917	
	Minimum	.40	
	Maximum	.70	
	Range	.30	
	Interquartile Range	.10	
	Skewness	-1.678	.365
	Kurtosis	2.613	.717
log_A4	Mean	.6185	.00899
	95% Confidence Interval for Mean Lower Bound	.6003	
	Upper Bound	.6366	
	5% Trimmed Mean	.6195	
	Median	.6232	
	Variance	.003	
	Std. Deviation	.05829	
	Minimum	.51	

Maximum	.70	
Range	.19	
Interquartile Range	.11	
Skewness	-.124	.365
Kurtosis	-1.215	.717

Table 5.23 above is the description of the different assumption variables for log\_A1, log\_A3 and log\_A4 against the following: Mean, 95% Confidence Interval for Mean: Lower Bound and Upper Bound, 5% Trimmed Mean, Median, Variance, Std. Deviation, Minimum, Maximum, Range, Interquartile Range, Skewness and Kurtosis. Descriptive statistics are an important first step in our data analysis because they help us understand the nature of our assumption variables, which in turn guide the statistical tests and analyses that follow.

### 5.2.2. Ordinal Regression

Ordinal regression is a statistical technique used when there is a dependent variable and one or more independent variables (Gutiérrez et al., 2015). In our case, A1 is the dependent variable, while A2 to A8 are the covariant variables. In ordinal regression, the case processing summary provides information about data management and processing during analysis (Gutiérrez et al., 2015). It comprises the number of cases, missing values, unweighted cases, weighted cases, the final model, model fit statistics, and information criteria (Gutiérrez et al., 2015). It is crucial to us to be aware of missing values, as they can affect the validity of results. Missing data can introduce bias, distort statistical analyses, and undermine the accuracy of findings, making it essential to address them appropriately through techniques such as imputation or sensitivity analysis.

By acknowledging and addressing missing values, researchers can enhance the integrity and robustness of their analyses, ensuring that conclusions drawn from the

data are sound and trustworthy. Understanding the case processing summary is essential for conducting accurate and trustworthy analyses, as it enables researchers to make informed decisions regarding the model's fit and validity.

Table 5.24: Ordinal Regression Case Processing Summary

Case Processing Summary			
		N	Marginal Percentage
A1	.20	1	2.3%
	2.20	2	4.7%
	2.60	2	4.7%
	2.80	2	4.7%
	3.00	6	14.0%
	3.20	6	14.0%
	3.40	9	20.9%
	3.60	8	18.6%
	3.80	4	9.3%
	4.20	2	4.7%
	4.40	1	2.3%
	Valid		43
Missing		0	
Total		43	

Table 5.24 above simply show shows the case processing summary for the ordinal regression where each of the assumptions is allocated a marginal percentage. For the ordinal regression analysis, we had a total of 43 valid representations which represent the 100% of our data set. This ordinal analysis will be used to determine our model-fitting information and the goodness of fit, pseudo-R-Square and the parametric

estimate of our data set. Below Tables, 5.25 to 5.30 show what the result of our ordinal regression analysis looked like.

*Table 5.25: Model Fitting Information*

<b>Model Fitting Information</b>				
Model	-2 Log-Likelihood	Chi-Square	df	Sig.
Intercept Only	172.301			
Final	127.178	45.122	7	.000

"Model Fitting Information" in ordinal regression analysis is the set of numbers and other data that show how well the chosen model fits the data that was collected (Omar, 2019). It is very important for figuring out how good and right the model is and for making smart choices about how the independent variable and the dependent variables are related (Omar, 2019). The likelihood ratio chi-squared statistic, variance statistic, log-likelihood value, number of parameters, and pseudo-R-squared measures are some of the most important pieces of model fitting information. Comparing the log-likelihood of the model with the data to the log-likelihood of a null model, we can find out how well the model fits the data generally. If your chi-squared estimate for the likelihood ratio is significant, it means that your model fits the data better than the null model.

Furthermore, the deviance statistic shows how well the model matches the data. It measures the difference between the data that was collected and the data that would have been expected if the model had been matched (Li, et al., 2008). A better fit to the data is shown by a lower deviance number. The likelihood ratio chi-squared measure is based on the difference between how different your model is from a null model in terms of difference (Omar, 2019). To figure out how much of the variation can be explained by the model, pseudo-R-squared measures are used. Overall, model fitting information is very important for figuring out if your ordinal regression model is good enough. It helps you figure out if the model does a good job of explaining how your independent variables relate to the dependent variables ordered groups. If you want to

draw valid conclusions from your research and make accurate predictions based on the model, you need to make sure the model fits well. Table 5.25 above shows that our framework fits our data set very well, you can see that this model fitting information is statistically significant. This is because the Sig value number here is less than 0.05, which means that our framework fits the data very well.

Table 5.26: Goodness of fit

<b>Goodness-of-Fit</b>			
	Chi-Square	df	Sig.
Pearson	288.509	333	.963
Deviance	118.836	333	1.000

Also, Table 5.26 above “goodness of fit” shows that Sig is 0.963 for Pearson and 1.000 for Deviance which is both greater than 0.05, therefore meaning that our framework fits our data set very well. This specific goodness of fit comprises the Pearson and Deviance tests, which are employed to assess the degree to which a model conforms well to the observed data. Negligible test results serve as indicators that the framework adequately corresponds to the data. The Pearson correlation coefficient (0.963) and the Deviance coefficient (1.000) are both non-statistically significant in our case, indicating that the framework suits the data set exceptionally well. Both the Pearson value (0.963), which exceeds the significance level of 0.05, and the Deviance value (1.000), which is also greater than 0.05, are positive. This demonstrates that our framework suits the data exceptionally well. We desire for neither of the two to be statistically significant.

Table 5.27: Pseudo R-Square

<b>Pseudo R-Square</b>	
Cox and Snell	.650
Nagelkerke	.659
McFadden	.243

Table 5.27 above shows the Pseudo R-square, for this we will focus on the Nagelkerke value of 0.658, which simply means the 66% change on the dependent variable A1 whereas a result of the independent variables A2 to A8. However, the next thing to look at is the parametric estimates but before we look at the parametric estimates, we look at the test of parallel lines.

### 5.2.3. Test of Parallel Lines

Table 5.28: Test of Parallel Lines

Model	-2 Log-Likelihood	Chi-Square	df	Sig.
Null Hypothesis	127.178			
General	62.846 <sup>b</sup>	64.332 <sup>c</sup>	63	.430

Table 5.28 above is the test of parallel line tests for the assumption of proportional odds. The proportional odds assumption in ordinal regression analysis assumes that the odds of an observation falling into a dependent variable's category are proportional across different levels of independent variables. We want the test of parallel line not to be statistically significant (Sig value) to make sure we haven't broken the proportional odds. This checks the non-hypothesis that each of the explanatory variables is consistent or different across various thresholds of the outcome variable. In our case here, table 5.28 above shows we have not violated it since our probability value here is greater than 0.05, we have 0.430. If the Sig p-value is significant, it implies that the assumption is violated, When the significance level (p-value) obtained from a statistical test is deemed significant, it suggests that the assumption being tested is violated. In other words, the observed data significantly deviates from what would be expected under the assumption being evaluated. This violation indicates that the

conditions required for the validity of the statistical analysis or model may not hold, prompting researchers to reconsider their approach or interpretation of the results. Since we have not violated the proportional probability odd, we can now proceed to interpret our parameters estimate table 5.29 and 5.30 below.

Table 5.29: Ordinal Regression Parametric Estimates of the Lower Bound

<b>Parameter Estimates</b>							95% Confidence Interval
		Estimate	Std. Error	Wald	df	Sig.	Lower Bound
Threshold	[A1 = .20]	6.759	20.804	.106	1	.745	-34.015
	[A1 = 2.20]	14.684	3.339	19.343	1	.000	8.140
	[A1 = 2.60]	15.793	3.393	21.667	1	.000	9.143
	[A1 = 2.80]	16.515	3.450	22.918	1	.000	9.754
	[A1 = 3.00]	17.871	3.578	24.946	1	.000	10.858
	[A1 = 3.20]	18.909	3.680	26.406	1	.000	11.697
	[A1 = 3.40]	20.486	3.854	28.255	1	.000	12.933
	[A1 = 3.60]	22.184	4.055	29.928	1	.000	14.236
	[A1 = 3.80]	23.507	4.182	31.601	1	.000	15.311
	[A1 = 4.20]	24.898	4.299	33.544	1	.000	16.472
Location	A2	.179	.315	.322	1	.570	-.439
	A3	-.611	.521	1.376	1	.241	-1.633
	A4	4.281	1.050	16.611	1	.000	2.222
	A5	-.838	.482	3.026	1	.082	-1.783
	A6	-.461	.457	1.019	1	.313	-1.357
	A7	1.327	.500	7.051	1	.008	.348
	A8	.738	.435	2.882	1	.090	-.114

In ordinal regression analysis, the estimation of model parameters is necessary in order to ascertain the manner in which the independent variables impact the probabilities or odds associated with the ordinal categories. Parameter estimates may be influenced by the particular ordinal regression model employed. When using ordinal regression models, the parameter values helped us figure out how the independent variables and the ordinal response are connected. So, when the coefficient is positive, the chances of being in a higher group go up, and when it is negative, they go down. For example, in our case, our proposed framework was analysed by selecting eight assumptions which are now our eight variables related to the concepts that formed our proposed framework:

- A1- Participant Cloud Experience Advantage -The research survey is more likely to be valid when participants have experience working with a cloud-based ERP system.
- A2 - Technology Impact - Cloud computing upgrades can impact enterprise system data security, potentially affecting previous technology, but this impact can be positive or negative.
- A3- Shared Responsibility - Sharing the security responsibility of the cloud system between the Cloud Service Provider and Cloud Service End-users leads to more secure enterprise data in the cloud.
- A4- Improved Security- Proper Access Management within the Cloud Service End-user enterprise can enhance their enterprise data security in the Cloud.
- A5- CSP Access Directory - The implementation of the proposed CSP Access Directory is expected to enhance Access Control Management in the Cloud for the adopting enterprise.
- A6- Enterprise Data Classification- Classifying enterprise data sets in the cloud can enhance security and create an Enterprise Access Directory by only transferring classified data.
- A7- Security Notification- System notifications to the Enterprise System Administrator when an unsuccessful login attempt occurs, is likely to enhance Enterprise data security in the Cloud.
- A8- Enterprise Database Fragmentation- The implementation of Enterprise Database Fragmentation in the Cloud can enhance the security of enterprise data within a Cloud-based ERP system.

When interpreting the parameter estimates, it is crucial to consider both the particular ordinal regression model that was employed and the characteristics of the data. The variability of the interpretation is contingent upon the assumptions and limitations of



the selected model. Consensus regarding the associations between the ordinal response and the independent variables is typically reached through examination of the estimated coefficients, their significance (p-values), and confidence intervals. In our case, we concluded that five variables (A2-Technology Impact, A3-Shared Responsibility, A5-CSP Access Directory, A6-Enterprise Data Classification, A8-Enterprise Database Fragmentation) A2, A3, A5, A6 and A8 have significant effects on participants' cloud experience in their enterprises, and that means the ordinal logistic regression model adopted has an ability to predict participant's cloud experience advantage level very well in relation to the responses to the survey question.

Table 5.30: Ordinal Regression Parametric Estimates of the Upper Bound

<b>Parameter Estimates</b>		95% Confidence Interval
		Upper Bound
Threshold	[A1 = .20]	47.534
	[A1 = 2.20]	21.228
	[A1 = 2.60]	22.443
	[A1 = 2.80]	23.277
	[A1 = 3.00]	24.884
	[A1 = 3.20]	26.121
	[A1 = 3.40]	28.040
	[A1 = 3.60]	30.132
	[A1 = 3.80]	31.703
	[A1 = 4.20]	33.324
Location	A2	.797
	A3	.410
	A4	6.339

A5	.106
A6	.434
A7	2.307
A8	1.590

#### 5.2.4. Nonparametric Correlation

Nonparametric correlation is a statistical method used to measure the strength and direction of association between two variables when the assumptions of traditional parametric correlation tests, such as Pearson correlation, are not met. Unlike parametric methods, nonparametric correlation does not rely on assumptions about the distribution of the data or the relationship between variables. Instead, it assesses the relationship between variables based on the ranks of their values. The table 5.31 and table 5.32 below shows the results of the correlation analysis and more detailed interpretation is found in section 5.2.5.

Table 5.31: Correlations Analysis I

<b>Correlations</b>			A1	A2	A3	A4
Spearman's rho	A1	Correlation Coefficient	1.000	.450**	.402**	.659**
		Sig. (2-tailed)	.	.002	.007	.000
		N	43	43	43	43
	A2	Correlation Coefficient	.450**	1.000	.495**	.470**
		Sig. (2-tailed)	.002	.	.001	.001
		N	43	43	43	43
	A3	Correlation Coefficient	.402**	.495**	1.000	.580**
		Sig. (2-tailed)	.007	.001	.	.000
		N	43	43	43	43

A4	Correlation Coefficient	.659**	.470**	.580**	1.000
	Sig. (2-tailed)	.000	.001	.000	.
	N	43	43	43	43
A5	Correlation Coefficient	.544**	.485**	.367*	.742**
	Sig. (2-tailed)	.000	.001	.016	.000
	N	43	43	43	43
A6	Correlation Coefficient	.410**	.439**	.380*	.594**
	Sig. (2-tailed)	.006	.003	.012	.000
	N	43	43	43	43
A7	Correlation Coefficient	.430**	.392**	.273	.237
	Sig. (2-tailed)	.004	.009	.077	.126
	N	43	43	43	43
A8	Correlation Coefficient	.543**	.527**	.583**	.538**
	Sig. (2-tailed)	.000	.000	.000	.000
	N	43	43	43	43

Table 5.32: Correlations Analysis II

		Correlations				
		A5	A6	A7	A8	
Spearman's rho	A1	Correlation Coefficient	.544**	.410**	.430**	.543**
		Sig. (2-tailed)	.000	.006	.004	.000
		N	43	43	43	43
	A2	Correlation Coefficient	.485**	.439**	.392**	.527**
		Sig. (2-tailed)	.001	.003	.009	.000
		N	43	43	43	43

A3	Correlation Coefficient	.367*	.380*	.273	.583**
	Sig. (2-tailed)	.016	.012	.077	.000
	N	43	43	43	43
A4	Correlation Coefficient	.742**	.594**	.237	.538**
	Sig. (2-tailed)	.000	.000	.126	.000
	N	43	43	43	43
A5	Correlation Coefficient	1.000	.483**	.363*	.586**
	Sig. (2-tailed)	.	.001	.017	.000
	N	43	43	43	43
A6	Correlation Coefficient	.483**	1.000	.363*	.410**
	Sig. (2-tailed)	.001	.	.017	.006
	N	43	43	43	43
A7	Correlation Coefficient	.363*	.363*	1.000	.450**
	Sig. (2-tailed)	.017	.017	.	.002
	N	43	43	43	43
A8	Correlation Coefficient	.586**	.410**	.450**	1.000
	Sig. (2-tailed)	.000	.006	.002	.
	N	43	43	43	43

### 5.2.5. Interpretation of the Data Presented in the Table 5.24 to 5.32.

The first result we have is a “case processing summary” as you can see here in table 5.24 and the second table 5.25 here is “model fitting information”. This model fitting information is statistically significant as you can see here, the model fitting table tells us how well the framework fits the data, as you can see here it is statically significant as the value here is less than 0.05 which means our framework fits the data very well. The next thing we need to look at is what we call the “goodness of fit” in table 5.26. This particular goodness of fit contains the Pearson and deviance test, which are used

to determine whether a model exhibits a good fit to the data. Non-significant test results are indicators that the framework fits the data well. In our case, you can see that the Pearson (0.963) and Deviance (1.000) are non-statistically significant, which clearly shows that the framework fits the data set very well. The Pearson value is (0.963) which is greater than (0.05) also the Deviance value is (1.000) which is also greater than (0.05). This goes to show our framework fits that data very well. We want the two not to be statistically significant.

The next we look at is the “Pseudo R – Square” in table 5.27, we simply concentrate on the “Nagelkerke”. This is more like the R-Square for Linear Regression. The particular value of the “Nagelkerke” (0.659) simply tells us that 66% percent change in the dependant variables as we can see here. The next thing we look at is the “parameter estimate” in table 5.29 and table 5.30, however before we look at this parameter estimate, we need to look at the “test of parallel lines” in table 5.28, to be sure we have not violated this particular test of parallel lines. This particular test of parallel lines here tests for the assumptions of proportional odds. This tests the non-hypothesis that the odds of each “explanatory variable” are constant or are distinct across the different thresholds of the outcome variables. Therefore, we want it not to be statistically significant for us to be sure we have not violated the test of proportional odds. In our case here we have not violated it because the probability value here is greater than 0.05 which is 0.430 which is the significant value here.

However, if we discover that we have violated the test of parallel lines assumption of proportional odds, let’s say now the sig value is less than (0.05), we will simply adopt what is called the “multinomial logistic regression” to explore our odds and analyse our data. Multinomial logistic regression (often just called 'multinomial regression') is used to predict a nominal dependent variable given one or more independent variables. It is sometimes considered an extension of binomial logistic regression to allow for a dependent variable with more than two categories. But in our case, we have not violated it, so we can go ahead and interpret these parameter estimates. Now for us to interpret these parameter estimates, we will take a look at some things first. As you

can see the independent variables here are A2, A3, A4, A5, A6, A7 and A8. The A4=0.000 and A7=0.008 are statistically significant going by the probability values which are less than 0.05. The A2, A3, A5, A6 and A8 are all not statistically significant as their sig value is greater than 0.05. So, to interpret this result, we interpret the coefficient as well as the sig value. The ordinal regression co-efficient is simply interpreted as the estimated or predicted change in log odds of being in a higher (as opposed to a lower) group or category on the dependent variables (controlling for the remaining independent variables) per unit increase on the independent variables.

The *positive* estimate or coefficients is interpreted as follows: For every one-unit increase on an independent variable, there is a predicted increase (of a certain value) in the log odds of falling at a higher level on the dependent variables. More generally, this indicates that there is an increased probability of falling at a greater level on the dependant variable as values rise on independent variables. For the A4 and A7 which have a significant positive predictor of A1, for every one-unit increase in A4 and A7, there is a predicted increase of (A4 = 4.281, A7 = 1.327) in the log odds of being at a higher level on A1 employee experience. This statement above is simply explaining the relationship between two independent variables, A4 and A7, and the ordinal dependent variable A1 (which represents employee experience) in the context of an ordinal regression analysis.

Furthermore, the paragraphs below are an evaluation of the fundamental points made in the above statement. "A4 and A7 which have a significant positive predictor of A1": This part of the statement is telling us that variables A4 and A7 are considered significant predictors of the ordinal variable A1 in the ordinal regression model. In other words, A4 and A7 have been found to have a statistically significant positive relationship with the employee experience variable A1. "For every one-unit increase in A4 and A7": This part indicates that the statement is focusing on the effect of a one-unit increase in the values of A4 and A7. "There is a predicted increase of (A4 = 4.281, A7 = 1.327) in the log odds of being at a higher level on A1 employee experience": This part provides specific information about the predicted impact of a one-unit

increase in A4 and A7 on the log odds of experiencing a higher level of employee experience (A1).

So, in practical terms, relating to our research questions and assumptions, if A4 increases by one unit, it is predicted that the log odds of being at a higher level on the employee experience scale (A1) will increase by 4.281. If A7 increases by one unit, it is predicted that the log odds of being at a higher level on the employee experience scale (A1) will increase by 1.327. In ordinal regression, the log odds represent the natural logarithm of the odds, and they are used to model the relationship between the independent variables and the ordinal response variable (Hedeker, 2008). A positive increase in the log odds suggests a higher probability of moving to a higher level on the ordinal scale (in this case, a better employee experience). These findings indicate that both A4 and A7 are positively associated with higher employee experience levels, and the specific values (4.281 for A4 and 1.327 for A7) quantify the strength of these associations in terms of log odds. This information helped in understanding and predicting the impact of changes in A4 and A7 on the likelihood of higher employee experience levels.

The *negative* estimates or coefficients are interpreted as follows: For every one-unit increase on the independent variable, there is a predicted decrease of a certain amount in the log odds of being at a higher level on the dependent variable. This simply means that, as the values of the independent variable increase, there is a decreased probability of falling at a higher level on the dependent variables. For A2, A3, A5, A6 and A8 which have a negative significant predictor of A1, The negative coefficient values ( A2=0.179, A3=-0.611, A5= -0.838, A6= -0.461, A8= 0.738) shows that every one unit increase in A2, A3, A5, A6 and A8, there is a predicated decrease of ( A2=0.179, A3=-0.611, A5= -0.838, A6= -0.461, A8= 0.738 ) in the log odds of being at a higher level on A1, which represents the number of years of experience for employees." Subsequently, "For A2, A3, A5, A6, and A8 which have a negative significant predictor of A1": This part of the statement indicates that variables A2, A3, A5, A6, and A8 are considered significant predictors of the ordinal variable A1 (employee

years of experience) in the ordinal regression model. However, these predictors have a statistically significant negative relationship with A1. "the negative coefficient values (A2=0.179, A3=-0.611, A5=-0.838, A6=-0.461, A8=0.738) show that every one-unit increase in A2, A3, A5, A6, and A8 results in a predicted decrease of (A2=0.179, A3=-0.611, A5=-0.838, A6=-0.461, A8=0.738) in the log odds of being at a higher level on A1": This indicates specific information about the impact of a one-unit increase in the values of A2, A3, A5, A6, and A8 on the log odds of experiencing a higher level of employee years of experience (A1).

So, in practical terms, relating to our research questions and assumptions, for A2, every one-unit increase in its value results in a predicted decrease of 0.179 in the log odds of having a higher number of years of experience (A1). For A3, every one-unit increase in its value results in a predicted decrease of 0.611 in the log odds of having a higher number of years of experience (A1). For A5, every one-unit increase in its value results in a predicted decrease of 0.838 in the log odds of having a higher number of years of experience (A1). For A6, every one-unit increase in its value results in a predicted decrease of 0.461 in the log odds of having a higher number of years of experience (A1). For A8, every one-unit increase in its value results in a predicted decrease of 0.738 in the log odds of having a higher number of years of experience (A1). These findings indicate that A2, A3, A5, A6, and A8 are negatively associated with having a higher number of years of experience. In other words, an increase in the values of these variables is associated with a decrease in the likelihood of having more years of experience. The specific coefficient values quantify the strength of these associations in terms of log odds. Simply put, a participant years of experience with cloud-based ERP system have no impact on the outcome of the responses gotten from the survey, although we assumed this should have an impact but from the data collected from participants show others for A2, A3, A5, A6, and A8 but for A4 and A7 is the opposite. For the second method used, one of the key differences between the first and second method results is the Exp(B) column and confidence interval. The Exp (B) column contains odds ratios reflecting the multiplicative change in the odds of being in a higher category on the dependent variable for every one-unit increase on the independent variable, holding the remaining independent variables constant. An odd ratio > 1



suggests an increased probability of being at a higher level on the dependent variable as values on an independent variable increase. Whereas a ratio  $< 1$  suggests no predicated change in the likelihood of being in a higher category as values on an independent variable increase. An odd ratio = 1 suggests no predicated change in the likelihood of being in a higher category as values on independent variables increase. The odds ratio for (A4 and A7), the odds ratio indicates that the odds of being in a higher level on employee number of years' experience A1 increases by a factor of (A4=8.115, A7 = 1.396), for every one-unit increase in A4 and A7.

The odds ratio for A2, A3, A5, A6 and A8; the odds ratio indicates that the odds of being in a higher level on employee number of years' experience A1 increases by a factor of (A2= 0.0573, A3= 0.186, A5= 0.160, A6= 0.252, A8= 0.866) for every one-unit increase in A2, A3, A5, A6 and A8. Given that the odds ratio is  $<1$ , this indicates a decreasing probability of being at a higher level on the employee performance as values increase on A2, A3, A5, A6 and A8. This is how the ordinal regression analysis was performed especially when our datasets are not normally distributed.

The next analysis we performed was the correlation analysis, knowing our dataset is not normally distributed, we are going to use Spearman Rank Correlation analysis instead of the Pearson correlation. As we can see from the non-parametric correlation, the correlation between A2 and Spearman rho A1 is 0.450 which shows a moderate correlation between the two, and it is also found to be statistically significant going by the probability value here which is 0.002, which is less than 0.05.

Also looking at the correlation between the A3 and the Spearman rho A1 is 0.402 which shows a moderate correction between the two and it is also found to be statistically significant going by the probability value here which is 0.007 is less than 0.05. Also looking at the correlation between the A4 and the Spearman rho A1 is 0.659 which shows a moderate correction between the two and it is also found to be statistically significant going by the probability value here which is 0.000 is less than 0.05. Also looking at the correlation between the A5 and the Spearman rho A1 is 0.544

which shows a moderate correlation between the two and it is also found to be statistically significant going by the probability value here which is 0.000 is less than 0.05. Also looking at the correlation between the A6 and the Spearman rho A1 is 0.410 which shows a moderate correlation between the two and it is also found to be statistically significant going by the probability value here which is 0.006 is less than 0.05. Also looking at the correlation between the A7 and the Spearman rho A1 is 0.430 which shows a moderate correlation between the two and it is also found to be statistically significant going by the probability value here which is 0.004 is less than 0.05. Also looking at the correlation between the A8 and the Spearman rho A1 is 0.543 which shows a moderate correlation between the two and it is also found to be statistically significant going by the probability value here which is 0.000 is less than 0.05. Subsequently, all the assumptions A1, A2, A3, A4, A5, A6, A7 and A8 have some moderate correlation to the spearman rho A1 and are all also statistically significant.

### **5.3 Summary of Chapter 5**

Chapter 5 provides an in-depth examination of the quantitative data analysis we conducted to gain a better understanding of how the perspectives of our survey participants support end-user security responsibility in ensuring enterprise data security in public cloud. This understanding is crucial for uncovering meaning and assisting in the formulation of explanations for deficiencies in the information security culture of small and medium-sized enterprises (SMEs) in Nigeria. The present chapter is structured into two distinct sections. "Quantitative Data Visualisation Using Tables and Bar Charts" is the title of the initial section 5.1, which includes a summary of each survey question and the corresponding data. We implemented bar charts and tables to visually represent the responses obtained for every survey inquiry. The statistical analysis of our research hypotheses comprises the second section of this chapter. This section will use SPSS to analyse the collected data to determine whether or not the proposed framework's assumptions are supported from the data collected from the survey. The tests of normality, ordinal regression, the test of parallel lines, and non-parametric correlations were conducted and are represented by tables in section 5.2.

The development of research assumptions and the conceptual framework were covered in the preceding chapter 2 and chapter 4. This chapter conducts an analysis of the data obtained from the survey participants through the utilisation of various data analysis techniques, including tests of normality, ordinal regression, the test of parallel lines, and non-parametric correlations. Assessments of validity and reliability were performed on the confirming data that the responses to the survey were valid and reliable. In order to produce suitable outcomes, data screening software including using SPSS were put to work. Following the application of various techniques to the data analysis, the research assumptions were evaluated, and the information provided accordingly.

A cumulative sum of 43 responses to the survey were gathered from the research participants. Out of the total 43 responses, there were no missing values. In order to assess the adequacy, dependability, and validity of the data, an analysis was conducted using tests of normality, test of parallel lines, ordinal regression and spearman rank correlation. The primary results suggest that there is a positive correlation between employee experience levels (A1) and both research assumptions A4 and A7. The severity of this relationship is measured in log odds for A4 (4.281) and A7 (1.327). This data facilitated comprehension and forecasting regarding the influence of modifications in A4 and A7 on the probability of increased employee experience levels (A1).

Additionally, our results show that research assumptions A2, A3, A5, A6, and A8 are all linked to having less experience compared to having more experience. That is, as these factors' values rise, the chance of having more years of experience falls. In terms of log odds, the specific coefficient numbers show how strong these links are. Simply put, the number of years of experience a participant has with a cloud-based ERP system doesn't change the results of the survey. We thought this would, but the data from participants shows that it doesn't for A2, A3, A5, A6, and A8. On the other hand, it does for A4 and A7.

## Chapter 6. Evaluation and Discussion

Chapter 6 provides a thorough analysis of our research findings, covering key aspects: section 6.1 Information and Trends about Research Participants: Insights into participant demographics contextualize our study. Section 6.2 Response Rate: Examining engagement levels helps assess sample representativeness. Section 6.3 Research Question Assessment: Critical evaluation ensures alignment with study objectives. Section 6.4 EAD and CSP Access Directories: Explores the roles and implications of these directories in cloud security. Section 6.5 Qualitative Discussion on Human Factors: Discusses how human behaviours influence cloud security. Section 6.6 summarizes research findings and section 6.7 Summary: Summarizes key findings and implications, guiding further exploration. In essence, Chapter 6 serves as a cornerstone in our research journey, offering a comprehensive evaluation and discussion of findings that not only enrich our understanding of the subject matter but also lay the groundwork for future investigations and advancements in the field of enterprise system security in public cloud environments.

The main goal of this study is to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. This study goal is accomplished by analysing the present status of cloud computing security models. Additionally, section 2.6 investigates the critical direct and indirect human factor elements that impact the security of enterprise data in the public cloud. Human factor is a frequent oversight by organisations when it comes to their enterprise data security in public cloud. Human factors research pertaining to cloud data security is scarce. Luo et al. (2011) said. The human element will inevitably be a component of any security system, regardless of design or implementation. We analysed the subsequent direct human factors: IT skills, human error, experience, data security awareness, apathy, stress, and negligence; and the subsequent indirect human factors: management support, enforcement of security

policies, enterprise security culture, enterprise budget, and enterprise incentives. Our analysis was informed by both a review of the relevant literature and the results of our preliminary investigation which a detailed discussion on the study is found in section 6.5, which revealed that one of the most significant obstacles encountered by small and medium-sized enterprises (SMEs) in Nigeria is a lack of knowledge. We classify the knowledge gap as a direct human factor element encompassing lack of employee experience, lack of data security awareness and lack of IT skills.

Consequently, our initial research assumption regarding A1 is as follows: "Participants who have prior experience utilising a cloud-based ERP system are more inclined to furnish accurate responses to our research survey." The study proposes an End-user Data Access Management Implementation Framework for enterprise ERP software based in the public cloud, which will be backed up by a critical review of employee actions that could jeopardise data security. The explanation of research questions is presented first in this chapter, based on the perspectives of study participants. Following that, a framework is demonstrated based on the findings of the study.

The information of a company must always be protected, and an ERP system's data is no exception. That is why it is critical to understand the ERP's security as well as the system's limitations especially when cloud is used. On the surface, it appears to be required to provide the highest level of security and assurance that business information is well protected and safeguarded. Even more so, given the level of detail in the data, the scope of the system's control, the delicate nature of the processes it manages, and particularly the modules or applications that deal with money. The number of constraints that can be combined in a system and the configurations that can be created is enormous. When deciding whether or not to implement this system, the level of security, control, and restriction of users, as well as the correct validation of business rules, are all important factors to consider.

We recommend conducting an ERP security assessment if you are unsure about the security of your ERP implementation. It's free, easy, and quick. Companies benefit

from having a high-quality, safe, and stable product, while software providers benefit from having a high-quality, safe, and stable product. The study's questionnaire was made up of fifteen questions, the first of which focused on the experience of study participants who worked with cloud-based ERP systems. For the impact of experience on employee knowledge, a variety of reviews are available. Sveiby, (1997) emphasised that knowledge is unaffected by experience. On the other hand, to support the notion that job experience can influence knowledge and performance, we can point out that Davenport and Prusak, (1998) reported that experience could have an impact on employees' knowledge of their jobs. A similar line of inquiry led to the confirmation of the findings by McDaniel, et al., (1988). According to the findings of the most recent study conducted by Ahmed, et al., (2012), feeling insecure about one's job can result in poor work performance and the failure to apply appropriate knowledge. Although almost every participant in this study had at least one month of experience in the information technology field, only 11% of those who took part in the study had eight years or more experience.

The demographic questions that followed attempted to determine the type of IT experience that the study participants had, and, more specifically, whether or not they had come across a cloud-based ERP system while working on their job assignments. The results of this question revealed that 47.73% of participants were currently utilising a cloud-based system in their organisation, with the remaining participants not utilising any cloud-based system at the time of the survey. According to this information, it is alarming that the adaptation of such systems is a matter of trust for businesses. Based on the research question of the study, this chapter is divided into the following parts:

- Information and trends about research participants
- Response Rate
- Research question assessment
- The EAD and CSP AD Directories
- Comparison of the features of the CSP AD the EAD
- Initial study discussion

## **6.1 Information and Trends about Research Participants**

The majority of the study's participants were IT professionals, with many of them having worked with a cloud-based ERP system. The demographics of our research participants' responses were determined using the survey questions SQ1 and SQ2. When compared to the initial sample sizes of the various targeted research groups, the number of research participants who took part in our research exercise is considered small, but the 43 professionals who participated in the research gave a valuable response to the survey question. All the people who took part in our study had at least a few months of experience working in the IT field as seen in the figure 6.1 below. The summary of the responses to SQ1 and SQ2 can be found in the section 5.1 of chapter 5. Because the results to SQ1 show that all of our respondents work in IT roles for various companies, we didn't feel the need to include "No Experience" as an option in our response to this question. We can safely proceed because all of our participants have at least one month of experience in an enterprise IT role, even if the majority of that experience is less than five years.

Furthermore, the responses to SQ2 revealed that a significant number of our research participants are currently using a cloud-based ERP system in their businesses, while a significant number are yet to do so. As a result, it's not surprising that slightly more than half of our respondents have yet to implement a cloud-based ERP system in their company. This could be due to a number of factors already discussed in the literature, but the two most notable are the security concerns businesses have with cloud-based ERPs or the fact that cloud-based ERPs are still a new IT solution, and it will take time for more businesses to adopt them. It's important to note that, while our research participants may not be using a cloud-based ERP solution, as IT professionals, they are familiar with the fundamentals of cloud computing security and thus feel comfortable participating in the study.

Finally, it's important to note that we didn't take into account demographics such as age, sexual orientation, gender orientation, location, industry, or level of education because these factors had no bearing on the quality of the responses we received. The

level of IT work experience and some experience working with a cloud-based ERP system were the most important factors in this study. Because our data were collected over the internet and our research participants could be anywhere in the world, the location was not taken into account. Although the aforementioned demographics influenced people's opinions, they had no bearing on our study because we were more interested in the impact that works experience would have on any type of person, regardless of industry, location, gender, or sexual orientation.

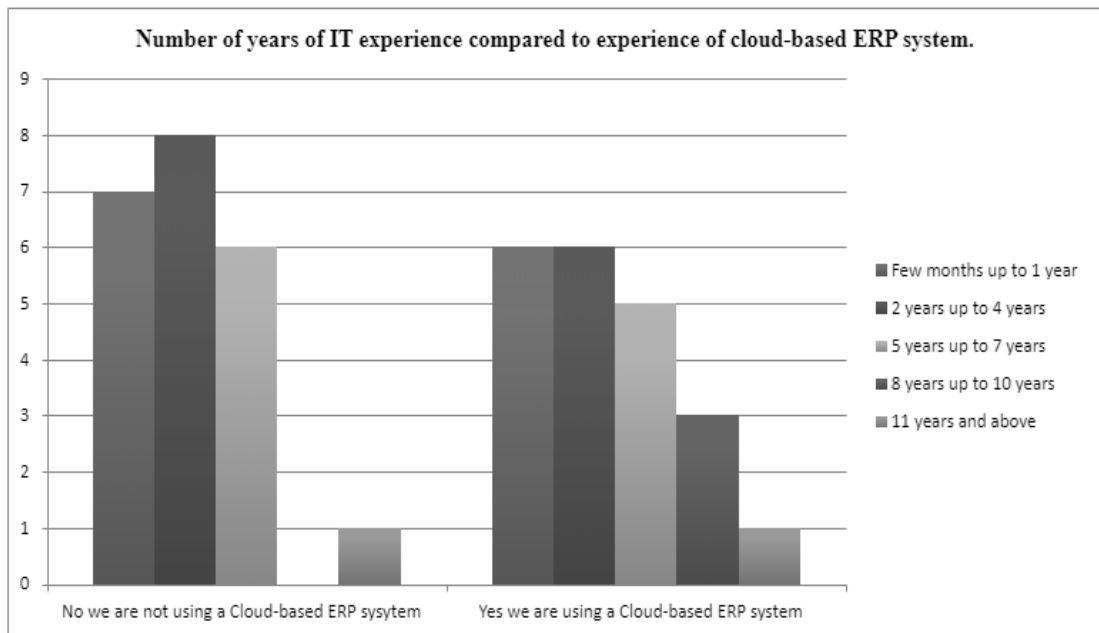


Figure 6.1: Summary of SQ1 and SQ2 that shows the IT and Cloud based ERP experience of our research participants (Eya, 2023)

## 6.2 Response Rate

When compared to the initial sample sizes of the various targeted research groups, the number of research participants who took part in our research exercise was considered to be below expectations. We had hoped to collect a minimum of 100 responses at the outset of the survey, but this was not realistic given the time constraints of the survey, even after providing an additional time window. It is possible to ensure a high quality of participants by ensuring that only those from closely related professional groups are contacted. At the time of data collection, we were well aware that the quality of the opinions we gathered was more important than the number of opinions we gathered. We developed a desire to conduct our research with the help of the best professionals



in the field because we believed that the opinion of a seasoned professional would be more reliable.

A total of two methods were used to recruit potential participants: the first was direct email contact with identified and well-known IT professionals; the second was recruiting participants on LinkedIn, considering their job profiles; and the third was using professional LinkedIn groups to distribute survey invitations. This worked well, though not at the speed we had hoped, and we were able to gradually recruit high-quality research participants to take part in our study over time. Direct emailing to participants, WhatsApp messages directly to participants, and distribution of the questionnaire through LinkedIn cloud computing research groups such as Virtualization & Cloud Computing Solutions with 25,024 members; Cloud Computing, Cyber-security, SaaS & Virtualization with 555,875 members; Enterprise Mobility: Mobile Cloud Computing & Enterprise Applications with 3918 members; Cloud Computing, Virtualization and Disaster Recovery in Nigeria with 3918 members; Cloud Computing, Virtualization and Disaster Recovery in Nigeria with 3918 members; Cloud Computing, Virtualization and Disaster Recovery.

There are 80 direct emails to participants as well as six shares on the various cloud computing LinkedIn groups in the initial sample size. Approximately 23 responses were received during the first two weeks of the campaign. This was disappointing given the sample size we started with. To remind research participants of their participation, we sent out reminders to them via email and re-shared the survey links on the six LinkedIn groups that we were using for our research. The research period will be extended to increase the number of participants, as previously decided. By the end of the eight weeks, we had already received 43 replies. We were confident that it was safe to move on to the next stage of the investigation at this point. The 43 professional-quality opinions on the proposed framework's points of view provided a safe landing for moving forward with data analysis. The decision to send direct emails to participants and to share on LinkedIn groups may have resulted in a 50 percent increase in the number of no responses received. Several factors can be responsible for

this, including outright ignoring the emails or simply not checking one's email or LinkedIn profile during the research period. However, because the world was amid a global pandemic at the time of research, meeting the research participants or participating enterprise in person would have resulted in a more favourable outcome, however, this was not possible at the time of research.

### **6.3 Research Question Assessment**

*“An evaluation of the attributes of the End-user Data Access Management Implementation Framework for Enterprise ERP software based in the Public Cloud.”*

The findings presented in section 5.1 of chapter 5 of the survey data analysis demonstrated that the majority of the survey questions that are directly related to the characteristics of our proposed framework have been supported by the participants of our research.. The research participants' consensus indicated that the End-user Data Access Management Implementation Framework for Enterprise ERP software based in the Public Cloud will promote increased end-user security responsibility, which the participants believed was critical for the cloud-based enterprise data's security. Additionally, the responses indicated that database fragmentation would enhance enterprise dataset security in the public cloud and that data classification should be incorporated into enterprise cloud-based ERP system implementations.

Additionally, both the enterprise access directory and the CSP access directory were supported by the research participants' responses. It demonstrated that when these two attributes are implemented, they will increase end-user involvement in the security of their enterprise datasets in the public cloud and will also increase the end-user enterprise's security awareness. Although the relationship between the EAD and the CSP AD requires additional research to ascertain their similarities and differences, their benefits to enterprise data security in the cloud were established during this research exercise. SQ13 was also used to access end-user access queries, which demonstrated that our research participants believed that prompting the system administrator following an unsuccessful login attempt would promote enterprise

dataset security in the cloud. As a result of the secondary and primary data analysis, the proposed framework's attributes appear to improve enterprise dataset security in the public cloud while also encouraging increased end-user participation in the security responsibility of their cloud dataset.

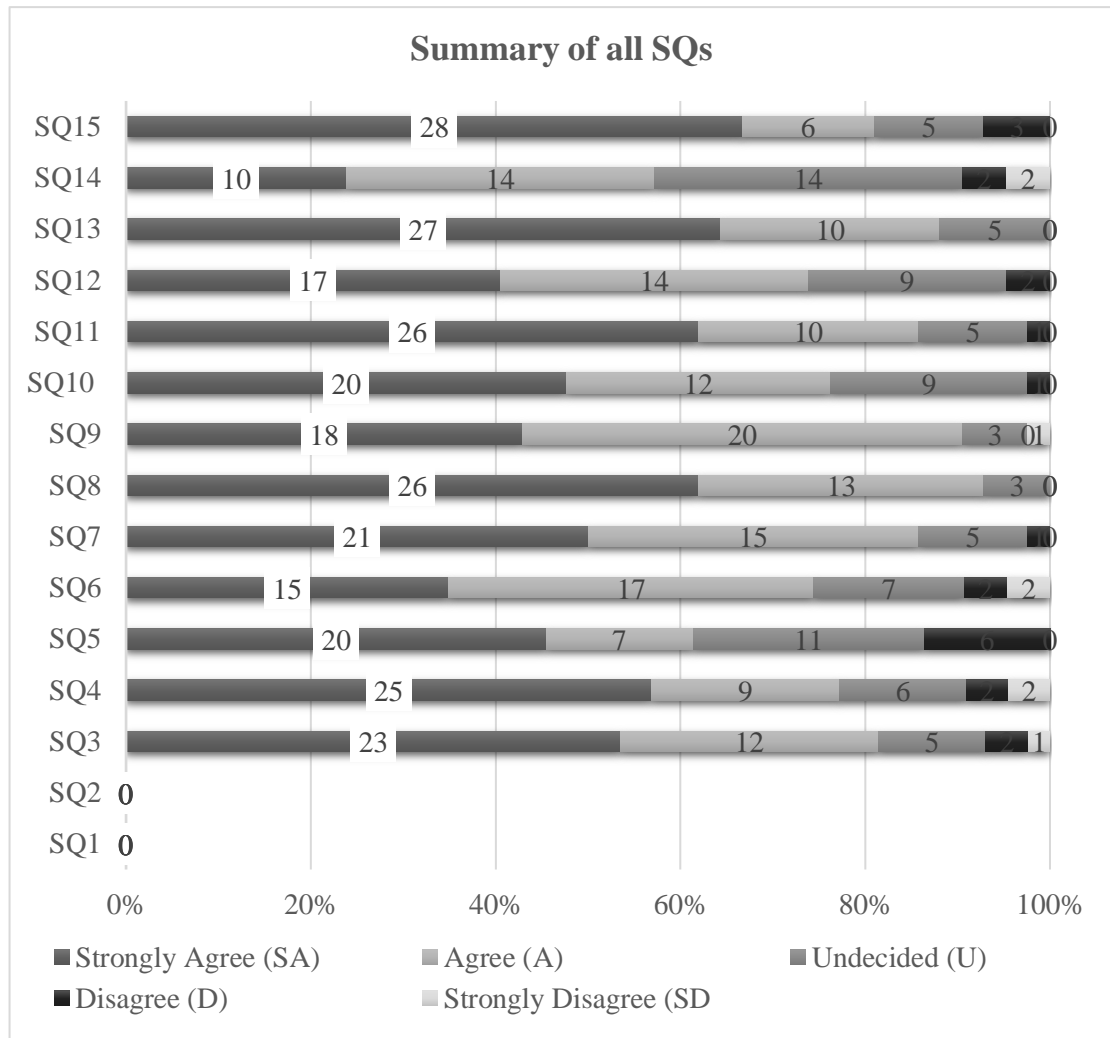


Figure 6.2: Summary of the responses to all the SQs showing the number of responses in each response category

The summary of all responses from the survey to the fifteen SQs used in the questionnaire is shown in figure 6.2. The response options for SQ1 and SQ2, which are demographic questions, were not included in the chart because they did not fit into the other SQs. SQ4, SQ8, SQ11, SQ13, and SQ15 are all highly positive, according to the chart, and many of the research participants agreed with those SQs' viewpoints. The SQ3, SQ5, SQ7, SQ9, SQ10, and SQ12 are moderately positive, while the SQ14,

which asks if the current security policy in the participants' enterprise meets the security requirements in the cloud, and the SQ6, which asks how important the participants' job description and responsibility are in determining the level or type of system access given to you in their enterprise systems, are neutral. As a result, the majority of respondents agree with the proposed framework's viewpoints. The following sections of this study will detail how the SQs responded to our research questions and the responses we received.

### **6.3.1. To what extent is End-user Access Control important in ensuring enterprise data security in the Cloud?**

End-users are employees of a company who have implemented or are about to implement a cloud-based ERP system. The end-user is a person who uses ERP systems in their company to carry out their daily tasks. End-users are expected to have some understanding of the system they are using to work, which can be gained through training and experience, and to be able to adhere to enterprise security policies to ensure data security in the cloud. Although the above is ideal, human factors leave room for errors, oversight, or intentional actions on the part of the end-user, which can compromise enterprise data security in the cloud. However, it is thought that controlling the level of access a specific end-user has to the enterprise data in the cloud will prevent known cases of malicious insiders because no single end-user will have access to the entire enterprise data in the cloud at the same time, as one of the attributes proposed in our framework.

Two of the features of our proposed framework, Enterprise Access Directory and CSP Access Directory, address this attribute. Directory of Enterprise Access: This is one of the framework's distinguishing characteristics. This is the directory that is created after the enterprise's initial data classification. The Enterprise Access Directory (EAD) is a list of key roles and responsibilities for various roles within the enterprise, as well as the level of data access for each role. This is the enterprise's roles and responsibilities database, which should be the first port of call when an end-user wants to access data in the cloud. The key benefit of the EAD is that no single role will have simultaneous

access to the entire enterprise dataset. This feature of the framework will mitigate the impact of a malicious insider incident on the organisation. Although a feature of the framework, the CSP Access Directory is not unique, as this feature was previously proposed by authors such as (Kumari and Nath 2018) in their paper "Data Security Model in Cloud Computing Environment." This is simply a directory of cloud usernames and passwords maintained by the CSP for the purpose of validating each time an end-user accesses cloud data.

As a result, assumption A5 of our research states that: When implemented, the proposed CSP Access Directory will improve Access Control Management in the Cloud, and assumption A4 states that: Proper Access Management within the Cloud Service End-user enterprise will positively improve their enterprise data security in the Cloud. Both research assumptions A4 and A5 are concerned with the research question "How important is end-user access control in ensuring enterprise data security in the Cloud?" The survey questions SQ5, SQ6, SQ7, SQ9, and SQ10 all addressed this research question in order to answer it. The summary of the SQs that addressed the research question "RQ1" is represented graphically below. The responses from our research participants showed that End-user Access Control is very important in ensuring enterprise data security in the Cloud, as shown in figure 6.3 below. The majority of the research participants strongly agreed or agreed with the SQs.

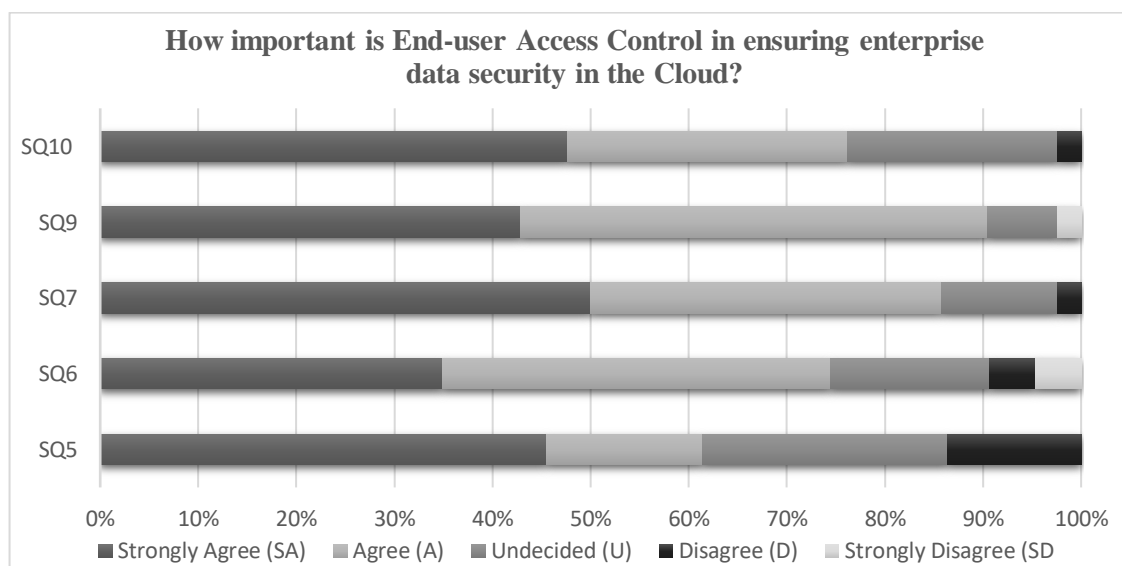


Figure 6.3: Summary of the SQs that addressed research question "RQ1"

Using the mean of the SQs, we were able to determine how critical End-user Access Control is in ensuring enterprise data security in the Cloud. The bar chart above shows that in all of the SQs, more than 60% of the participants strongly agree or agree with the SQs, implying that the results are very positive. Although over 60% of our research participants agreed or strongly agreed with the SQs, the data from SQ5 shows a higher level of disagreement and undecided.

### **6.3.2. How important is shared security responsibility between CSP and enterprise end-user in ensuring enterprise dataset security in a cloud-based ERP system?**

Shared responsibility is a strategy for ensuring that businesses understand their responsibilities for the security of their data in various cloud delivery environments (Lane, et al., 2017). The term "security responsibility" was coined to describe the different CSM security sharing responsibilities. It simply states who in the different CSMs has more security responsibility between the end-user and the CSP. In some CSM, the end-user is more responsible for security, such as in a cloud delivery model like IaaS. (Infrastructure as a service). However, in the case of SaaS (software as a service), the CSP is responsible for more security.

Depending on the cloud delivery model that a particular CSM is targeting, the security responsibility of that CSM is also determined (Chou, 2010). In addition, he attempted to classify the end-users and CSP's responsibilities sharing structure, which can be seen in his diagram Figure 4.2: data responsibilities are not the end-user's responsibility in a SaaS cloud deployment model, but the end-user shares or holds the responsibility of data in all other deployment models. Servers, storage, and networking are all important computing features of cloud security; therefore, if the CSP is in charge of these features, it's safe to assume they're also in charge of cloud security. This is only true in On-Premises or Private Cloud environments, where the end-user is responsible for the entire cloud system. The sharing of security responsibilities between the CSP and the end-user is expected to encourage more end-user involvement in cloud data security and raise data security awareness among end-user

enterprises. As a result, our research hypothesis A3 states that when the Cloud Service Provider and Cloud Service End-users share security responsibility for the cloud system, the enterprise data in the cloud will be more secure. The shared security responsibility model recognizes that achieving robust security in a cloud-based ERP system requires collaboration between the CSP and the enterprise end-users. Both parties must actively contribute to various aspects of security, leveraging their respective expertise and resources. This shared approach is essential to addressing the dynamic and evolving nature of cybersecurity threats and ensuring the overall integrity, confidentiality, and availability of enterprise datasets in the public cloud. The research question "How important is shared security responsibility between CSP and enterprise end-user in ensuring enterprise dataset security in a cloud-based ERP system?" is the focus of research assumption A3. And the SQ4 and SQ8 will be used to access this research assumption A3. The summary of the SQs that addressed the research question "RQ2" is represented graphically below. The responses from our research participants show that shared security responsibility between the CSP and the enterprise end-user is important in ensuring enterprise dataset security in a cloud-based ERP system, as shown in figure 6.4 below. The majority of the research participants strongly agreed or agreed with the SQs.

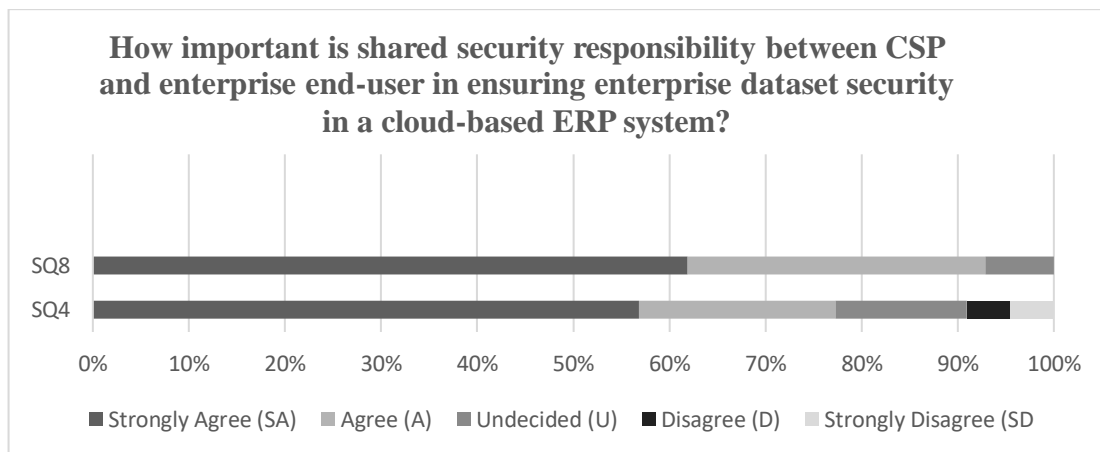


Figure 6.4: Summary of the SQs that addressed research question "RQ2"

Taking the mean value of the SQs that helped to answer how important it is for CSP and enterprise end-users to share security responsibility in ensuring enterprise dataset security in a cloud-based ERP system, the bar chart in figure 6.4 above shows that in all of the SQs, more than 75% of the participants either strongly agree or agree with

the SQs, implying that it is highly positive. Although over 75% of our research participants agreed or strongly agreed with the SQs, the data from SQ4 shows a higher level of disagree and undecided.

### **6.3.3. Should Enterprise dataset classification form part of a Cloud-based ERP implementation to promote enterprise data security in the cloud?**

Dataset classification is a prescriptive method of describing a dataset in which the data is clustered or presented in such a way that it is easy to access when needed. Different approaches to data classification are used, the most important of which is the sensitivity of the data, which determines the subgroup where the data can be clustered. For example, an enterprise can classify data as public or private, confidential, or non-confidential, high risk or non-high-risk, controlled or non-controlled, restricted, or non-restricted, and so on (Hababeh, et al., 2018). Because some enterprises handle more sensitive datasets than others, the level of data classification requirement will vary depending on the nature of the business. For example, a hospital will have a lot of sensitive personal information when compared to a fast-food restaurant. For this study, enterprise data set classification refers to the process of categorising enterprise data sets according to their end-users' key roles and responsibilities, which will determine the level of access each end-user will have and the data they can access in the cloud. We believe that enterprise data set classification should be an integral part of the enterprise's preparations to move data to the cloud. As a result, we have our research hypothesis A6, which states that performing enterprise data set classification as part of the process of moving enterprise data sets to the cloud will aid in the creation of the Enterprise Access Directory and improve enterprise data security in the cloud because only classified data will be moved. This research hypothesis A6 focuses on our research question: "Should Enterprise dataset classification be included in a Cloud-based ERP implementation to promote enterprise data security in the cloud?"

We used the SQ11 to gain access to the perspectives of our research participants on this research assumption A6. The visual representation of the SQ11 summary that addressed the research question "RQ3" is shown below. As shown in Figure 6.5, the



majority of our research participants strongly agreed or agreed that enterprise dataset classification should be included in a Cloud-based ERP implementation to promote enterprise data security in the cloud; this is seen as the majority of the research participants strongly agreed or agreed with the SQ11.

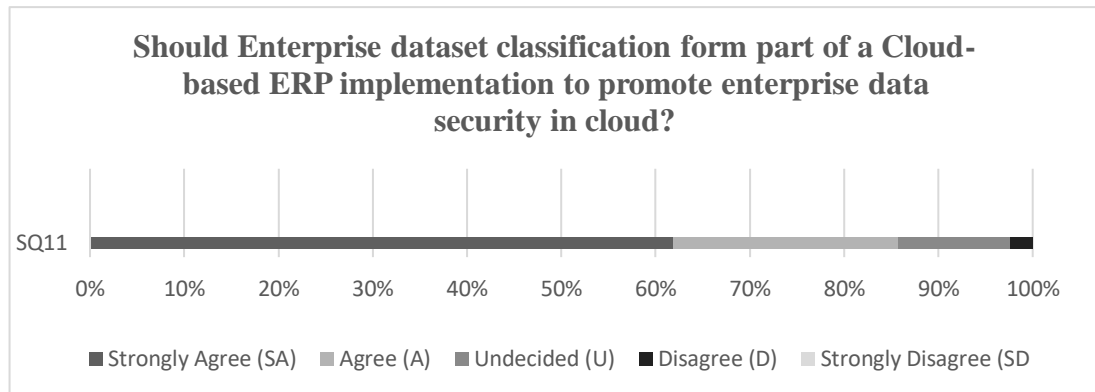


Figure 6.5: Summary of the SQ11 that addressed research question “RQ3”

According to figure 6.5 above, 61.90% strongly agreed that enterprise data set classification should be included in a Cloud-based ERP implementation to promote enterprise data security in the cloud, 23.81% agreed with the SQ11, and 11.90% were undecided. They thought it might or might not make a difference. About 2.38% of respondents believe that enterprise data set classification has no bearing on cloud data security. For the study participants, considering something as an integral part of cloud-based ERP implementation in an enterprise can have multiple meanings. However, more than half of the study participants agreed that this classification system is critical for the security of enterprise data in the cloud and, as a result, for the enterprise's positive progress.

#### 6.3.4. Can Enterprise Database Fragmentation in the Cloud improve enterprise data security of a Cloud-based ERP software system?

Enterprise Database Fragmentation: This feature of our framework proposes that after an enterprise has undergone data classification as part of the procedures for moving data to a private, public, or hybrid cloud, the CSP should provide enterprise database fragmentation for each set of enterprise data being moved to the cloud. Enterprise database fragmentation is a strategic approach employed to optimize the performance

and reliability of large-scale database systems in enterprise environments, enabling organizations to effectively manage and leverage their data assets for business operations and decision-making processes. A fragmented enterprise database in the cloud means that enterprise authorised end-users only have access to the information they need to perform their job at the company.

We used the research assumption A8, which states that Enterprise Database Fragmentation in the Cloud would improve Enterprise data security of a Cloud-based ERP system, to find the information. The research question "Can Enterprise Database Fragmentation in the Cloud improve enterprise data security of a Cloud-based ERP software system?" is addressed in assumption A8. We used the SQ12 to gain access to the perspectives of our research participants on this research assumption A8. The visual representation of the summary of the SQ12 that addressed the research question "RQ4" is shown below in figure 6.6. According to the results of our research, Enterprise Database Fragmentation in the Cloud can improve enterprise data security of a Cloud-based ERP software system, as evidenced by the fact that the majority of the research participants strongly agreed or agreed with the SQ12. Our research findings indicate that implementing Enterprise Database Fragmentation in the Cloud has a positive impact on enhancing the data security of Cloud-based ERP software systems. This conclusion is supported by the overwhelming agreement among the majority of our research participants with Statement Question 12 (SQ12).

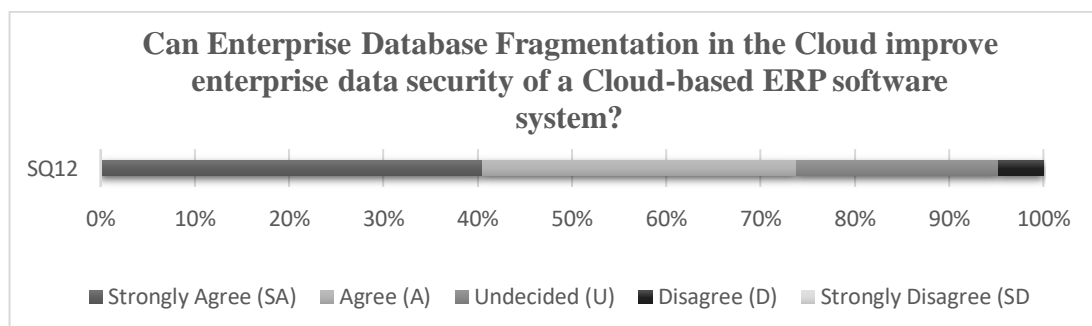


Figure 6.6: Summary of the SQ12 that addressed research question "RQ4"

The importance of fragmentation was emphasised by the majority of study participants for the SQ12. 40.48% thought Cloud service providers should store enterprise data in fragments and implement access control for each fragment of the database, 33.33%

agreed with the SQ12, but 21.43% were undecided, and 4.76% disagreed with the statement. As a result, dealing with issues or problems related to database fragmentation in an enterprise is critical. The fragmentation problem refers to the partitioning of information in order to distribute each part to the various network sites. The question of what a reasonable unit of distribution is arises immediately. Fragmentation in the public cloud is important for strategic decision-making, risk mitigation, and optimization of resources. It enables organizations to design resilient and flexible cloud architectures that align with their specific needs, regulatory requirements, and business objectives. By carefully considering fragmentation in their cloud strategies, organizations can enhance their overall cloud experience and achieve a balance between performance, cost, and security.

### **6.3.5. Can cloud computing have an impact on enterprise system data security?**

Determining if cloud computing had an impact on enterprise system data security was our last research question. This was an important research question for us considering the circumstances that gave rise to the research exercises, where we experienced enterprises implementing an ERP declining to use a cloud-based ERP system as they believe it will impact their enterprise data security. The enterprise declined regardless of the cost-effective benefits a cloud-based ERP system stands to offer them. To access this, we had a research assumption A2 which states: Ideally any upgrade in technology should have an impact on the previous technology, although this impact can either be positive or negative. Therefore, Cloud computing would have an impact on Enterprise system data security in Cloud. To be able to access the views of our research participants with regards to this research assumption A2, we used the SQ3. Below figure 31 is the visual representation of the summary of the SQ3 that addressed the research question “RQ5”. From the below, we can see that the responses from our research participants showed that cloud computing has an impact on enterprise system data security, this is seen as the majority of the research participants strongly agreed or agreed with the SQ3. Our final research question was to see if cloud computing had an impact on enterprise system data security. Given the circumstances that led to the research exercises, this was an important research question for us. We saw enterprises

implementing ERP systems decline to use a cloud-based ERP system because they believe it will compromise their enterprise data security. Regardless of the cost-effective benefits, a cloud-based ERP system could provide, the company declined. To do so, we used research assumption A2, which states: Ideally, any upgrade in technology should have an impact on the previous technology, which can be positive or negative. As a result, Cloud computing will have an impact on the data security of Enterprise systems in the Cloud. We used the SQ3 to gain access to the perspectives of our research participants on this research assumption A2. The visual representation of the summary of the SQ3 that addressed the research question "RQ5" is shown below in figure 6.7. The responses from our research participants showed that cloud computing has an impact on enterprise system data security, as evidenced by the fact that the majority of the research participants strongly agreed or agreed with the SQ3.

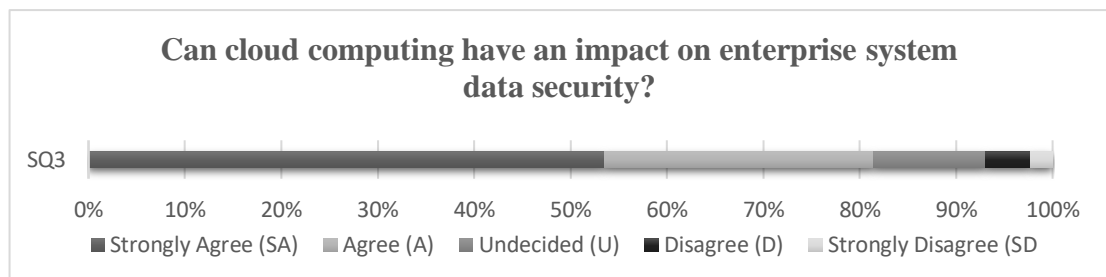


Figure 6.7: Summary of the SQ12 that addressed research question "RQ5" (Eya, 2023)

According to figure 6.7, 53.49% strongly agree that cloud computing has an impact, 27.49% agree that cloud computing has an impact, and 11.6% are undecided about whether cloud computing has an impact. About 6.98% of respondents believe cloud computing has little or no impact on enterprise data security in the cloud. "Impact" refers to the effect or influence that something has on a person, a system, an organization, or the environment. It often describes the tangible or intangible outcomes, consequences, or changes resulting from a particular action, event, decision, or phenomenon. The term "impact" can encompass a wide range of effects, including positive or beneficial outcomes, negative consequences, or even neutral changes. The meaning of "impact" to each participant can be an influencing factor in why they choose a particular answer in this case. Although it is not safe to assume that our participants who stated that cloud computing has no impact on enterprise data security

are looking at the word "impact" in a negative light. Other researchers, such as Mather, et al. 2009, Al Noor, et al. 2010, and Gupta, et al. 2013, agreed with this study's conclusion that cloud computing has an impact on data security.

#### **6.4 The EAD and CSP AD Directories**

Finally, we presented an End-user Data Access Management Implementation Framework for Enterprise ERP software based in the Public Cloud. The proposed framework is divided into two phases, the first of which is handled by the end-user enterprise and the second by the CSP enterprise. The first security responsibility phase occurs when the enterprise classifies its data set based on its security importance and prepares its Enterprise Cloud Directory, known as Enterprise Access Directory EAD, by applying its distinct enterprise roles and responsibilities to the already classified dataset. The end-user enterprise is in charge of the EAD and its security in this first phase. When a classified end-user uses the correct username and password to gain access to a portion of the enterprise database in the cloud, the second phase begins. The CSP Access Directory (CSP AD), Enterprise Database Fragmentation, and End-user Access Queries are the three features of the second phase. The three features are managed by the Cloud Service Provider (CSP), and the CSP is solely responsible for ensuring their security. When compared to other existing models, the proposed framework will encourage more end-user participation in enterprise data security in the cloud. Because no single user can access the entire enterprise database in the cloud at the same time, the framework mitigates the impact of a malicious insider on the enterprise cloud data set in the cloud.

##### **6.4.1 Comparison of the features of the CSP AD the EAD**

In the contents of our research findings, we noted that the features of the CSP AD and the EAD may be similar but different. They are similar as both directories are used to manage the access to enterprise datasets in the cloud. With this in mind, the table 6.1 below shows some of the differences that can be noted, and future research can find out how these differences will impact an enterprise data security in the cloud.

Table 6.1: Difference between the CSP AD and EAD (Eya, 2023)

CSP Access Directory	Enterprise Access Directory
The security responsibility lies with the CSP	The security responsibility lies with the end-user enterprise
The CSP have absolute control of the resources contained in the CSP AD.	The end-user enterprise has absolute control of the resources contained in the EAD.
This directory is required to be prepared and developed in fragments, therefore fragmentation of the contents of the directory is a must-have.	For this directory, fragmentation of the contents of the directory is not a must-have, although it is preferred that data classification is done before the preparation and development of the EAD.
For the CSP to prepare this CSP AD, they will rely on the already classified data received from the end-user enterprise, there a classified dataset is an already refined form of data.	For the end-user enterprise to prepare the EAD, they rely on raw data generated from their enterprise and because this data is still in its raw form, data classification is required before the EAD can be prepared.
In the CSP AD, it is expected that the directory can be a lot more generic so it can be able to accommodate a wider range of different enterprises who are their service users. We would expect to see a more generic terminology in the CSP AD than you will see in the EAD, for instance, the departments can be Finance, Inventory, Human Resource, Admin etc.	The EAD will be more detailed and more specific to the end-user enterprise. It is expected to have more specific terminologies relating to the end-user enterprise. For instance, a farmhouse enterprise can have departments like Egg Collection department, Feed Dispensing Department, Hashing Department etc
There is no requirement for the CSP AD to be created at the starting phase of the implementation, it can be introduced at any phase the CSP deems it okay to implement.	The EAD will always be required to be created during the starting phase of a cloud-based ERP implementation. This is because the contents of the directory will be required for the implementation to process to the other phases.

## **6.5 Discussion on the Study of the Role of Human Factors on Enterprise System Security in Public Cloud.**

Thematic analysis which looks for patterns in data and reports them was used in the qualitative data analysis of our interview data. It included putting together and making sense of our textual data in a planned way to find meaningful themes that show experiences, points of view, or things that are being studied. The initial steps we took were getting to know the data by reading our interview transcript thoroughly, doing the first round of coding, looking for themes, going over the themes, describing and naming the themes, generating the word cloud using NVivo and writing a report based on the understandings from the data. The important things we considered when doing this thematic analysis was its reliability, validity, flexibility and the critical thinking involved. We considered thematic analysis as adaptable since it can be used with different types of study designs and data, such as textual and visual data. During the study process, it was important to be aware of our own points of view and any possible biases we had as this may impact the outcome of the interpretation. To improve reliability and validity of the thematic analysis done, the researcher got some feedback from some other researchers using similar technique.

A word cloud is a visual representation of textual data in which the proportions of the words vary to signify their frequency or significance (Cui et al., 2010). Word clouds are utilised in qualitative research to present a concise summary of the most significant words or terms present in a given dataset. By preprocessing textual data, eliminating frequent words, and calculating the frequency of each remaining word, they are generated (Cui et al., 2010). Word clouds are produced by utilising software applications or online platforms, wherein the font size of more significant words is increased. The analysis of the word cloud yields valuable insights regarding the primary themes, topics, or concepts that are evident within the dataset. Word clouds facilitate the identification of themes and the visualisation of crucial terms; they can also be utilised as a means of communication in research reports or presentations (Gambette and Véronis, 2010). Nonetheless, word clouds cannot replace comprehensive qualitative analysis.

Table 6.2: Initial Study Coding Themes (Eya, 2023)

<b>Initial Study Theme Clusters</b>
Cloud-based ERP system impact on enterprise data security
Data Management Security Policies
DMS policies and senior management end-user involvement in DMS policies
DMS policies and enterprise incentive policies
End-user skills and end-user roles
Employees' actions and security risks
Number of staff in your enterprise
Organization data security culture
Training programs and organization EIS regulations
EIS awareness programs and its effectiveness
End-user knowledge of cloud-based ERP systems





Figure 6.8: Word cloud for Cloud-based ERP system impact on enterprise data security

As mentioned, the table 6.2 above, there are some code themes we used in analysing the responses from our initial study. Some themes emerge from figure 6.8. The first obvious remark is that ‘impact, data, cloud and security’ are the most often terms mentioned as all the quotes extracted refer to it. Furthermore, more, terms like ‘trust’, ‘loss’, ‘believe’ and ‘control’ suggests that CSP is conceived as a third party who is not in control of enterprise data and that it will require some level of trust and the risk of data loss. The term ‘cloud’ appears to be mentioned very often, this suggests that the participants referred to cloud computing when answering the interview question. In responses to the interview questions regarding the impact of a cloud-based ERP system on enterprise data security. Participant (Main Transcript Participant 02) MTP02 mentions “*Am not aware of any impact, maybe the ICT department may be more informed about the impact we might be facing right now as a company if any.*” And when asked if he will find it difficult moving their enterprises’ data to the cloud due to this impact, he stated “*It wasn’t my decision, and I don’t know much about that.*” And to the question of if he feels that adopting a cloud-based ERP system, your enterprise will lose the security control of your enterprise’s data. He responded “*Is possible since you are outsourcing the data to another party. But if you are confident*

*in the other party, why not. **It is not an automatic loss if you trust the other party like your own employees.***”

Furthermore, the next participant (Main Transcript Participant 03) MTP03 in his words “**Well no huge difference, the only difference now is that we need constant electricity and internet to function with. With respect to data security, we can say we are more relaxed as security is now dependent on our cloud providers. And like I said before there has not been a security incident that led to data loss, so we trust they are on top of their game. I do not believe there is any huge impact on the enterprise data security in the cloud**”. Although he identified that they found it a bit challenging classifying the data and choosing the ones to move to the cloud as not all their data set was key to their business. He agreed that sometimes they nursed the fear of losing their enterprise data in the cloud but over time they are beginning to build confidence. “**Sometimes we nursed that fear. But gradually we are beginning to have confidence in the system.**”

The participant (Main Transcript Participant 04) MTP04 had the following to say: “*Let’s say it was more affordable than the regular ones we used in the past, **it also helped us to establish different values of different data, at least now it is very clear to us that some data are more valuable than others, so we try to preserve those kinds of data within our control***”,

*“**Preparing the data to move to the cloud was a very big task, it involved a lot of data cleaning and visiting archives to retrieve data. It was daunting but once we moved, it became a lot easier to input data into the system and work with it.**”*

*“We already adopted it and so far, **our data are safe, although now we know a third party has access to our operating data, we choose to trust them, there may not be any data breach. That said, we still did not move all our critical data to the cloud, not that we don’t trust the third-party providers, but we feel the need to safeguard these critical data ourselves.**”* Regarding the impacts of cloud computing impact on enterprise data security. He believed a cloud-based ERP system was more affordable but acknowledged the data classification challenges at the implementation stage. He also

mentioned the concept of trusting the third but regardless of taking charge of the enterprise's most sensitive data within the enterprise.

For our next participant (Main Transcript Participant 05) MTP05, his opinion was similar but there are some key differences. He had the following to say: *“Data security is always a concern but we the users must do our own part to ensure good data security. In this company, we do our best to ensure data security, especially by awareness in the forms of training. So far, we are yet to experience a major setback because of poor data security.”*

*“The cloud one has a different interface, and now you are aware there are third parties involved in the data processing and storage. The cloud one is also faster.”*

*“No, it is only the required time but not difficult. Although in my opinion data sensitivity should always be considered.”*

*“Yea we may lose total control of the data, but we are not losing the data or even the data integrity.”* In his opinion, he believed cloud-based solutions are faster than traditional IT solutions but also acknowledges the time it will take to implement such solutions when taking into consideration data sensitivity and classification. He also was quick to admit that although there were security challenges.

The next participant (Main Transcript Participant 06) MTP06 was quick to admit he had little knowledge of cloud computing, and he was not able to confirm if they had any data in the cloud but believed that with every new thing comes an impact of some sort. MTP06: I believe I have heard about it but am not an expert in the field. He had the following to say: *“I am not able to describe it that is if we have any data in the cloud.”*

*“Everything new thing has an impact, am not aware what the impact is but I do believe there is an impact.”*

*“I don't believe it will be such a difficult thing for the company management to decide but am sure is a good thing since it is a new technology”.*

*“Just like I know **everything has an impact**, I believe the more skilled staff have, the better they can perform their job. **I believe IT skills have become an essential skill** to have in this 21st century at the least how to use the computer on daily basis to work.”*

*“**I don’t really understand the cloud thing very much**, so I will not really say”.*

Subsequently, the next participant (Main Transcript Participant 07) MTP07 on answering questions relating to the impact of cloud computing on enterprise data security in the cloud, he mentioned the need to trusting the third party but also being very security conscious. He acknowledges that there may be some impact, but the major difference was that now the data is stored in the cloud and a third party is now involved. For this he had the following to say:

*“There is nothing really to describe, is still the same dataset we have got. The only difference is that now in the cloud a **third party is involved**, and we have got to **trust** them to play their part in securing the company data, so is the same data set? “*

*“Cloud computing has exposed us to the **third party**, so we must be **more security conscious**.”*

*“**It is difficult to trust a third party with sensitive data**. But at the end of the day, you must adopt it if you **need to**.”*

When asked if he felt that adopting a cloud-based ERP system, their enterprise would lose the security control of their enterprise data. He had the following to say: *“No, I don’t think so. With proper planning during the adoption process and after, **no huge security challenges should be faced**. And when if they do happen, is best to document the incidents and how it was resolved to prevent future occurrence.”*

Following this, the participant (Main Transcript Participant 08) MTP08 had a similar view, that any new thing will have some form of impact but also acknowledged he is not very knowledgeable about cloud computing. When asked questions in regard to this, he said *“**I don’t know**” “I don’t think so. **I mean is a new technology but just like with every new thing, there will be good sides and there will be bad sides**.”*. To the same questions, participant (Main Transcript Participant 09) MTP09 mentioned

that IT professionals will have more knowledge of the impact of cloud computing than himself: *“Am not aware of any impact, maybe the ICT department may be more informed about the impact we might be facing right now as a company if any.”* We asked how their enterprise mitigate the risk associated with the use of cloud-based ERP systems? he says: *“Well the last I checked, you were **required to change to a new password quite frequently**, like say every three to four months intervals”*, When asked if he felt that adopting a cloud-based ERP system, your enterprise would lose the security control of his enterprise data. He says *“**Is possible since you are outsourcing the data to another party**. But if you are confident in the other party, why not. It is not an automatic loss if you trust the other party like your own employees.”*

Conclusively, our study participants in this study believed that for any new technology like cloud computing, there is definitely some impact on the enterprise systems data security and even on the enterprise data in the cloud. But most are of the opinion that trusting the third party was okay but also being security conscious of the associated risk of storing the enterprise data with a third party was advised. A few participants suggested that although data classification can be time-consuming but is necessary to determine the sensitive enterprise data and how to move them to the cloud. Some participants also suggested that to mitigate some risks associated with cloud computing, enterprises should prioritize hiring knowledgeable personnel in the ICT department and encourage data security breach incident documentation.

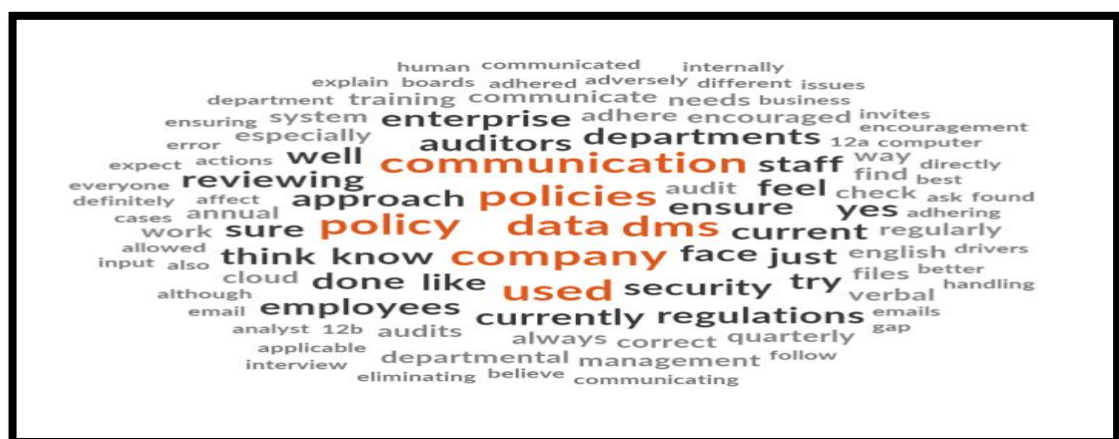


Figure 6.9: Word cloud for Data Management Security Policy (Eya, 2023)

Some themes emerge from figure 6.9. The first obvious remark is that ‘communication, policies, company, used’ and ‘data’ are the most frequent terms mentioned as all the quotes extracted refer to it. Furthermore, more, terms like ‘auditors’, ‘ensure’, ‘reviewing’ and ‘regulations’, suggests that many enterprises used auditors to review and ensure compliance to data management security regulation. In response to the interview questions regarding the Data Management Security Policies, we had two sub-coding as follows: DMS policies and senior management end-user involvement to DMS policies, DMS policies, and enterprise incentive policies.

Our research participants when asked what the current DMS approach is currently used in your enterprise. Participant MTP02 had the following to say, “*We have quarterly departmental **audits** and annual company **audits**. The auditors check that all data files are correct*”, MTP03 said, “*We have this policy of **reviewing data regularly** and ensuring that only **trained staff** is allowed to key in data from the different department.*”, MTP04 said, “*That is data management security approach, eliminating manual handling of data, and **reviewing of data both internally and by auditors.***”, MTP06 said, “I do not really know.”, MTP07 said, “*Data input into the system is only done by **qualified staff** to reduce human error. So many other strategies we used especially always **reviewing the data regularly.***”, MTP07 said, “*I wouldn’t know to expect I ask but am sure they have a way of ensuring our data security, all this data analyst will know better.*”, MTP09 said, “*We have quarterly departmental **audits and annual company audit**. The auditors check that all data files are correct.*”.

From the responses from our research participants, regular data review by both internal and external auditors was identified as a DMS approach currently used. They also identified the importance of ensuring only skilled staff who have the right level of skills is permitted to input data into the enterprise systems, this they believed will reduce human errors and any associated risks of data being handled by the unskilled staff. Some of our participants admitted not knowing the current DMS policies currently being used in their enterprise and one participant believed the data analyst in their enterprise is in a better position to know.

Furthermore, when our participants were asked how they communicate DMS policies to ensure that employees understood; and that the policy does not adversely affect the business. Participant MTP09 said, *“I am not in the position to do that. But most communication within our company is done through **emails**.”* and then went on to suggest, *“Well I believe there still needs to be more done especially in terms of how the policies are communicated and spread. This will ensure a wider understanding of the policy.”*, MTP08 said, *“In plain **English** language that everyone understands using our work **email**.”*, MTP07 said, *“Always on **emails**, but for DMS policies well am not so sure. I will try to find out after this interview”*, MTP05 said, *“Our main mode of communication is via a **written mail** to employees; all communication is in **English** languages. Although recently have started to try other means of communication like the **notice boards, verbal face-face and letters** sends directly to the departments. We found that verbal face-to-face communication works best for our low-skill workers like company drivers, who in most cases do not use the computer to work, so we try to explain the new regulations or policies verbally in a way they will understand. Letter sent to departments is mostly used to schedule meeting invites or communicate the training timetable for the departments.”*, MTP03 said, *“Most IT official communication is communicated through company **email** to all staff.”* From the above responses from our participants, we were made to understand that DMS policies within the enterprise are communicated in the enterprise’s official language, in these instances here, the English Language was identified as the means of communication. The channels of communication were emails for most of the participants although the MTP05 went further to mention that their enterprise does other channels of communication depending on their target audience, here face-to-face channels were used for low-skill workers who sometimes do not have access to emails within the enterprise.

Going forward, our research participants were asked about DMS policies and end-user responses to DMS policies. We were hoping to understand how the participants feel about the DMS policies and to know if they feel encouraged to adhere to those policies

if any. We ask our participants, “*Do you feel that you are encouraged to respond to DMS policies within the enterprise; or do you feel reluctant to implement them?*”, our participants had the following to say, MTP05 “*Sometimes I feel the **management needs to do more** to ensure policies are adhered to. When they don’t show much encouragement, then it is likely the policy will struggle.*”, MTP06 said, “*Just like with all other policies and regulations, not just DMS policies, **we are encouraged to follow them**. This company I find keep to rules and regulations a lot.*”, MTP07 said, “*I think **we are encouraged**. But what am not sure is if staff know the required policy and how to adhere to it. I think knowledge is the gap here not the weather we are ready to adhere to it.*”, MTP08 said, “*Yes, **definitely** just like with other policies because that is what keeps the company working*”, MTP09 said, “*Well I believe there **still needs to be more done** especially in terms of how the policies are communicated and spread. This will ensure a wider understanding of the policy.*” MTP03 said, “*We are **doing our best to encourage** good data management strategy, although sometimes we feel left alone, it will go a long way **if management can support more** than they currently do, both financially and otherwise. There are **encouragements in place**, but it can be improved.*”, MTP04 said, “*Reluctant to implement it No, but **we are encouraged to follow** any policies or guidelines on how to use the system.*”, (Main Transcript Participant 01) MTP01 said, “*We **feel encouraged to implement it***” and the MTP02 said, “*Well I believe there **still needs to be more done** especially in terms of how the policies are communicated and spread. This will ensure a wider understanding of the policy.*”. Summarily, our participants felt they are encouraged to adhere to their enterprise DMS policies just like every other policy within the enterprise, although a few of them felt that more could be done on the part of management to encourage the enterprise employees. Some of the participants went further to mention that the management of their enterprise could do more in the areas of financial budgeting for DMS and communication of the policies.

Furthermore, for the DMS policies and enterprise incentive policies, we asked questions to enquire if enterprises have incentive policies and how effective these incentives are at encouraging adherence to DMS policies. We ask “*Do you have any incentive policy in your organization to reward your engagement in adhering to DMS*



policies of a cloud-based ERP system? “, for this question the participant MTP01 said, “**Yea** sure we do give our employees **some benefits** to encourage them” When asked what kind of benefits, he said, “*Maybe by **cash** or also **promotion** most times or also sometimes some **further training**.*”. MTP02 said, “*None that am aware of.*”, MTP03 said, “*Incentives, **no not at all**, although at times at the discretion of the management, they can choose to **add bonuses** to staff I don’t think it has anything to do with DMS.*”, MTP04 said, “*I don’t think so.*”, MTP05 said, “*I don’t even encourage such, is like **bribing** people to do the right thing, **we don’t have** but **we don’t need one** either to adhere to set out policies in our organization.*”, MTP06 said, “*I don’t think is right to give the incentive to staff for obeying company policy, **we don’t have** such that am aware of.*”, MTP07 said, “*Incentive policy **yea** maybe by **word of mouth** but **not money** incentives*”, MTP08 said, “*Incentive, what type, am **not sure** we do*” and the MTP09 said, “*None that am aware of.*”.

Summarily, our participants believed that incentives are not really needed to encourage staff to adhere to enterprise policies. Some likened it to bribing staff to do the right thing, a few admitted not having any incentives in their enterprises while others also admitted that their enterprises have incentive policies and went on to describe the types of incentives like promotion, bonuses, and further training. A lot of our participants did not admire cash incentives and believed it will not achieve better company culture.

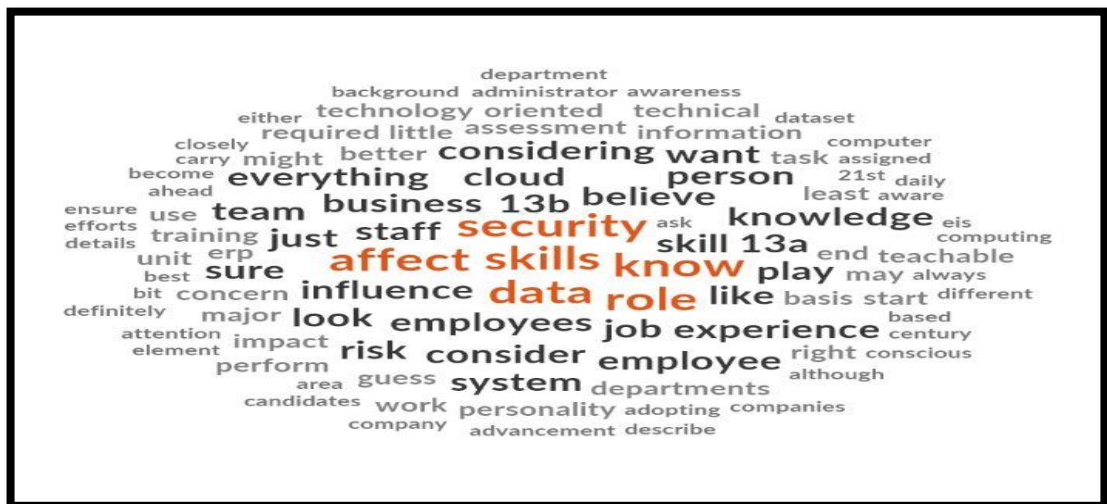


Figure 6.10: Word cloud for End-user skills and end-user roles

Some themes emerge from figure 6.10. The first obvious remark is that ‘skills’ and ‘roles’ are among the most frequent terms mentioned as all the quotes extracted refer to it. Furthermore, more, terms like ‘experience’, ‘knowledge’, ‘influence’ and ‘system’, suggests that experience and knowledge is conceived as a key factor to consider in an employee when considering data security in cloud. In response to the interview questions regarding the end-user skills and end-user roles within the enterprise and some employees’ actions and security risks, which is a subcode in this theme. We asked the participants questions like “*What skills do you look for in an employee when considering data security in the cloud?*” and “*How would you say the IT skills of your employee influence or affect your data security?*”, this is to enable us to understand how the enterprises take into consideration staff skills when assigning their roles and also how some of the actions of employee poses a risk to the enterprise data in the cloud. For this question, what skills do you look for in an employee, when considering data security in the cloud?, participant MTP02 said “*Am not in HR but I guess they might want technical **IT skills***”, MTP03 said, “*I would go for candidates that **have experience** in using ERP system, I know we can give training, but we prefer a little **bit of experience.***”, MTP04 said “***Attention to details, experience, and teachable personality.***”, MTP05 said, “***Meticulous person** with a teachable personality.”, MTP06 said, “*I don’t really know what skills they consider before hiring the **IT staff.***”, MTP07 said “***Data security awareness, the person must be security aware and conscious.***”, MTP08 said, “***An honest person** with integrity is important so at least you will not worry about malicious insider messing up your dataset.”, and MTP09 said *it definitely technical **IT skills**, although the human resources have a better understanding*”. It is interesting to see how most of our participants agreed that having IT skills and experience are requirements they considered when hiring IT staff. Some went further to talk about the persona of the intending staff, where attributes like honesty, teachability, meticulousness, attention to detail, and awareness of data security concepts were preferred.**

Furthermore, for this question how would you say the IT skills of your employees influence or affect your data security? Participant MTP02 said, “*IT skills are everything, when you have the right skills, **security would not be a major concern.***”,

MTP03 said, “ *IT skills do have an impact.* ”, MTP04 said, “ *If they have IT skills and knowledge, it makes them better prepared for the task ahead.* ”, MTP05 said, “ *So far because we always train staff, we ensure they have the required skill for any task they are assigned to do. This is because we know that if the required skill to do their job, we may be risking the quality of our output as a company.* ”, MTP06 said, “ *Just like I know everything to have an impact, I believe the more skilled staff have they better they can perform their job. I believe IT skills have become an essential skill to have in this 21st century at the least how to use the computer on daily basis to work.* ”, MTP07 said, “ *If staff doesn’t have the skill, they are likely to perform poorly at the job. So is best to get people with sound background on the job you did like them to carry out for you.* ”, MTP08 said, “ *Am not sure how it does but I know it definitely does affect it.* ” and MTP09 said, “ *IT skills are everything when you have the right skills, security would not be a major concern.* ”. Summarily, our participants believed that employees’ IT skills will have an impact on their enterprise data security but are not clear on the actual impact. Most of the participants believed the impact will be on the performance of the employee and also the associated risk of having a poor output for the enterprise.

Subsequently, for the employees’ actions and security risks it poses within the enterprise, we asked our participants the following questions, “ *Do you feel that there are actions of employees that pose a risk to data security? And is this applying also to cloud data security in the cloud?* “. For this question, MTP02 answered “ *Yes of course* ”, MTP03 said, “ *Yes of course especially the lack of the basic knowledge of how the system works.* ”, MTP04 said, “ *Yes, when people are ignorant of their actions most especially. That is why in Finance we do weekly data check to be sure the data we continue to work with is the right data.* ”, MTP05 said, “ *Sure, why not.* ”, MTP06 said, “ *Yes, I do feel so.* ”, MTP07 said, “ *Always* human actions matter a lot. Like for instance human error.”, MTP08 said, “ *Definitely, yes.* ”, and MTP09 said, “ *Yes of course* ”. Going from what our participants said, they all agreed that there are actions of employees that pose a risk to data security, some of the participants identified human error, and lack of required knowledge as some of the things that lead to those actions of employees that pose a risk to data security.



Furthermore, more, terms like ‘big’, ‘number’ and ‘enterprise’ suggests that some of the research participants considered their enterprises as big. In response to the interview question regarding the number of staff in your enterprise, we had one subcode which is the organization’s data security culture. For this, we asked our participants questions like “*What is the number of staff currently working in your enterprise?*”, MTP02 said, “*We have **above eighty** employees or colleagues of mine.*”, MTP03 said, “***I don’t know** but we are considered a big enterprise.*”, MTP04 said, “*My depart is about 10 staff, **but am sure** some department is bigger than us, the company is big in terms of how many persons work here, although most persons are the low key staff like drivers and the rest.*”, MTP05 said, “*I honestly **don’t know**.*”, MTP06 said, “*Our company is big, but I **do not know** the number of staff we have, but we have offices in three states in the country.*”, MTP07 said, “***Am not in HR to know** but in my unit, we are about seven of us.*”, MTP08 said, “***I don’t know.***”, and MTP09 said, “***a little bit over eighty** employees I believe”. It is observed from the responses of our participants that a few described their enterprise as “big” but are not sure the actual number of employees, about two of our participants acknowledged that their enterprises would have over eighty personnel, for these two participants their enterprises can be classified as medium size enterprise as described in table 2.1 in chapter 2 of this thesis.*



Figure 6.12: Word cloud for Organization data security culture

Some themes emerge from figure 6.12, the first obvious remark is that ‘training’, ‘security’, ‘data’, ‘skills’, ‘risk’ and ‘organisation’ are the most frequent terms mentioned as all the quotes extracted refer to it. Regarding the organizational data security culture, we asked our research participants, “*how would you describe the culture of your organization in terms of security risk appetite, in terms of data security risk appetite, do you find your organization culture being in line with data security policies and procedures.*”. MTP01 said “*Yes sure, is in line with data security procedures, but we are also more open to innovations with regards to this. We are **doing our best** with data security procedures.*” (Main Transcript Participant 01) MTP01 when asked if he was convinced that their organization allocates a reasonable budget to deal with cloud DM issues. He said, “*Well I won’t say my organization allocates so much money, but we are **doing our best.***”. For other participants we asked them “*How do you or your enterprise mitigate the risk associated with the use of cloud-based ERP systems?*”, MTP05 said, “*Over the years, we have managed to run several **training courses** for our different departmental needs. The training is normally focused, so for instance, we train the Finance guys on the financial module extensively and then an introductory training for them on the other modules they may come across. When you say EIS regulation, I understand that is different as you travel across countries with respect to the Nigerian environment, **we do our best to abide by the set-out rules** by NCC and the likes. But training is never such a demanding task to the regulations. You may find the regulations cover more items like network requirements, data policies, and insurance policies, some of which cannot be covered with the training of employees alone.*”.

MTP06 said, “*All work associated risk is mitigated by keeping to the rules and regulations guiding such activity in the company.*”. MTP07 said, “*We manage risk by **proper planning before handling sensitive data.** We also encourage proper documentation and even incident document.*”, and MTP09 said, “*Well the last I checked, you were **required to change to a new password quite frequently**, like say every three to four months intervals.*”. Summarily, our participants felt their enterprises are doing their best to adhere to data security procedures and also in the allocation of money for data security activities in the enterprise. Some believed that mitigating risk

associated with the use of cloud-based ERP systems will involve proper training of employees and also proper planning before handling sensitive data.

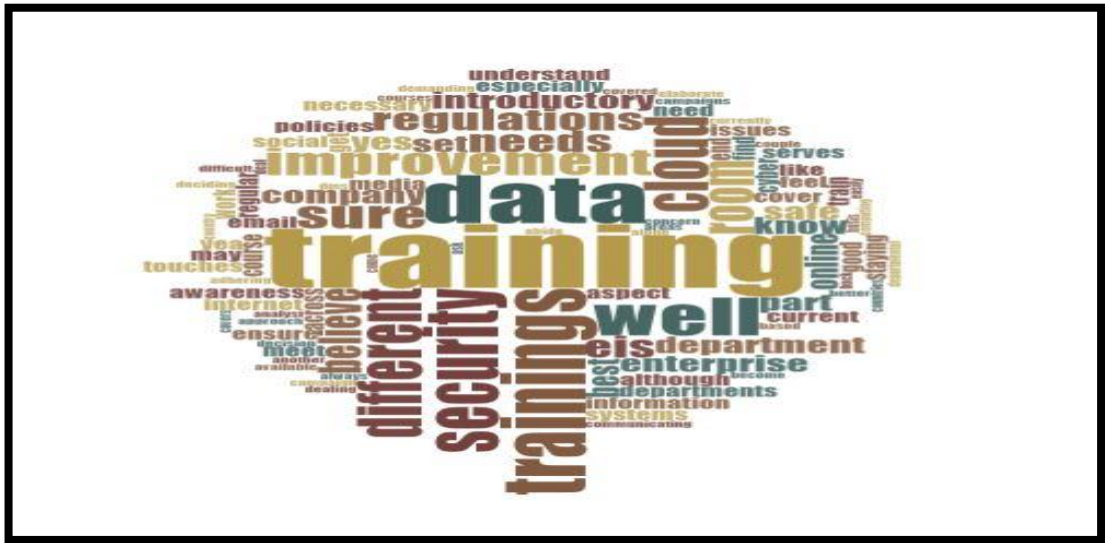


Figure 6.13: Word cloud for Training programs and organization EIS regulations

Some themes emerge from figure 6.13. The first obvious remark is that ‘training’ is the most frequent term mentioned as all the quotes extracted refer to it. Furthermore, in response to the interview question regarding the training programs and organization EIS regulations, we had two subcodes which are EIS awareness programs and their effectiveness and End-user knowledge of cloud-based ERP systems. We asked the participants question like, “The training program in your enterprise, does it cover all the areas of EIS regulations? If yes, can you give an example of how it covers recognized threats in cloud computing?“, MTP09 said, “**Yea we do have a couple of training** in our company, although different groups or departments get different at different times to serve their respective needs. But in general, I feel the training available serves our current need, although there is room for improvement.”, MTP08 said, “I am not so sure, but one thing is sure, **we do have some training**”, MTP07 said, “Well I feel **our regular training program is very good** and I believe we learn a lot of skills from them.”, MTP06 said, “**We have some training** but am not sure how they meet the regulations.”, MTP05 said, “Yes, **we do have awareness campaign** on how to stay safe online and how to identify a spam or scam email in your work email. We felt it was necessary to introduce this because we found that there is a growing number of internet scammers in the country and persons who work in an organization like ours

*can easily become a soft target. So as a proactive measure, we started these campaigns. Since Cloud could as well be the internet on a layman's understanding, I would say **it does meet the company's needs**. We sometimes go even further to train people on how best to use social media and the type of information not to put on social media.”*. Then,

MTP04 said, “**The training we get on a regular basis** serves our need as a department to understand how to deal with another department.”, MTP03 said, “**Well Yea especially the fundamental ones.**”, and MTP02 said, “**Well we have some training, but I cannot say there is no room for improvement. Of course, there is room for improvement. I would say the training on introductory cyber security touches on some aspects of staying safe online, which I do believe is part of cloud systems.**”. Summarily, our participants acknowledge that they have training programs within their enterprises, but most were not clear on if the training meets the EIS regulations although the majority believed the training was satisfactory.

Subsequently, regarding the end-user knowledge of cloud-based ERP systems, we asked our research participants question like, “*How would you describe your knowledge of a cloud-based ERP system?*”, MTP09 said, “**I only know the basics, like that it exists and is an advancement to the traditional computing**”, MTP08 said, “**I don't think am knowledgeable in that area although I have read about it online in the past.**”, MTP07 said, “*I believe is the trending thing now, most companies are adopting it; just like other ERPs, am sure it will be user friendly and secure to use. **I know a little about it. There is nothing really to describe, is still the same dataset we have got. The only difference is that now in the cloud a third party is involved, and we have got to trust them to play their part in securing the company data. So is the same dataset. Cloud computing has exposed us to the third party, so we must be more security conscious. It is difficult to trust a third party with sensitive data. But at the end of the day, you must adopt it if you need to.***”, MTP06 said, “*I believe I have heard about it but am not an expert in the field.*”, MTP05 said, “**I believe am very good at it. Since Cloud could as well be the internet on a layman's understanding**”, MTP04 said, “**I am quite knowledgeable on it especially the Finance module because our work is**



*dependent on it.*”, MTP03 said, *“I have a good knowledge of cloud ERPs. Basically, are the same ERP systems but the difference is that you need 24-hour internet to always have access to it and you have to have a steady electricity supply to maintain it.”*, and MTP02 said, *“I don’t know much about this. I just believe we are safe and that IT security guys are on top of their games.”*. Summarily, most of our participants acknowledge having little knowledge of cloud-based ERP systems, but MTP04 and MTP05 stated that they are very knowledgeable of cloud-based ERP systems.

Conclusively, among the most significant findings of the interviews is that a large number of people lack the necessary knowledge to operate the sophisticated technical system of cloud computing, which is a significant factor. Because of a scarcity of highly qualified cloud specialists, the development of the cloud market has been slowed significantly. As a result, in 2021, and most likely in the next few years, the professionalism and stability of a service provider's information technology team will determine the company's position in the cloud market. Qualifications and experience enable us to carry out complex tasks for businesses that deal with complex projects that must be completed within strict time constraints. They indicated that they play a variety of roles in their organisation, which can be broadly divided into technology, business, and risk assessment categories.

Another factor that will have a direct impact on the market positions of cloud market players is their ability to provide an optimal range of services for businesses. Product strategy built on knowledge of the real needs and requirements of the client enables us to provide the optimal set of tools for implementing that highly balanced hybrid solution most efficiently. Only by taking this approach will you be able to reap the full benefits of cloud computing technologies in your organisation. When a portfolio of services is developed using an approach in which the product vision does not take into account the requirements and specific features of various types of businesses, such services at best go unclaimed, and at worst, the customer does not receive the promised solution to his or her business problems, which has a negative impact on the level of trust in the cloud in general.

Cloud computing, according to popular belief, is simply the outsourcing of computing power and data storage. Companies, however, are increasingly turning to the cloud as a more complex technology solution as a result of the increased demand for digital products. In this particular instance, the implementation has the effect of transforming internal operational processes from within the organisation. It is important not to overlook incident management activities such as monitoring and forecasting, reporting, and response to incidents. Continuous monitoring is required to determine whether a cloud computing service is operating normally across the entire network infrastructure (for example, monitoring the performance of the virtualized platform and virtualized machine in real-time). This enables the system to collect information about the security status of the service, identify abnormal conditions, and provide early warning of security overloads, operational disruptions, service outages, and other such occurrences, among other things. Following the occurrence of security incident events, problem identification and rapid incident response are provided either automatically or with the assistance of a human administrator, depending on the configuration.

Participants in the interview stated that, in general, a great deal of work remains to be done to fully utilise technology in the context of data security systems. Information, processes, and systems, as well as information and information systems, are all at risk of being damaged by cloud computing security threats, which can cause significant financial and operational consequences for organisations. They can be of elemental origin, and they can be accidental or intentional; they can occur within or outside the organisation; and they can be classified as either casual or intentional, as well as either active or passive. The specific threats that are detected are highly dependent on the cloud service that has been selected. Data loss and leakage, unprotected service access, and internal threats are all potential security threats for CSPs. Internal threats to CSP security include unauthorised administrative access.

Considering the specialised nature of the creation of new, complex computer systems, we believe that this estimate is valid in some cases. Off-the-shelf software as a service

is widely available, which has the potential to significantly reduce the time it takes to deploy systems in organisations. The deployed system will be in operation for up to four years before reaching the break-even point, according to the participants. Putting together a list of estimates for the length of time it will take to complete various stages of the migration process to the cloud computing model. It is acceptable to consider a component to be well-configured if it is simple to use, requires little setup time, and scales readily (i.e., the component interacts well with a large number of identical components). Well-tuned components make it simple to assemble seamless processes and services that automatically scale in response to changing workloads as dictated by business requirements.

Modern specialised computer systems are complex, and configuring one is not an easy task. Using a very simplified framework, consider the hardware component, which executes operating system code, on top of which a whole set of interconnected services provided by platform and middleware software is executed, and on top of which an application is launched that provides a specific service to the consumer. When different components are executed on different computers, this raises questions about intersystem and inter-program interaction, among other things. The state of a computer's software stack is described by thousands of parameters, each of which is unique to that computer. Finding the most optimal, or at the very least functional, the combination of these parameters - a process known as software tuning - is more akin to an artistic endeavour than a technological endeavour. Making even minor changes to the configuration of a system can frequently result in the system becoming completely inoperable as if the software components were a house of cards that had collapsed. The system is not operational. To get back to a usable state of the system, we must either repeat the steps we took to get there or restore the system to its previous state. In contrast to physical computer technologies, there are specialised, highly effective technologies available for virtual machine technologies that allow you to save and, if necessary, restore various states of the entire system at a minimal cost. This makes it acceptable and justified to "make a scrap" when changes are made to the programme workpiece, and in the event of an obvious failure, discard the configuration and quickly return to the original workpiece, and in the event of a successful outcome,

save a new, good snapshot of the system state, as described above. In the process of building a software stack, we save a series of snapshots of the state of the system. By doing so, we are cementing each layer of the house, and in the event of an unsuccessful move to a higher level, we can quickly get out of storage a finished structure that contains all the previous floors and continue construction from the point of acceptance of the erroneous decision.

The preceding analogy illustrates the distinction between the incremental approach of saving states and the monolithic approach, in which one unsuccessful movement on the upper floors results in a pile of cards on the table. It should be noted that occasionally, the issue of replacing the system's low-level components - such as replacing the card at the lower levels of an already constructed house - arises. When the completed system's operating period arrives, our preliminary calculations for the system's load level are likely to be incorrect, which is easily corrected by the system's scalability property. At the conclusion of the project, the system's software components are incorporated into a library of pre-built solutions, while the hardware component is released and prepared for deployment on new projects.

Cloud computing, as a novel economic, organisational, and technological phenomenon, can be classified according to a variety of criteria due to its complexity and richness of internal interdependencies. We primarily used the technological criterion in this work. The selection of this criterion enabled the use of pre-existing classification developments for information technologies in general, and in the form of services in particular. It was discovered that the technological division of software into system, application and middle-level software is quite applicable to cloud computing, with some caveats. It was sufficient for our analysis to develop this fundamental classification, which enabled us to trace the evolution of technology and the emergence of new economic forms on its basis.

The organisational and economic benefits of the Cloud Computing model of consuming information processing services are demonstrated in comparison to more

traditional models and processes for utilising information technologies in enterprises and organisations. Cloud computing is a very fruitful idea for converting computers into pure computing utilities. Utility elasticity is critical for businesses that provide information processing services to end-users and deliver their services to consumers via the Internet, as the volume of services provided may grow (or contract) significantly faster than it did just a few years ago. Whereas it used to take years for a consumer base to reach several million users, it now takes months, if not days. For already-operational businesses that leverage information technology to solve their problems, the elasticity property is also extremely attractive, as it enables the avoidance of equipment shortages or downtime due to improper planning of equipment utilisation levels.

## **6.6 Summary of Research Findings with Emphasis on Research Questions**

Summarizing research findings with a focus on research questions is a crucial step in the research process. It ensures clarity and focus, aligns the reported findings with the posed inquiries, and contributes to existing knowledge. It also allows for an evaluation of the research design, enhances reader engagement, and guides future research. The summary effectively communicates the significance of the study, highlighting its contributions to key inquiries. It also aids decision-makers in applying the study's outcomes to practical scenarios, providing actionable insights directly linked to the initial research questions. Overall, summarizing research findings with a focus on research questions provides a structured, coherent, and focused representation of the study's outcomes, guiding future research endeavours.

The study's questionnaire was divided into fifteen items, with the first question focusing on study participants' experience with cloud-based ERP systems. For the impact of experience on employee knowledge, a variety of types of reviews are available. Sveiby, (1997) pointed out that experience has no bearing on knowledge. On the other hand, Davenport, (1998) reported that job experience can influence employee knowledge and performance, which supports the notion that job experience can influence knowledge and performance. In a similar vein, McDaniel, (1988)

confirmed the findings. According to Ali and his colleagues' most recent study, job insecurity can lead to poor work performance and the implementation of adequate knowledge.

Only 11% of study participants had 8 years or more of experience in the IT field, even though almost every participant had at least a month. 47.73% of participants use a cloud-based system in their business, while the remaining participants do not use any such system. According to this data, it is alarming that the adaptation of such systems is a matter of trust for businesses. The table 6.3 below shows the summary of our research assumptions, the SQ addressing each of the assumptions and the number of responses gotten from our research participants for each option in the SQs and finally the summary of whether the assumption is supported or not. The research assumptions can be found in section 3.1.2.

Based on the research question of the study, this section 6.6 is divided into the following parts:

- Impact of cloud computing on the enterprise data security system.
- End-user security responsibility in ensuring enterprise data security in Cloud.
- Fragmentation of databases.
- Concerns concerning the implementation of ERP.

### **Impact of cloud computing on the enterprise data security system**

One of the study's primary research questions is to determine the importance of cloud computing in an enterprise's data security system. The study's third question examines the impact of cloud computing on an enterprise's data security system. 53.49% of respondents indicated that cloud computing affects an enterprise's data security system. Only 2.3% of respondents indicated that cloud computing has had no impact on their enterprise's data security system. In this regard, we propose that the shared responsibility principle for enterprise data security in cloud computing is a critical perspective to consider, as it is one of the key principles of our proposed framework.

Table 6.3: Summary of the Research Assumption Validation Results.

Research Assumptions	Research Question	Survey Questions	Strongly Agree (SA)	Agree (A)	Undecided (U)	Disagree (D)	Strongly Disagree (SD)	Supported
A1		SQ1	2	3	11	14	13	Direct effect (No-significant negative) Total effect (No)
A1		SQ2	23	0	0	0	21	Direct effect (No-significant negative) Total effect (No)
A2	RQ5	SQ3	23	12	5	2	1	Yes
A3	RQ2	SQ4	25	9	6	2	2	Yes
A4	RQ1	SQ5	20	7	11	6	0	Yes
A4	RQ1	SQ6	15	17	7	2	2	Yes
A4	RQ1	SQ7	21	15	5	1	0	Yes
A3	RQ2	SQ8	26	13	3	0	0	Yes
A4	RQ1	SQ9	18	20	3	0	1	Yes
A4, A5	RQ1	SQ10	20	12	9	1	0	Yes
A6	RQ3	SQ11	26	10	5	1	0	Yes
A8	RQ4	SQ12	17	14	9	2	0	Yes
A1, A7		SQ13	27	10	5	0	0	Yes
A1		SQ14	10	14	14	2	2	Direct effect (No-significant negative) Total effect (No)
A1		SQ15	28	6	5	3	0	Direct effect (No-significant negative) Total effect (No)

Sharma (2017) also emphasised the importance of cloud computing in support of this notion. This research focuses exclusively on the issue of external control. As organisations migrate more critical components of their business ICTs to the cloud, they must understand the best technology and security procedures that both the cloud provider and the organisation can implement to effectively mitigate risks and ensure an appropriate level of data security. The Bright Internet Initiative establishes an excellent framework for establishing responsibility for Internet traffic origination and distribution. However, we believe that by incorporating shared responsibility, the Bright Internet framework can be enhanced. Other researchers concur with this study's conclusion that cloud computing affects an enterprise's data security system, for example, Gupta, (2013); Mather, (2009); Saidu, (2010).

#### **6.6.1 End-user security responsibility in ensuring enterprise data security in the cloud.**

The fourth question specifies that security responsibility for a Cloud system within an enterprise is critical; the Cloud Service Provider (CSP) and Cloud Service End-users are the two systems chosen for division of responsibility in this question. The enterprise employees who use the enterprise system to work are known as cloud service end-users. More than half of the participants in the study said it's critical to divide security responsibilities between CSPs and CS End-Users. Morozan (2014) investigated the multi-cloud database model and emphasised the value of CSP. AlZain (2012) stated that the security it provides is insufficient to protect a single cloud. To ensure confidentiality, it uses the process of requesting "multiple sharing" of various cloud services between different servers. And there's the extreme cloud climate. Chou, (2015) attempted to divide the role-sharing model between the end-user and the CSP, demonstrating that the data function in the SaaS cloud delivery product model is not the end-user role.

Software-as-a-Service (SaaS), Software-as-a-Subscription (SaaS), or ERP Software as a Service (SaaS) refers to a software delivery model in which a software application is



made available as a service over the Internet. As a result, there is no need for the service user to install or update the application on their computers. This model enables the use of new software without requiring a significant upfront investment in licences or equipment. The investment is solely based on the use of SaaS services, which have a low short-term cost. The applications can be used in a very short period after the service agreement or SLA has been established with the provider. As a result, SaaS is primarily focused on lowering the cost of implementing and using computer systems associated with managing an organization's business resources (such as ERP and CRM). Because of the economy of scale and high specialisation of the companies that provide these services, the cost is reduced because the initial investment is very low, and the fees for subsequent use of SaaS services are also very low.

We believe that using cloud services by a company is a shared responsibility for storing potentially sensitive data in a system that the company cannot control. While most cloud service providers promise to take "reasonable" precautions to protect data security and privacy, the burden of evaluating a cloud service provider's security practice falls largely on the client enterprise. The Internet Initiative will be able to achieve its primary goals of preventing malicious attacks of unknown origin while maintaining freedom of expression and privacy protection thanks to a shared responsibility that includes clear expectations from both the "end-user" side and the Cloud Service Provider.

By adhering to relevant legal jurisdictions and privacy laws, you can maintain your privacy in the cloud. Question 7 of the study deals with when a single system end-user is accessible to the Enterprise data set in the Cloud. This could make the Enterprise more vulnerable to a successful cyber-attack. According to the results, 50% agreed with the statement, and 35.71% likely agreed. This simply means that ensuring that no single system end-user has access to the entire enterprise dataset in the cloud at the same time is part of the end-user enterprise security responsibility. This strengthens our proposed framework attribute, which encourages businesses to use their enterprise

roles and responsibilities to determine the level of access each role should have to enterprise data in the cloud.

For the 10th question of the study in which the majority of study participants agreed that managing access control would improve access control management in the cloud, The importance in the design of distributed databases refers, in general, to make decisions about the location of data and programs across the different sites of a computer network. As we can see, this problem is related to the design of the same computer network; however, in this course, only the database design will be what we consider. The decision of where to place the applications has to do with both the Database Management System (DBMS) software and the applications to be run on the database.

#### **6.6.2 Fragmentation of databases.**

Question 12 of the questionnaire can be used to gather information for the "RQ4" research question, which deals with database fragmentation. The majority of study participants emphasised enterprise database fragmentation and better accessibility in response to question 12 of the survey. However, 21.43% of those polled were undecided, and 4.76% of those polled disagreed with the given statement. As a result, it was assumed that enterprise database fragmentation in the Cloud would improve the security of a Cloud-based ERP system's enterprise data. As a result, dealing with issues or problems related to database fragmentation in an enterprise is critical. The fragmentation problem refers to the partitioning of information to distribute each part to the various network sites. The question of what a reasonable unit of distribution is arising immediately.

A full relationship can be considered appropriate since user views are subsets of relationships; however, the full use of relationships does not support efficiency issues, especially those related to query processing. One of the possible dissuasive elements for the effective implementation of "cloud computing" is the absence of an adequate

sense of certainty about the confidentiality and security guarantees that this service offers. Distrust is more accentuated, if possible, in the case of the various public administrations. Indeed, the latter consider the opportunity to entrust third parties with the storage but note that they also handle certain information. When we host our documents, files, and databases on a third-party site, we trust that it has adopted all the required security measures to guarantee the integrity of our information. Although this is the case in a high percentage of cases, it is not always this way.

### **6.6.3 Concerns concerning the implementation of ERP.**

The study's fifth research question examines the data security implications of an enterprise's ERP adaptation. To ascertain the answer to the research question, participants were asked to complete Question 15 of the questionnaire. Concerns about ERP software adaptation in one's enterprise were raised in the fifteenth question. 66.66% of study participants agreed with the statement. This indicated that if ERP software is implemented, data security may become a concern. Apart from data security, the ERP software has several other issues, risks, and disadvantages. Despite the numerous benefits, there are several drawbacks, without which a description of modern ERP systems would be incomplete. It's worth noting that ERP systems are constantly evolving and refining their capabilities.

Among the inconveniences associated with the implementation of ERP systems are the following:

1. Employees may attempt to sabotage changes. This resistance has the potential to be quite strong.
2. Expensive and time-consuming implementation. The substantial initial investment has a delayed effect
3. The system has a high total cost of ownership. Support costs, specialist maintenance, and system development must all be constantly updated and refined.
4. Project risks associated with the organization's information maturity and automation level, debugging business processes, the software products used,

the degree of resistance and qualifications of personnel, and management involvement, among others.

5. The requirement for product refinement, can significantly increase the implementation cost. Unfortunately, despite efforts, there is no such thing as a universal, flexible system that can meet the needs of any organisation. Generally, it is necessary to adapt the system to the specific requirements of an organisation.

## **6.7 Summary of Chapter 6**

The primary objective of this research is to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. This study goal is accomplished by analysing the present status of cloud computing security models. It also examines the essential human factor elements that influence the adoption of a cloud-based ERP systems in such organisations. The study proposes an End-user Data Access Management Implementation Framework for enterprise ERP software based in the public cloud, which will be backed up by a critical review of employee actions that could jeopardise data security. Cloud Computing's most visible and widespread application is email over the Internet or Webmail. The user delegated email storage to the "cloud," which enables him to send and receive data over the network via a set of functionalities.

The study's primary conclusion is that cloud computing has a sizable impact on the data security system. Additionally, while the majority of study participants favour implementing cloud computing in their businesses, they expressed some reservations about cloud ERP software. Fragmentation elicited a range of responses from study participants. In a nutshell, the Cloud computing model is the outsourcing of technology services to specialised companies, which enables the company that chooses to outsource to concentrate on the core of its business, on what it does best, rather than on the two scarce resources available in the modern world: talent and money.

Along with the benefits, this thesis seeks to mitigate risks and build confidence in the implementation of an ERP system and its return on investment. It is necessary to conduct a thorough analysis of how the system's implementation will contribute to the resolution of your company's problems and evaluate the system's effectiveness. One of the most effective ways to accomplish this is to conduct a thorough pre-project survey.

## Chapter 7. Conclusion and Recommendations

This chapter presents project's conclusion. It begins by summarising all of the tangible research findings in section 7.1 and the research contribution in section 7.2. The project appraisal follows, in which the project's strengths, challenges, limitations, and weaknesses, as well as the methodology chosen, are critically examined in sections 7.3 and section 7.4. Finally, we discussed the implications of our research findings and made recommendations for future research in section 7.5. This chapter is called conclusion and recommendation as it bring together all the summary of the thesis and proffer some recommendations.

### **7.1 Summary of Main Research Contribution**

This thesis reviews several Cloud Computing Security Models with a close look at the model that addresses data security challenges in cloud-based Enterprise Resource Planning (ERP) systems. The study's key findings are that impact of cloud computing is significant on the data security system. The project aims were achieved, and several strengths and weaknesses of this project were presented. The attributes of the proposed framework were favoured by the research participants. A new study can investigate and evaluate more how the CSPA.D and E.A.D could be similar or different.

#### **7.1.1 Theoretical Implications**

Theoretical implications of this research transcend its practical implementations. This work enhances the theoretical comprehension of various aspects related to cloud computing security, including policy and governance considerations, the impact of human factors on cloud security models, communication protocols that prioritise adopting end-users' needs, dynamic and adaptive security strategies, and the foundational principles governing data fragmentation as a security mechanism in cloud computing.

### **7.1.1.1 Recommendation for Shared Security Responsibility**

This study enhances understanding regarding the manner in which Cloud Service Providers (CSPs) and end-users (e.g., adopting enterprises employees) divide security responsibilities. The need for adopting enterprise end-user to share a greater security responsibility in the SaaS delivery model of cloud computing have been identified by previous authors such as: Saa, Moscoso-Zea et. al., (2017); Ahmed and Kommos, (2012); Weli. 2021; Feuerlicht and Govardhan, (2010); Orosz, Selmecei et.al., (2019) and Al-Okaily, Alkhwalidi, et. al., (2022). The dynamics of security responsibility are delineated, with an emphasis on the respective duties and obligations of all involved parties. This research also recognises the unique attributes of various cloud service delivery models, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), which influence the allocation of security obligations. According to the research findings, it might be necessary to modify security guidelines and best practices in accordance with the selected service delivery model. For instance, security considerations for SaaS models may differ substantially from those of IaaS models.

Enhancing comprehension of the shared security responsibility across various models facilitates the implementation of more precise risk assessment and management strategies. The research may offer valuable insights into the effective assessment and management of security hazards by organisations, contingent upon the model they select. Additionally, user awareness and education are vital, as end-users must recognise their shared obligation for security maintenance, particularly in areas where the CSP is also responsible. The research may provide suggestions for the development of efficacious awareness and training initiatives for adopting enterprise end-users. The knowledge acquired from the study may make a valuable contribution to the formulation of security protocols that are congruent with the complexities inherent in various cloud service delivery frameworks. Acquiring this knowledge enables organisations to effectively navigate the intricate realm of cloud security, establishing a solid groundwork for judicious decision-making, risk mitigation, and the creation of customised security protocols.

### **7.1.1.2 Recommendation for the Significance of Human Factor Elements when Developing Information Security Systems and Cloud Security Models**

This research emphasises the significance of human factors when developing information security systems and cloud security models, with a specific focus on small and medium-sized enterprises (SMEs) in Nigeria. Sarkar (2010) believes that the role of human factors in cloud data security has been underestimated and concluded by encouraging more research that will focus on how best to mitigate human factors to reduce their impact on data security systems. The importance of the impact of individual direct and indirect actions, behaviours, and decisions within SMEs on the efficacy of these cloud security models is duly recognised by authors like Mortazavi-Alavi (2016). Recognising this is of the utmost importance in the development of robust and all-encompassing security protocols for cloud computing.

This research enhances the collective comprehension of information security by recognising the integration of human elements, including direct and indirect human elements such as: employee IT skills, human mistake, data security awareness, experience, apathy, stress, negligence, management support, security policy enforcement, enterprise security culture, enterprise budget and enterprise incentives as seen in the review in section 2.6. Comprehending these processes is critical in order to adequately mitigate vulnerabilities that arise from human activities. This research may yield valuable insights regarding the development of cloud security models tailored particularly for small and medium-sized enterprises (SMEs) in Nigeria, which frequently encounter distinctive challenges such as resource scarcity and limited knowledge as noted from the results of the first study in section 6.5. This research was conducted on SMEs at Nigeria enterprises; this presents an opportunity for other researchers to further test these theoretical findings on other countries, and cultures. Perhaps other large enterprises might be used and could yield a similar insight or different.



Additionally, this research contributes to the identification and recommendation of methods for mitigating human-induced security risks as reviewed in section 2.6 of this thesis. These encompass suggestions for effective training initiatives, security interfaces that are intuitive for users, and organisational policies that foster a climate of security awareness. This research goes beyond theoretical considerations and provides SMEs with practical implications. The results of this study can be utilised by policymakers to develop focused endeavours that enhance information security protocols, raise awareness regarding security matters, and diminish susceptibilities associated with human interactions. In brief, the research strengthens the current understanding of information security by highlighting the significance of human factors in the development of cloud security systems and models, with a particular focus on small and medium-sized enterprises (SMEs). Recognising this is essential in order to formulate security protocols that accurately reflect the challenges and complexities encountered by lesser enterprises.

#### **7.1.1.3 Parametric Analysis of the Various Cloud Security Models**

An investigation that centres on the parameters associated with security models for cloud computing has yielded novel insights regarding the manner in which these attributes are employed to differentiate between different security models as seen in the review in section 4.1. The subject matter of this research is parameter evaluations, which involve a methodical examination of specific components comprising security models for cloud computing. Technology used, security responsibility, security effectiveness, security porosity, targeted cloud feature and security practicality are examples of these parameters. Certain parameters have been identified by scholars such as Zarger and Chaturvedi (2015), Sharma and Kaur (2014), and Chou (2010) in their comparisons of different cloud computing security models. However, our study focuses specifically on the following new parameters: security practicality, targeted cloud feature, and security porosity. As the research progresses, additional insights emerge that enhance the overall understanding of the significance and purpose of parameters in the context of cloud security. The parametric analysis study's methodology involves the construction of a framework named "*End-user Data Access*

*Management Implementation Framework for Enterprise ERP Software based in the Public Cloud*” for assessing and contrasting the attributes of different cloud security models, such as their strength and weaknesses as seen in section 4.2.

The parameters may encompass several critical factors, such as shared security responsibility, enterprise access directory (EAD), enterprise database fragmentation (EDF) in the cloud, and end-user access queries (EAQ) to manage who has access to enterprise data in the cloud, compliance with industry regulations, and adaptability to emergent risks. The study's findings have significant theoretical implications for both SME organisations in Nigeria and individuals engaged in the field of cloud computing security. These observations will provide guidance to decision-makers as they choose and execute cloud security solutions that correspond to their specific needs. Through the provision of novel insights and perspectives on the application of these parameters, this study significantly contributes to the overall advancement of knowledge in the field of cloud computing security models. Consequently, this contributes to the collective comprehension of how to effectively assess and enhance security protocols within the context of cloud computing.

### **7.1.2 Practical Implications**

This research contributes significantly to the understanding and practical implementation of cloud security models, particularly in the context of cloud-based ERP systems. It addresses data security concerns, involves end-users, and provides practical insights like effective communication for organizations aiming to enhance data security in the cloud.

#### **7.1.2.1 Recommendations for Addressing Data Security Concerns**

This research acknowledges that there is widespread concern among organisations regarding the security of data stored in the cloud, particularly concerning enterprise resource planning (ERP) software that is hosted in the cloud. This apprehension stems from the growing prevalence of cloud computing, which is propelled by its intrinsic

benefits including scalability, affordability, and availability. Nevertheless, the hesitancy of organisations to completely adopt cloud-based enterprise resource planning (ERP) can be attributed to the utmost significance attributed to safeguarding and maintaining the privacy and security of critical information. With the intention of addressing these concerns in a proactive and strategic manner, the research proposes a framework for implementation.

The purpose of this framework is to provide a comprehensive collection of principles and protocols that seek to alleviate concerns related to cloud data security. This research endeavours to provide enterprises with practical solutions that surpass theoretical assurances and offer concrete measures to improve security while capitalising on the operational efficiencies of cloud-based ERP systems through the delineation of a methodical strategy. The primary objective of the proposed implementation framework is to strike a balance between leveraging the benefits of cloud computing, particularly within the context of ERP applications, and ensuring robust data security. This involves a meticulous examination of various components, including 'Enterprise Access Directory,' 'Cloud Service Provider Access Directory,' 'Enterprise Database Fragmentation,' and 'End-user Access Queries.' Each of these elements plays a crucial role in fortifying the overall security posture of the enterprise's cloud-based ERP environment.

This research aims to provide organisations with a methodical and practical structure that enables them to make well-informed choices and execute security protocols that are customised to their unique needs. This methodology is especially pertinent in the ever-changing realm of cloud computing, where conventional on-premises frameworks are undergoing a redefinition that requires flexible and inventive security models. In essence, this research aims to promote a fundamental change in which organisations can securely adopt cloud-based enterprise resource planning (ERP) solutions, assured that their data security apprehensions are not only recognised but proactively resolved via a practical and precisely delineated implementation structure. The objective of this proactive approach is to cultivate a perception of confidence and

trustworthiness within organisations, motivating them to leverage the revolutionary capabilities of cloud technologies while safeguarding the confidentiality and integrity of their most vital business information.

#### **7.1.2.2 Recommendations for Involving End-Users in Cloud Security**

The focal point of the proposed implementation framework lies in the active participation and engagement of end-users in the overarching landscape of cloud security. The emphasis on leveraging tools such as the 'Enterprise Access Directory,' 'Cloud Service Provider Access Directory,' 'Enterprise Database Fragmentation,' and 'End-user Access Queries' within this framework underscores a strategic focus on enlisting end-users as integral contributors to the security paradigm of enterprise data in the cloud.

Historically, end-users have been perceived as passive recipients of security protocols, lacking active involvement in the protection of their enterprise data. At the same time, this perception must change due to the complex nature of cloud-based environments and the ever-changing threat landscape. The framework acknowledges the critical importance of end-users in determining the security posture as a whole. It comprehends that their behaviours and engagements with cloud resources have a substantial influence on the durability of the security infrastructure.

The framework's 'Enterprise Access Directory' and 'Cloud Service Provider Access Directory' represent a methodical strategy for defining and controlling access privileges. Organisations can establish a transparent and accountable system that enables precise definition and control of access rights by integrating end-users into these directories. This not only strengthens the protection of data but also cultivates a sense of accountability among end-users, as they are consciously cognizant of their responsibilities in upholding the security of the cloud environment. Furthermore, the framework's 'Enterprise Database Fragmentation' component adds a strategic dimension to the processes of data storage and modification. Data is inherently

dispersed across multiple segments during fragmentation, which increases the complexity of unauthorised access attempts. By strictly adhering to access protocols and policies, end-users play a crucial role in safeguarding the integrity of these fragmented data components, thereby enhancing the overall resilience of the defence against potential security intrusions.

The incorporation of 'End-user Access Queries' highlights a proactive and adaptable security strategy. Through the provision of end-user inquiry capabilities pertaining to their data security status and access permissions, the framework fosters an environment that encourages vigilance and responsibility. By encouraging end-users to actively monitor and assess the security of their data, this participatory role fosters a sense of collective responsibility regarding the maintenance of a secure cloud environment. Fundamentally, the strategic prioritisation of engaging end-users in the security framework signifies an esteemed acknowledgment of their capacity to actively contribute to the overall effectiveness of cloud security. This perspective extends beyond the conventional understanding of security as an exclusively technological undertaking and recognises end-users as crucial stakeholders in the ongoing endeavour to strengthen the cloud infrastructure. By adopting this inclusive approach, the organisation not only strengthens its security stance but also fosters a security-aware culture among end-users, thus establishing a more resilient defence against ever-changing cyber threats in the cloud environment.

### **7.1.2.3 Recommendations for better Communication Practices**

The recognition of the significance of communication in the initial study highlights a crucial comprehension among researchers that proficient communication is of the utmost importance in the realm of cloud data security. This acknowledgment signifies a practical understanding that surpasses the technical complexities of security protocols and emphasises the critical importance of effective and transparent communication in guaranteeing the triumph and effectiveness of security measures within a cloud computing setting. The results of the initial study demonstrate that effective communication within the enterprise is an essential element of any

comprehensive cloud data security strategy and not solely an auxiliary one. When considering security protocols, specifically those related to Enterprise Resource Planning (ERP) systems hosted in the cloud, it becomes apparent that a clear and transparent communication framework is essential. The framework ought to comprise a variety of communication channels, protocols, and guidelines that enable a smooth and uninterrupted exchange of information among distinct stakeholders within the institution. Effective channels of communication are critical for the distribution of critical information pertaining to security policies, updates, and optimal methodologies. This ensures that all relevant parties, such as administrators, decision-makers, and end-users, are adequately apprised regarding the implemented security protocols and understand their responsibilities in upholding the integrity of the cloud environment. Additionally, it facilitates the distribution of prompt alerts and notifications regarding security incidents or policy modifications, thereby encouraging a proactive reaction to emergent threats.

Moreover, the prioritisation of communication protocols implies a methodical framework for transmitting data pertaining to the security of cloud-based data. This entails the establishment of uniform protocols for the reporting of security incidents, the pursuit of explanation regarding access inquiries, and the distribution of notifications regarding the ever-changing threat environment. These procedures are streamlined by clearly defined communication protocols, which reduce ambiguity and guarantee the efficient transmission of vital security information across the entire enterprise. The initial study provides enterprises with practical teachings that offer valuable insights into improving communication practices with regard to cloud data security. These lessons have the potential to function as a manual for executing communication tactics that are not only efficacious but also customised to the unique intricacies of cloud computing. This may entail the incorporation of communication tools that are intuitive for adopting enterprise end-users, regular training sessions pertaining to security protocols, and the cultivation of a communication environment that promotes openness and cooperation. Fundamentally, the emphasis on communication that was emphasised in the initial study emphasises the fact that

effective communication is critical to the successful implementation of cloud security measures.

The pragmatic lessons that can be extracted from this prioritisation offer enterprises practical insights that can be utilised to cultivate improved communication practices. This, in turn, enhances the resilience and responsiveness of the approach towards cloud data security. The confirmation of the value of communication in the domain of cloud data security through a initial study adds practical validity to the research findings. It demonstrates that the proposed framework and associated recommendations are not purely theoretical but have practical implications that align with real-world scenarios.

#### **7.1.2.4 Enhanced Cloud Adoption among Nigerian SMEs**

This study addresses the concerns surrounding data security in the cloud, a barrier to widespread adoption among Nigerian SMEs. It provides a strategic response to these concerns by proposing an implementation framework that offers practical solutions to mitigate these concerns. The framework aims to instil confidence among enterprises considering cloud services, particularly in cloud-based Enterprise Resource Planning (ERP) software. The framework's focus on robust security measures not only alleviates fears but also instils trust and assurance in the security capabilities of cloud environments. This enhanced confidence is poised to act as a catalyst for increased cloud adoption among Nigerian enterprises. The assurance provided by the proposed security measures could potentially tip the balance in favour of cloud adoption, overcoming one of the most significant hurdles that have impeded organizations from fully harnessing the advantages of cloud computing technologies. By fostering an environment where data security concerns are effectively addressed through the proposed framework, organizations stand to benefit from the inherent advantages offered by cloud services. The cost-effectiveness and scalability of cloud computing, coupled with the flexibility it affords, become more accessible to enterprises that may have hesitated due to security apprehensions. This enables organizations to optimize their operations, streamline IT infrastructure, and respond more effectively to the dynamic demands of a digital business landscape. In summary, the emphasis on

addressing data security concerns and providing a practical implementation framework has tangible implications for organizational decision-makers.

### **7.1.3 Policy Implications**

The research has significant implications for cloud service providers and enterprises in terms of service level agreements (SLAs) and cloud security models. These include the inclusion of security measures in SLAs, prerequisites for dataset classification, mandatory Enterprise Access Directory requirements, user training and awareness programs, customization of security models, and continuous auditing and monitoring of performance. Service level agreements (SLAs) can be revised and improved to incorporate specific security measures highlighted in the research. Enterprises should prioritize the preparation of a comprehensive dataset classification before migrating their data to the cloud. Cloud service providers may provide instructions or tools to help adopting enterprises in classifying their datasets, ensuring a standardized and secure approach to data management.

A mandatory Enterprise Access Directory is required by cloud service providers, which can be described in SLAs as an up-to-date requirement for efficient access control and user management especially in the Nigerian content. This requirement can be clearly stated in SLAs, stating that an up-to-date directory is necessary for efficient access control and user management. Programs for user training and awareness can be developed through SLAs, educating end-users about the importance of their activities in ensuring cloud data security. Cloud service providers may also stipulate resources, training materials, or support to assist adopting enterprises in educating their employees on the implications of cloud computing security. Customization of the security model can be incorporated into organizational policy by executives in charge of information technology within enterprises. This could involve measures to mitigate the influence of end-user activities on overall security posture. Regular audits can be included to evaluate the efficiency of security measures and the degree to which policies agreed upon are being adhered to. In conclusion, the research findings emphasize the importance of having clear contractual agreements (SLAs) that reflect



the complex security requirements of cloud computing. These agreements should be dynamic, allowing for changes and improvements in security measures over time. Collaboration between cloud service providers and adopting enterprise is crucial for creating a secure cloud environment.

## **7.2 Project Strengths**

This thesis reviews academic literature on enterprise, data, information security fundamentals, cloud computing, cloud computing security models, and human factors concepts. It examines cloud computing security models and end-user security responsibility in ensuring enterprise data security in public cloud environments. The study aims to identify deficiencies in the culture of information security within SMEs organizations in Nigeria and proposes an End-user Data Access Management Implementation Framework for enterprise ERP software based in the public cloud.

The proposed framework uses Enterprise Access Directory (EAD), Enterprise Database Fragmentation (EDF), and End-user Access Quires (EAQ) to control who has access to enterprise data in the cloud. The goal is to encourage end-user participation in enterprise cloud data security while reducing the impact of malicious insiders on the data. The framework can be classified as a cloud-based SaaS data security framework. The research findings show that the proposed framework's attributes, such as proper access management within the Cloud Service, are preferred by the research participants.

The project also investigates how both direct and indirect human factors can affect enterprise data security. The concept of Enterprise Database Fragmentation in the Cloud improves enterprise data security of a Cloud-based ERP software system, contributing to the academic literature on these areas. The initial study of the research exercise revealed enterprise employees' trust concerns about the Cloud Service Provider (CSP) and the blame culture among them regarding enterprise data security in the cloud. Further literature reviews and interviews with enterprise employees contributed to the academic literature in these areas.

### **7.3 Project Limitation**

The study used a mixed-method research evaluation methodology, which had limitations during implementation. The creation of survey questions was limited due to the lack of standard questions in literature reviews. The study also faced risks due to global pandemic instability, which limited the options for alternative research methodologies. The mixed-method approach relied heavily on internet data collection and included both quantitative and qualitative data sections. Despite these limitations, the mixed method supported the concept of the proposed model. The number of participants was small compared to the initial sample sizes, but the quality of opinions was prioritized. To increase the number of participants, the study extended the research period and received 43 responses by the end of eight weeks.

### **7.4 Further Research Recommendation**

A few recommendations for future research:

1. **Exploring End-User Involvement in Cloud Data Security:** Future research could delve deeper into understanding the role of end-users in cloud data security within enterprises. This could involve investigating the motivations, challenges, and best practices for promoting end-user participation in ensuring the security of enterprise data in the cloud. Exploring strategies to incentivize and empower end-users to actively engage in security measures could be particularly insightful.
2. **Enhancing Communication Strategies for Policy Adherence:** Building upon the findings regarding the significance of communication in influencing end-user adherence to security policies, future research could focus on developing and testing effective communication strategies. Investigating the impact of different communication methods, channels, and content on end-user compliance with security policies could provide valuable insights for enhancing data management security within enterprises.
3. **Evaluation of Framework Implementation Across Diverse Enterprises:** Further research could involve implementing and evaluating the proposed

framework across a diverse range of enterprises. This would allow for the assessment of the framework's effectiveness and adaptability in different organizational contexts and industries. Additionally, exploring any challenges or barriers encountered during the implementation process and identifying strategies for overcoming them would be beneficial.

4. **Longitudinal Studies on Cloud Computing Security:** Conducting longitudinal studies to track the evolving landscape of cloud computing security over time would provide valuable insights into emerging trends, challenges, and best practices. By examining how security models and frameworks adapt to technological advancements and changing threat landscapes, researchers can contribute to the ongoing refinement and enhancement of cloud security measures.

In summary, future research endeavors should focus on exploring end-user involvement in cloud data security, enhancing communication strategies for policy adherence, evaluating framework implementation across diverse enterprises, and conducting longitudinal studies on cloud computing security. Addressing these areas will contribute to advancing knowledge and practices in securing enterprise data in the cloud, ultimately facilitating the wider adoption of cloud-based Enterprise Resource Planning systems.

## **7.5 Summary of Chapter 7**

This research sought to develop an enterprise data management security model for enterprise system software in the public cloud, which will be supported by the critical review of the actions of an employee that poses a risk to data security within the enterprise. This thesis reviews several Cloud Computing Security Models with a close look at the model that addresses data security challenges in cloud-based Enterprise Resource Planning (ERP) systems and is confident in introducing an End-user Authentication Control model for public cloud-based ERP systems.

This cloud computing security model uses Enterprise Access Directory, Enterprise Data Fragmentation in the cloud and End-user Access Queries, to ensure that End users share greater security responsibility with the cloud service provider. The model was compared with other existing models, and it is clear that more adopter end-user participation in enterprise data security in the public cloud is essential. The proposed framework also shows that to mitigate the impact that a malicious insider will have on the enterprise cloud data set, no single user should be able to gain access to the whole cloud-based enterprise database. The proposed model considers the end-user role and responsibility within the enterprise to determine the level of access to data in the cloud-based ERP system.

The study's key findings are that impact of cloud computing is significant on data security. In addition, most of the study participants favoured implementing cloud computing in their enterprises, yet they also had concerns about ERP software. The concepts of the proposed model and its different attributes were reviewed. The findings show that the attributes of the proposed model were favoured by the research participants. For instance, the research assumption 4: a proper Access Management within the Cloud Service End-user enterprise would positively improve their enterprise data security in Cloud, was explored using the following research questions SQ5, SQ6, SQ7, SQ9 and SQ10 and, in all instances, the research participants favoured research assumption 4.

It is necessary to conduct a thorough analysis of how the implementation of the proposed model will help solve the problems facing cloud-based ERP implementation and to evaluate the effect of the implementation using other possible research methods. The project aims were achieved, and several strengths and weaknesses of this project were presented in section 7.2 and section 7.3. Several areas of further research were also identified and discussed in this thesis. For instance, a new study can investigate and evaluate more how the similarity and difference of CSPA.D. and E.A.D will enhance the security of the enterprise data in the public cloud, this is an interesting area to explore more as it will contribute to the literature in this field.

## Reference

- A Vouk, M., *Cloud computing—issues, research and implementations*. Journal of Computing and Information Technology, 2008. **16**(4): p. 235-246.
- Abbdal, S.H., et al. *An Efficient Public Verifiability and Data Integrity Using Multiple TPAs in Cloud Data Storage*. in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*. 2016. IEEE.
- Abd Elmonem, M. A., et al. (2016). "Benefits and challenges of cloud ERP systems—A systematic literature review." *Future Computing and Informatics Journal* 1(1-2): 1-9.
- Aberdeen, T. and Yin, R.K., 2013. Case study research: Design and methods . Thousand Oaks, CA: Sage. *Can J Action Res*, 14, pp.69-71.
- Abi T. T., 2022, September. The 67 Biggest Data Breaches. [https://www.google.co.uk/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CAMQw7AJahcKEwi4jcXLk5z7AhUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.upguard.com%2Fblog%2Fbiggest-data-breaches&psig=AOvVaw3Ont7c4LWZdKUKF\\_\\_idyRI&ust=1667912937064451](https://www.google.co.uk/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CAMQw7AJahcKEwi4jcXLk5z7AhUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.upguard.com%2Fblog%2Fbiggest-data-breaches&psig=AOvVaw3Ont7c4LWZdKUKF__idyRI&ust=1667912937064451)
- Abubakar, A., et al. (2014). "Cloud computing: Adoption issues for sub-saharan African SMEs." *The Electronic Journal of Information Systems in Developing Countries* 62(1): 1-17.
- Aceto, G., et al. (2018). "The role of Information and Communication Technologies in healthcare: taxonomies, perspectives, and challenges." *Journal of Network and Computer Applications* 107: 125-154.

- Achunike, V. U. and F. C. Egbuna (2016). "Synopsis of Cyber-attacks Incidents and Impacts on Oil and Gas Critical Infrastructures: A Nigerian Perspective."
- Adebola, B. D. (2014). The determinant of information security practices towards organizational performance in the banking sector evidence from Nigeria, Universiti Utara Malaysia.
- Afolabi, A., et al. (2022). "Gauging parameters for e-procurement acquisition in construction businesses in Nigeria." *International Journal of Construction Management* 22(3): 426-435.
- Aggarwal S, Kumar N. Hashes. In *Advances in Computers* 2021 Jan 1 (Vol. 121, pp. 83-93). Elsevier.
- Aghaunor, Gabriel, and Bukky E. Okojie. "Factors Influencing the Implementation of Information Security Risk Management: A case study of Nigerian Commercial Banks." *Digitala Vetenskapliga Arkivet DiVA*, <https://www.diva-portal.org/smash/get/diva2:1672230/FULLTEXT01.pdf> (2022).
- Aghimien, D. O., et al. (2021). "Unravelling the factors influencing construction organisations' intention to adopt big data analytics in South Africa." *Construction Economics and Building* 21(3): 262-281.
- Ahmad, S., et al. (2016). Tokenization based service model for cloud computing environment. 2016 International Conference on Inventive Computation Technologies (ICICT), IEEE.
- Ahmad, W., et al. (2021). "Cyber security in IoT-based cloud computing: A comprehensive survey." *Electronics* 11(1): 16.
- Ahmed Elragal and Malak El Kommos, "In-House versus In-Cloud ERP Systems: A Comparative Study," *Journal of Enterprise Resource Planning Studies*, vol. 2012, Article ID 659957, 13 pages. DOI: 10.5171/2012. 659957.
- Ahmed, Munir, et al. "Human errors in information security." *International Journal of Advanced Trends in Computer Science and Engineering* 1.3 (2012): 82-87.

- Ahmed, A. and T. Zakariae (2018). "IaaS cloud model security issues on behalf cloud provider and user security behaviors." *Procedia Computer Science* 134: 328-333.
- Ahn, B. and H. Ahn (2020). "Factors affecting intention to adopt cloud-based ERP from a comprehensive approach." *Sustainability* 12(16): 6426.
- Ahn, Byungchan, and Hyunchul Ahn. "Factors affecting intention to adopt cloud-based ERP from a comprehensive approach." *Sustainability* 12.16 (2020): 6426.
- Aiken, M., et al. (2006). "15 Social Enterprise in the UK." *Social Enterprise in Western Europe*: 253.
- Ajoudanian, Sh, and M. R. Ahmadi. "A novel data security model for cloud computing." *International Journal of Engineering and Technology* 4.3 (2012): 326 – 329.
- Akin, O. C., et al. (2014). "The impact and challenges of cloud computing adoption on public universities in Southwestern Nigeria." *International Journal of Advanced Computer Science and Applications* 5(8): 13-19.
- Akintokunbo, O. O. and B. E. Arimie (2021). "Supply Chain Management: A Game Changer in the Oil and Gas industry in Nigeria: A Review of Literature." *International Journal of Supply Chain and Logistics* 5(3): 54-68.
- Albulayhi, K., et al. (2020). Fine-grained access control in the era of cloud computing: An analytical review. 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), IEEE.
- Al-Darwish AI, Choe P. A framework of information security integrated with human factors. In *International Conference on Human-Computer Interaction 2019 Jul 26* (pp. 217-229). Springer, Cham.
- Al-Ghofaili, A. A. and M. A. Al-Mashari (2014). ERP system adoption traditional ERP systems vs. cloud-based ERP systems. Fourth edition of the *International Conference on the Innovative Computing Technology (INTECH 2014)*, IEEE.

- Al-Johani, A. A. and A. E. Youssef (2013). "A framework for ERP systems in SME based on cloud computing technology." *International Journal on Cloud Computing: Services and Architecture* 3(3): 1-14.
- Al-Okaily, M., Alkhwalidi, A.F., Abdulmuhsin, A.A., Alqudah, H. and Al-Okaily, A. (2022), "Cloud-based accounting information systems usage and its impact on Jordanian SMEs' performance: the post-COVID-19 perspective", *Journal of Financial Reporting and Accounting*, Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/JFRA-12-2021-0476>
- Al Noor, Shahid, et al. "A proposed architecture of cloud computing for education system in Bangladesh and the impact on current education system." *IJCSNS International Journal of Computer Science and Network Security* 10.10 (2010): 7-13.
- Aldossary S, Allen W. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications*. 2016;7(4).
- Alhogail, Areej, and Abdulrahman Mirza. "A FRAMEWORK OF INFORMATION SECURITY CULTURE CHANGE." *Journal of Theoretical & Applied Information Technology* 64.2 (2014). p. 540 – 541
- Alhomdy, S., et al. (2021). "The role of cloud computing technology: A savior to fight the lockdown in COVID 19 crisis, the benefits, characteristics and applications." *International Journal of Intelligent Networks* 2: 166-174.
- Ali, Azham Md, and Hamidah Yusof. "Quality in qualitative studies: The case of validity, reliability and generalizability." *Issues in Social and Environmental Accounting* 5.1 (2011): 25-64.
- Ali, U. T., et al. (2021). "Investigating Factors Influencing Electronic Commerce Adoption in Developing Countries: The Case of Nigeria." *Journal of Emerging Technologies and Innovative Research* 8.
- Alqudah, M. and R. Razali (2016). "A review of scaling agile methods in large software development." *International Journal on Advanced Science, Engineering and Information Technology* 6(6): 828-837.



- Altman, D., et al. "Why do a initial study." *National Centre for Replacement, Refinement and Reduction of Animal in Research* 12 (2006). Consulted 2.2.2011 <http://www.nc3rs.org.uk/downloaddoc.asp?id=400>.
- Alzahrani, A., et al. (2021). "End users' resistance behaviour paradigm in pre-deployment stage of ERP systems: evidence from Bangladeshi manufacturing industry." *Business Process Management Journal* 27(5): 1496-1521.
- AlZain, Mohammed A., et al. "Cloud computing security: from single to multi-clouds." *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2012.
- Amue, G. J. and H. Ozuru (2014). "Supply chain integration in organizations: An empirical investigation of the Nigeria oil and gas industry." *International Journal of Marketing Studies* 6(6): 129.
- Anakath, A., et al. (2019). "Privacy preserving multi factor authentication using trust management." *Cluster Computing* 22(Suppl 5): 10817-10823.
- Ananya, B., et al. (2023). "Survey of applications, advantages, and comparisons of AES encryption algorithm with other standards." *International Journal of Computational Learning & Intelligence* 2(2): 87-98.
- Anciaux N, Bonnet P, Bouganim L, Nguyen B, Pucheral P, Popa IS, Scerri G. Personal data management systems: The security and functionality standpoint. *Information Systems*. 2019 Feb 1;80:13-35.
- Anderson, Kathryn, and Dana C. Jack. "Learning to listen: Interview techniques and analyses." *The oral history reader*. Routledge, 2002. 171-185.
- Annamalai, C., and T. Ramayah. "Does an implementation stage act as a moderator in enterprise resource planning (ERP) projects in India? An empirical study." *Asian Journal of Research in Banking and Finance* 2.2 (2012): 200-227.
- Aral S, Brynjolfsson E, Wu L. Three-way Complementarities: Performance pay, Human Resource Analytics, and Information Technology. *Management Science*. 2012 May;58(5):913-931.

- Arbanas, Krunoslav, Mario Spremic, and Nikolina Zajdela Hrustek. "Holistic framework for evaluating and improving information security culture." *Aslib Journal of Information Management* (2021).
- Arif, M., et al. (2005). "Enterprise information systems: technology first or process first?" *Business Process Management Journal* 11(1): 5-21.
- Ary, Donald, et al. "Introduction to research in education: Cengage Learning." *Journal of Correctional Education* (2013): 9-22.
- Ashish, M. K. S. V. K. (2014). "Security and concurrency control in distributed database system." *International Journal of scientific research and management (IJSRM)* 2(12).
- Avram, M.G. Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology*. 2014 Jan 1, 12, pp.529-534.
- Avstriyskaya, E. M., and L. I. Voronova. "Determination of effective technical device ensuring the security of transmitted information over a communication channels in industrial control systems at industrial enterprises in the Russian Federation." *Computer Applications for Management and Sustainable Development of Production and Industry (CMSD2021)*. Vol. 12251, pp. 36-40 SPIE, 2022.
- Awan, M., et al. (2021). "An empirical investigation of the challenges of cloud-based ERP adoption in Pakistani SMEs." *Scientific Programming* 2021: 1-8.
- Aw B.Y., Productivity dynamics of small and medium enterprises in Taiwan (China). World Bank Institute; 2001.
- Ayofe, A. N. and B. Irwin (2010). "Cyber security: Challenges and the way forward." *Computer Science & Telecommunications* 29(6).
- Badidi, E. *A cloud service broker for SLA-based SaaS provisioning*. in *International Conference on Information Society (i-Society 2013)*. 2013. IEEE.
- Bagretsov, G.I., Shindarev, N.A., Abramov, M.V. and Tulupyeva, T.V., 2017, May. Approaches to development of models for text analysis of information in social network profiles in order to evaluate user's vulnerabilities profile. In *2017 XX*

*IEEE International Conference on Soft Computing and Measurements (SCM)* (pp. 93-95). IEEE.

Bahssas, D. M., et al. (2015). "Enterprise resource planning (ERP) systems: design, trends and deployment." *The International Technology Management Review* 5(2): 72-81.

Balachandran, Bala M., and Shivika Prasad. "Challenges and benefits of deploying big data analytics in the cloud for business intelligence." *Procedia Computer Science* 112 (2017): pp. 1112-1122.

Balawejder B, Dankiewicz R, Ostrowska-Dankiewicz A, Tomczyk T. The role of insurance in cyber risk management in enterprises. *Humanities and Social Sciences*. 2019 Dec 31;26(4): pp.19-32.

Baldini, I., et al. (2017). "Serverless computing: Current trends and open problems." *Research advances in cloud computing*: 1-20.

Balfour, R. E. (2014). An emergency information sharing (EIS) framework for effective shared situational awareness (SSA). *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*, IEEE.

Barona, R. and E. M. Anita (2017). A survey on data breach challenges in cloud computing security: Issues and threats. 2017 International conference on circuit, power and computing technologies (ICCPCT), IEEE.

Beck, Ulrich. *Individualization: Institutionalized individualism and its social and political consequences*. Vol. 13. Sage, 2002.

Beleț, T. and A. A. Purcărea (2017). "The Evolution of Enterprise Resource Planning Systems." *International Journal of Advanced Engineering, Management and Science* 3(12): 239942.

Bell, E., Bryman, A., & Harley, B. (2018). *Business research methods*. Oxford University Press.

Bello, P. (2021). The role of digitalization in decarbonizing the oil and gas industry. *SPE Nigeria Annual International Conference and Exhibition*, SPE.

- Bellovin, S. M. and W. R. Cheswick (1994). "Network firewalls." *IEEE communications magazine* 32(9): 50-57.
- Bender, B., et al. (2022). "A proposal for future data organization in enterprise systems—an analysis of established database approaches." *Information Systems and e-Business Management* 20(3): 441-494.
- Berry, M.J. and Linoff, G.S. *Data mining techniques: for marketing, sales, and customer relationship management*. John Wiley & Sons. 2004.
- Berry, Pamela Ruth. *Financial Planning and Control Systems: Essential tools to increase the survival rate of micro and small manufacturing enterprises in the Tshwane Metropolitan area*. PhD dissertation., University of South Africa, 2010.
- Besnard, D. and B. Arief, *Computer security impaired by legitimate users*. *Computers & Security*, 2004. **23**(3): p. 253-264.
- Bezemer, C.-P. and A. Zaidman (2010). Multi-tenant SaaS applications: maintenance dream or nightmare? Proceedings of the joint ercim workshop on software evolution (evol) and international workshop on principles of software evolution (iwps).
- Bhardwaj, S., et al. (2010). "An approach for investigating perspective of cloud software-as-a-service (SaaS)." *International Journal of Computer Applications* 10(2): 40-43.
- Bhardwaj, Sushil, Leena Jain, and Sandeep Jain. "Cloud computing: A study of infrastructure as a service (IAAS)." *International Journal of Engineering and Information Technology* 2.(1) (2010): 60-63.
- Bhardwaj, S., L. Jain, and S. Jain, *An approach for investigating perspective of cloud software-as-a-service (SaaS)*. *International Journal of Computer Applications*, 2010. **10**(2): p. 40-43.
- Bhuyar, P., et al. (2012). "Horizontal fragmentation technique in distributed database." *International Journal of Scientific and Research Publications* 2(5): 1-7.

- Bijon, K.Z., R. Krishnan, and R. Sandhu. *A formal model for isolation management in cloud infrastructure-as-a-service*. in *International Conference on Network and System Security*. 2015. Springer.
- Birk, D. and C. Wegener (2011). Technical issues of forensic investigations in cloud computing environments. 2011 Sixth IEEE international workshop on systematic approaches to digital forensic engineering, IEEE.
- Bisong, Anthony, and M. Rahman. "An overview of the security concerns in enterprise cloud computing." arXiv preprint arXiv:1101.5613 (2011).
- Biswas, S., et al. (2022). The art and practice of data science pipelines: A comprehensive study of data science pipelines in theory, in-the-small, and in-the-large. Proceedings of the 44th International Conference on Software Engineering.
- Bjelland, E. and M. Haddara (2018). "Evolution of ERP systems in the cloud: A study on system updates." *Systems* 6(2): 22.
- Bollinger, A.S. and Smith, R.D. Managing organizational knowledge as a strategic asset. *Journal of knowledge management*. 2001 Mar 1.
- Bond, Michael Harris. "Finding universal dimensions of individual variation in multicultural studies of values: The Rokeach and Chinese value surveys." *New research on moral development: Moral development a compendium* (1994): 385-391.
- Borghoff, U.M. and R. Pareschi, Information technology for knowledge management. *Journal of Universal Computer Science*, 1997. 3(8): p. 835-842.
- Borky, J. M., et al. (2019). "Protecting information with cybersecurity." *Effective Model-Based Systems Engineering*: 345-404.
- Boruch, R. F. (1971). "Educational research and the confidentiality of data: A case study." *Sociology of Education*: 59-85.
- Bradford, M., et al. (2014). "Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization

- Environment framework." *International Journal of Accounting Information Systems* 15(2): 149-165.
- Brennan, L., Voros, J., & Brady, E. (2011). Paradigms at play and implications for validity in social marketing research. *Journal of Social Marketing*, 1(2), 100-119.
- Brown, L. T. (2018). Human factors and the insider threat to electronic health records: A case study, Northcentral University.
- Bryman, A., *Of methods and methodology*. *Qualitative Research in Organizations and Management: An International Journal*, 2008. 3(2): p. 159-168.
- Bryman, A., Becker, S., & Sempik, J. (2008). Quality criteria for quantitative, qualitative and mixed methods research: a view from social policy. *International Journal of Social Research Methodology*, 11(4), 261-276.
- Bryman, A. (2012). *Social research methods*. 4th Edn. Oxford University Press.
- Brymer, R.A. Stress and your employees. *Cornell Hotel and Restaurant Administration Quarterly*. 1982, 22(4), pp.61-66.
- Brzycki D, Dudt K. Overcoming barriers to technology use in teacher preparation programs. *Journal of Technology and teacher education*. 2005 Oct;13(4):619-641.
- Bui, Thuy Linh. *Internal Communication in the Digital Workplace: Digital Communication Channels and Employee Engagement*. (2019).
- Bushell, E.J., *The Widespread Consequences of Outsourcing*. *Air Power Australia Analyses*, 2010. 7(3): p. 1.
- Cameron, Kim S., and Robert E. Quinn. *Diagnosing and changing organizational culture: Based on the competing values framework*. John Wiley & Sons, 2011.
- Carney, W. J. (1994). "Limited liability companies: Origins and antecedents." *U. Colo. l. rev.* 66: 855.
- Carr, Linda T. "The strengths and weaknesses of quantitative and qualitative research: what method for nursing?." *Journal of advanced nursing* 20.4 (1994): 716-721.

- Carroll, J. M. (1990). The three faces of information security. *Advances in Cryptology—AUSCRYPT'90: International Conference on Cryptology Sydney, Australia, January 8–11, 1990 Proceedings 1*, Springer.
- Carroll, M., et al. (2011). Secure cloud computing: Benefits, risks and controls. 2011 *Information Security for South Africa*, IEEE.
- Carstens, Deborah Sater, Pamela R. McCauley-Bell, Linda C. Malone, and Ronald F. DeMara. Evaluation of the human impact of password authentication practices on information security. *Informing Science Journal Volume 7*, (2004): 68-85
- Casaló, L. V., et al. (2011). "The generation of trust in the online services and product distribution: the case of Spanish electronic commerce." *Journal of Electronic Commerce Research* 12(3): 199.
- Castellani, D., et al. (2022). "International connectivity and the location of multinational enterprises' knowledge-intensive activities: Evidence from US metropolitan areas." *Global Strategy Journal* 12(1): 82-107.
- Cavusoglu, H., et al. (2009). "Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems." *Information Systems Research* 20(2): 198-217.
- Cecelja, F. (2002). *Manufacturing Information and Data Systems: Analysis, Design and Practice*, Elsevier.
- Cérin, C., et al., *Downtime statistics of current cloud solutions*. International Working Group on Cloud Computing Resiliency, Tech. Rep, 2013.
- Cetindamar D, Abedin B, Shirahada K. The Role of Employees in Digital Transformation: a preliminary study on how employees' digital literacy impacts use of digital technologies. In *IEEE Transactions on Engineering Management*. 2021 Jun 28. pp. 1-12. doi: 10.1109/TEM.2021.3087724.
- Chadwick, D.W., et al., *A cloud-edge based data security architecture for sharing and analysing cyber threat information*. *Future Generation Computer Systems*, 2020. **102**: p. 710-722.

- Charles, M. and P. Le Billon (2021). "Corporate accountability and diplomatic liability in overseas extractive projects." *The Extractive Industries and Society* 8(1): 467-476.
- Chaturvedi, D.A. and S.A. Zarger, *A review of security models in cloud computing and an Innovative approach*. *International Journal of Computer Trends and Technology (IJCTT)*, 2015. **30**(2): p. 87-92.
- Chauhan, M. and S. Shiaeles (2023). "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions." *Network* 3(3): 422-450.
- Che J, Duan Y, Zhang T, Fan J. Study on the security models and strategies of cloud computing. *Procedia Engineering*. 2011 Jan 1;23(1): pp.586-593.
- Chen, D. and H. Zhao (2012). Data security and privacy protection issues in cloud computing. 2012 international conference on computer science and electronics engineering, IEEE.
- Chen, S.-L., et al. (2014). "A new approach to integrate internet-of-things and software-as-a-service model for logistic systems: A case study." *Sensors* 14(4): 6144-6164.
- Cheng, F.-C. and W.-H. Lai, *The impact of cloud computing technology on legal infrastructure within internet—focusing on the protection of information privacy*. *Procedia Engineering*, 2012. **29**(1): p. 241-251.
- Cherdantseva, Y. and J. Hilton (2013). A reference model of information assurance & security. 2013 International Conference on Availability, Reliability and Security, IEEE.
- Chittenden, F., et al. (2003). "Tax regulation and small business in the USA, UK, Australia and New Zealand." *International Small Business Journal* 21(1): 93-115.
- Chofreh, A. G., et al. (2014). "Sustainable enterprise resource planning: imperatives and research directions." *Journal of Cleaner Production* 71: 139-147.
- Choi, D. Y. and E. R. Gray (2008). "The venture development processes of "sustainable" entrepreneurs." *Management Research News* 31(8): 558-569.



- Choi, Namjoo, et al. "Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action." *Information Management & Computer Security* (2008). **16**(5) pp. 484-501.
- Chou, D.C., *Cloud computing: A value creation model*. Computer Standards & Interfaces, 2015. **38**: p. 72-77.
- Chou, Y., *Cloud Computing Primer for IT Pros*. Microsoft: TechNet, 2010.
- Choudhary, A. S., et al. (2018). A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks. 2018 3rd International Conference on Inventive Computation Technologies (ICICT), IEEE.
- CHU, Hai Hong Thi, and Thuy Van NGUYEN. "*Factors Influencing Successful Implementation of Cloud ERP Solutions at Small and Medium Enterprises in Vietnam*." *The Journal of Asian Finance, Economics and Business*. **9**(5) (2022): 239-250.
- Chung, N.N., Hung, P.D. (2020). Logging and Monitoring System for Streaming Data. In: Luo, Y. (eds) *Cooperative Design, Visualization, and Engineering*. CDVE 2020. *Lecture Notes in Computer Science*, 2020 Oct 25 (pp. 184-191). vol 12341. Springer, Cham. [https://doi.org/10.1007/978-3-030-60816-3\\_21](https://doi.org/10.1007/978-3-030-60816-3_21)
- Ciampa, P. D. and B. Nagel (2020). "AGILE Paradigm: The next generation collaborative MDO for the development of aeronautical systems." *Progress in Aerospace Sciences* 119: 100643.
- Cioloa, C. and M. Georgescu (2011). "Increasing database performance using indexes." *Database Systems Journal* 2(2): 13-22.
- Coetzee, L. and J. Eksteen (2011). The Internet of Things-promise for the future? An introduction. 2011 IST-Africa Conference Proceedings, IEEE.
- Colwill, Carl. "*Human factors in information security: The insider threat—Who can you trust these days?*." *Information Security Technical Report* 14.4 (2009): 186-196.
- Computing, C. and M. Creeger (2009). "Cloud computing: An overview." *Distributed Computing* 7(5).

- Coronado, A.S., *Corporate computer and network security*. 2012, Taylor & Francis.
- Cowling, M., et al. (2023). "Ethnicity and bank lending before and during COVID-19." *International Journal of Entrepreneurial Behavior & Research* 29(3): 614-642.
- Coyne, E. and T. R. Weil (2013). "ABAC and RBAC: scalable, flexible, and auditable access management." *IT professional* 15(03): 14-16.
- Creswell, John W., and J. David Creswell. *Research design: Qualitative, quantitative, and mixed methods approaches*. (2nd ed.). London: Sage Publications Ltd, 2003.
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approach* (3rd ed.). Thousand Oaks, CA: Sage.
- Creswell, John W., and Wanqing Zhang. "The application of mixed methods designs to trauma research." *Journal of Traumatic Stress: Official publication of the international society for traumatic stress studies* 22.6 (2009): 612-621.
- Creswell, J. W., & Plano Clark, V. L. (2007). *Designing and conducting mixed methods research*. Thousand Oaks: CA, Sage.
- Creswell, J. W. (2012). *Qualitative inquiry and research design: Choosing among five approaches*: Thousand Oaks, CA: Sage Publications.
- Crusto, M. F. (2001). "Extending the Veil to Solo Entrepreneurs: A Limited Liability Sole Proprietorship Act (LLSP)." *Colum. Bus. L. Rev.*: 381.
- D'arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*. 2011 Nov; 20(6): pp. 643-658.
- Da Xu, L. (2011). "Enterprise systems: state-of-the-art and future trends." *IEEE transactions on industrial informatics* 7(4): 630-640.
- Danquah M, Amankwah-Amoah J. Assessing the relationships between human capital, innovation and technology adoption: Evidence from sub-Saharan Africa. *Technological Forecasting and Social Change*. 2017 Sep 1;122: pp.24-33.

- Davenport, T.H. and L. Prusak, *Working knowledge: How organizations manage what they know*. 1998: Harvard Business Press.
- David, D.P., M.M. Keupp, and A. Mermoud, *Knowledge absorption for cyber-security: The role of human beliefs*. *Computers in Human Behavior*, 2020. **106**: p. 106255.
- De Vicente Mohino, J., et al. (2019). "The application of a new secure software development life cycle (S-SDLC) with agile methodologies." *Electronics* 8(11): 1218.
- Dees, J. G. and B. B. Anderson (2017). *Sector-bending: Blurring the lines between nonprofit and for-profit*. In *search of the nonprofit sector*, Routledge: 51-72
- Demi, S. and M. Haddara (2018). "Do cloud ERP systems retire? An ERP lifecycle perspective." *Procedia Computer Science* 138: 587-594.
- Denning, D. E. and P. J. Denning (1979). "Data security." *ACM computing surveys (CSUR)* 11(3): 227-249.
- Denscombe, M. *The Good Research Guide* Open University Press, Chapter 13 &15, (2014).
- Denzin, N. K. *Aesthetics and the practices of qualitative inquiry*. *Qualitative inquiry*, (2000). 6(2), 256-265.
- Denzin, N. K., & Lincoln, Y. S. (Eds.). *The SAGE handbook of qualitative research* (4th ed.). London, England: SAGE (2011).
- Derenyiolo, B. and E. M. Joseph (2018). "Risk management and enterprise risk management in Nigeria: Implications for national development and growth." *Arabian Journal of Business and Management Review (Kuwait Chapter)* 7(3): 29-40.
- Dharmawansa, A.D. and R. Madhuwanthi, *Evaluating the Information Security Awareness (ISA) of Employees in the Banking Sector: A Case Study*. *International Research Conference Articles (KDU IRC)* 2020.

- Di Costanzo, Alexandre, Marcos Dias De Assuncao, and Rajkumar Buyya. "Harnessing cloud technologies for a virtualized distributed computing infrastructure." *IEEE internet computing* 13.5 (2009): 24-33.
- Dillon, T., C. Wu, and E. Chang. *Cloud computing: issues and challenges*. in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*. 2010. IEEE.
- Dobrin GI. Types of enterprises-main risk and impact factors specific to the complex business area. *Journal of Public Administration, Finance and Law*. 2015, (07): pp. 49-61.
- Doherty, N. F., Ashurst, C., & Peppard, J. *Factors affecting the successful realisation of benefits from systems development projects: findings from three case studies*. *Journal of Information Technology*, (2012). 27(1), 1-16.
- Domingo-Ferrer, J., et al. (2019). "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges." *Computer Communications* 140: 38-60.
- Doyle, L., Brady, A. M., & Byrne, G. *An overview of mixed methods research*. *Journal of Research in Nursing*, (2009). 14(2), 175-185.
- Driouchi, Ahmed, Cristina Boboc, and Nada Zouag. *Emigration of Highly Skilled Labor: Determinants & Impacts*. Institutue of Economic Analysis Prospective Studies, Al Akhawayn University (2009).
- Drucker PF. The new productivity challenge. In *Quality in Higher Education*. 2018 Apr 24 (pp. 37-46). Routledge. <https://doi.org/10.4324/97811351293563>
- Duan, J., et al. (2013). "Benefits and drawbacks of cloud-based versus traditional ERP systems." *Proceedings of the 2012-13 course on Advanced Resource Planning*.
- Duncan, B., A. Bratterud, and A. Happe. *Enhancing cloud security and privacy: Time for a new approach?* in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*. 2016. IEEE.
- Duncan, B. and Westerlund, M., *Cost-Effective Permanent Audit Trails for Securing SME Systems when Adopting Mobile Technologies*.

- Durana, P., et al. (2021). "Artificial intelligence data-driven internet of things systems, real-time advanced analytics, and cyber-physical production networks in sustainable smart manufacturing." *Econ. Manag. Financ. Mark* 16: 20-30.
- Eisa, Islam, Rashed Salem, and Hatem Abdelkader. "A fragmentation algorithm for storage management in cloud database environment." In 2017 12th International Conference on Computer Engineering and Systems (ICCES), pp. 141-147. IEEE, 2017.
- El-Bably, Amar Y. "Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management." *Journal of Information Security and Cybercrimes Research* 4.1 (2021): 95-102.
- Elbahri, F. M., et al. (2019). Difference comparison of SAP, Oracle, and Microsoft solutions based on cloud ERP systems: A review. 2019 IEEE 15th International Colloquium on Signal Processing & Its Applications (CSPA), IEEE.
- Eldabi, T., Irani, Z., Paul, R. J., & Love, P. E. *Quantitative and Qualitative Decision-Making methods in simulation modelling. Management Decision*, (2002). 40(1), 64-73.
- El-Gazzar RF. A literature review on cloud computing adoption issues in enterprises. In International Working Conference on Transfer and Diffusion of IT 2014 Jun 2 (pp. 214-242). Springer, Berlin, Heidelberg.
- Elragal, A. and M. Haddara (2013). "The impact of ERP partnership formation regulations on the failure of ERP implementations." *Procedia technology* 9: 527-535.
- Eminağaoğlu, M., E. Uçar, and Ş. Eren, *The positive outcomes of information security awareness training in companies—A case study*. Information Security Technical Report, 2009. **14**(4): p. 223-229.
- Esparza, J. M. (2019). "Understanding the credential theft lifecycle." *Computer Fraud & Security* 2019(2): 6-9.
- Evans, N. D. (2002). *Business agility: strategies for gaining competitive advantage through mobile business solutions*, FT Press.

- Eya N and Weir G.R. End-User Authentication Control in Cloud-based ERP Systems. In 2021 National Computing Colleges Conference (NCCC) 2021 Mar 27 (pp. 1-6). IEEE.
- Eya, N. G. (2023). An End-User Centred Framework for Data Access Management and Security in the Enterprise Public Cloud. Computer and Information Science University of Strathclyde PhD: 432.
- Fan, H., et al., *An integrated personalization framework for SaaS-based cloud services*. Future Generation Computer Systems, 2015. **53**: p. 157-173.
- Farhan, A. S. and G. M. Mostafa (2018). A methodology for enhancing software security during development processes. 2018 21st Saudi Computer Society National Computer Conference (NCC), IEEE.
- Fay J.R. What form of ownership is best?. The CPA Journal. 1998 Aug 1;68(8): pp.46.
- Feuerlicht, G. and Govardhan, S. Impact of cloud computing: beyond a technology trend. *Systems integration*. 2010. 2. pp.262-269.
- Firestone, J. M. (2007). Enterprise information portals and knowledge management, Routledge.
- Fisher M.A. Protecting confidentiality rights: The need for an ethical practice model. American Psychologist. 2008 Jan; 63(1):pp.1-13. <https://doi.org/10.1037/0003-066X.63.1.1>
- Flowerday, S. & Von Solms, R. "What constitutes information integrity?." South African Journal of Information Management 9(4) (2007): 1-19.
- Forte, Andrea, Nazanin Andalibi, and Rachel Greenstadt. "Privacy, anonymity, and perceived risk in open collaboration: A study of Tor users and Wikipedians." *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 2017. (pp. 1800-1811)
- Fraenkel, J. R., & Wallen, N. E. *Introduction to qualitative research. How to Design and Evaluate Research in Education*, 7th ed. Boston, MA: McGraw-Hill International Edition (2008).

- Freedman, J. (2000). "Limited Liability Partnerships in the United Kingdom-Do They Have a Role for Small Firms." *J. Corp. L.* 26: 897.
- Freeman, M.P., et al., *Guarding the gate: remote structured assessments to enhance enrollment precision in depression trials.* *Journal of Clinical Psychopharmacology*, 2017. **37**(2): p. 176-181
- Furht, B., *Cloud computing fundamentals*, in *Handbook of cloud computing*. 2010, Springer. p. 3-19.
- Gagne, P. and G.R. Hancock, *Measurement model quality, sample size, and solution propriety in confirmatory factor models.* *Multivariate Behavioral Research*, 2006. **41**(1): p. 65-83.
- Gajanayake, Randike, Renato Iannella, and Tony Sahama. "Sharing with care: An information accountability perspective." *IEEE Internet Computing* 15(4) (2011): 31-38.
- Gajbhiye, A. and K. M. P. Shrivastva (2014). *Cloud computing: Need, enabling technology, architecture, advantages and challenges.* 2014 5th International Conference-Confluence The Next Generation Information Technology Summit (Confluence), IEEE.
- Gambette, P. and J. Véronis (2010). *Visualising a text with a tree cloud. Classification as a Tool for Research: Proceedings of the 11th IFCS Biennial Conference and 33rd Annual Conference of the Gesellschaft für Klassifikation eV, Dresden, March 13-18, 2009*, Springer.
- Gascon, H., et al. (2011). "Analysis of update delays in signature-based network intrusion detection systems." *Computers & Security* 30(8): 613-624.
- Gill, J., Johnson, P., & Clark, M. *Research methods for managers* (4th ed.). London: Sage Publications Ltd (2010).
- Glass, S., Hiller, T., Jacobs, S. and Perkins, C. *Mobile IP authentication, authorization, and accounting requirements* (No. rfc2977). 2000, pp.1-27.
- Glesne, C., & Peshkin, A. *Becoming qualitative researchers: An introduction.* White Plains, NY: Longman (1992).

- Gnatyuk, S., et al. (2021). "Modern SIEM Analysis and Critical Requirements Definition in the Context of Information Warfare." *Cybersecurity Providing in Information and Telecommunication Systems II 2021* 3188(2): 149-166.
- Goddard, W. and S. Melville, *Research methodology: An introduction*. 2004: Juta and Company Ltd.
- Gökalp E, Martinez V. Digital transformation capability maturity model enabling the assessment of industrial manufacturers. *Computers in Industry*. 2021 Nov 1; 132:pp.103522.
- Gondree, M. and Z. N. Peterson (2013). Geolocation of data in the cloud. Proceedings of the third ACM conference on Data and application security and privacy.
- Gong, C., et al. *The characteristics of cloud computing*. in *Parallel Processing Workshops (ICPPW), 2010 39th International Conference on*. 2010. IEEE.
- Gonzalez, H., et al. (2010). Google fusion tables: data management, integration and collaboration in the cloud. Proceedings of the 1st ACM symposium on Cloud computing.
- Goyal S. Public vs private vs hybrid vs community-cloud computing: a critical review. *International Journal of Computer Network and Information Security*. 2014;6(3): pp.20-29.
- Grabski, S. V., et al. (2011). "A review of ERP research: A future agenda for accounting information systems." *Journal of information systems* 25(1): 37-78.
- Greene, S. S. *Security Program and Policies: Principles and Practices*. Pearson Education (2014).
- Griesser, G. (1978). Data security—a challenge to medical informatics, Taylor & Francis. 3: 71-75.
- Grobauer, B., T. Walloschek, and E. Stocker, *Understanding cloud computing vulnerabilities*. IEEE Security & Privacy, 2011. 9(2): p. 50-57.
- Grover, P. and A. K. Kar (2017). "Big data analytics: A review on theoretical contributions and tools used in literature." *Global Journal of Flexible Systems Management* 18: 203-229.



- Gul, I., et al. (2011). Cloud computing security auditing. The 2nd International Conference on Next Generation Information Technology, IEEE.
- Gundu, T. and S. Flowerday, *Ignorance to awareness: Towards an information security awareness process*. SAIEE Africa Research Journal, 2013. **104**(2): p. 69-79.
- Gunasekaran, Angappa, Eric WT Ngai, and Ronald E. McGAUGHEY. "Information technology and systems justification: A review for research and applications." *European Journal of Operational Research* 173.3 (2006): 957-983.
- Guo, Jingzhi, et al. "Document-oriented heterogeneous business process integration through collaborative e-marketplace." *Proceedings of the 10th international conference on Electronic commerce*. 2008. (pp. 1-10)
- Gupta, M. and A. Kohli (2006). "Enterprise resource planning systems and its implications for operations function." *Technovation* 26(5-6): 687-696.
- Gupta, P., A. Seetharaman, and J.R. Raj, *The usage and adoption of cloud computing by small and medium businesses*. *International Journal of Information Management*, 2013. **33**(5): p. 861-874.
- Gupta, S., et al. (2019). "Role of cloud ERP and big data on firm performance: a dynamic capability view theory perspective." *Management Decision* 57(8): 1857-1882.
- Gutiérrez, P. A., et al. (2015). "Ordinal regression methods: survey and experimental study." *IEEE Transactions on Knowledge and Data Engineering* 28(1): 127-146.
- Hababeh, I., et al., *An integrated methodology for big data classification and security for improving cloud systems data mobility*. *IEEE Access*, 2018. **7**: p. 9153-9163.
- Haddara, M., et al. (2022). "Challenges of cloud-ERP adoptions in SMEs." *Procedia Computer Science* 196: 973-981.

- Haddara, M. and T. Päivärinta (2011). Why benefits realization from ERP in SMEs doesn't seem to matter? 2011 44th Hawaii International Conference on System Sciences, IEEE.
- Hadlington, Lee. "The "human factor" in cybersecurity: Exploring the accidental insider." Research anthology on artificial intelligence applications in security. IGI Global, 2021. 1960-1977.
- Hajli, N., et al. (2017). "Branding co-creation with members of online brand communities." Journal of Business Research 70: 136-144.
- Halabi, T. and M. Bellaiche, *A broker-based framework for standardization and management of Cloud Security-SLAs*. Computers & Security, 2018. **75**: p. 59-71.
- Hallin, Daniel C., and Stylianos Papathanassopoulos. "Political clientelism and the media: Southern Europe and Latin America in comparative perspective." Media, Culture & Society 24.2 (2002): 175-195.
- Halpern, P., et al. (1980). "An economic analysis of limited liability in corporation law." U. Toronto LJ 30: 117.
- Hardwicke, T.E., et al., *Data availability, reusability, and analytic reproducibility: Evaluating the impact of a mandatory open data policy at the journal Cognition*. Royal Society Open Science, 2018. **5**(8): p. 180-448.
- Harfoushi, Osama, et al. "Data security issues and challenges in cloud computing: A conceptual analysis and review." Communications and Network 2014 (2014).
- Harrell, J., Frank E and F. E. Harrell (2015). "Ordinal logistic regression." Regression modeling strategies: with applications to linear models, logistic and ordinal regression, and survival analysis: 311-325.
- Harvey, W.S., *Strategies for conducting elite interviews*. Qualitative Research, 2011. **11**(4): p. 431-441.
- Hassan, Yusuf, et al. "Understanding talent management for sports organizations- Evidence from an emerging country." The International Journal of Human Resource Management. 33 (11) (2022): 2192-2225.

- Hauglid, J. O., et al. (2010). "DYFRAM: dynamic fragmentation and replica management in distributed database systems." *Distributed and Parallel Databases* 28(2-3): 157-185.
- Hayes, Bronwyn, Ann Bonner, and Clint Douglas. "An introduction to mixed methods research for nephrology nurses." *Renal Society of Australasia Journal* 9(1) (2013): 8-14.
- Hedeker, D. (2008). Multilevel models for ordinal and nominal variables. *Handbook of multilevel analysis*, Springer: 237-274.
- Helo, P. and Y. Hao (2022). "Artificial intelligence in operations management and supply chain management: An exploratory case study." *Production Planning & Control* 33(16): 1573-1590.
- Herath, Tejaswini, and H. Raghav Rao. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness." *Decision Support Systems* 47.2 (2009): 154-165.
- Herath, T. and H. R. Rao (2009). "Protection motivation and deterrence: a framework for security policy compliance in organisations." *European Journal of information systems* 18: 106-125.
- Hermann C. Structural adjustment and neoliberal convergence in labour markets and welfare: The impact of the crisis and austerity measures on European economic and social models. *Competition & Change*. 2014 Apr;18(2): pp.111-130. <https://doi.org/10.1179/1024529414Z.000000000051>
- Herring, S. C. (2010). "Computer-mediated conversation Part I: Introduction and overview." *Language@ internet* 7(2).
- Herzog, P., *Security, trust, and how we are broken*. Catalonia, Spain: ISECOM, 2010.
- Ho, R. (2013). *Handbook of univariate and multivariate data analysis with IBM SPSS*, CRC press.
- Höfer, C. and G. Karagiannis (2011). "Cloud computing services: taxonomy and comparison." *Journal of Internet Services and Applications* 2(2): 81-94.

- Hoffa, Christina, et al. "On the use of cloud computing for scientific workflows." 2008 *IEEE fourth international conference on eScience*. IEEE, 2008. (pp. 640-645).
- Hofstede, G. (2005). *Cultures and organisations: Software of the mind*. McGraw-Hill Publishing Co.
- Hofstede, Geert, Gert Jan Hofstede, and Michael Minkov. *Cultures and organizations: Software of the mind*. Vol. 2. New York: Mcgraw-hill, 2005.
- Houmansadr, A., et al. (2013). I want my voice to be heard: IP over Voice-over-IP for unobservable censorship circumvention. NDSS.
- Hrishev, R. (2020). ERP systems and data security. IOP Conference Series: Materials Science and Engineering, IOP Publishing.
- Hsieh, Y. C. (2017). "A case study of the dynamics of scaffolding among ESL learners and online resources in collaborative learning." *Computer Assisted Language Learning* 30(1-2): 115-132.
- Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*. 2012 Aug; 43(4): pp.615-660.
- Huang, Q., et al. (2021). Understanding Cloud-based ERP Customization from Key Stakeholders' Perspectives: a Research Model. ECIS.
- Hudic, A., et al. (2013). "Data confidentiality using fragmentation in cloud computing." *International Journal of Pervasive Computing and Communications* 9(1): 37-51.
- Hughes-Lartey, Kwesi, et al. "Human factor, a critical weak point in the information security of an organization's Internet of things." *Heliyon* 7(3) (2021): e06522.
- Hung, M., et al. (2017). "Interpretation of correlations in clinical research." *Postgraduate medicine* 129(8): 902-906.
- Hussey, J. & Hussey, R. (1997). *Business research: a practical guide for undergraduate and postgraduate students*. Basingstoke: Macmillan.

- Hustad, E., et al. (2020). "Moving enterprise resource planning (ERP) systems to the cloud: The challenge of infrastructural embeddedness." *International journal of information systems and project management* 8(1): 5-20.
- Ifinedo, P., et al. (2019). Factors that influence workers' participation in unhygienic cyber practices: A initial study from Nigeria. *International Conference on Social Implications of Computers in Developing Countries*, Springer.
- Iivari, J. and R. Hirschheim, *Analyzing information systems development: A comparison and analysis of eight IS development approaches*. *Information Systems*, 1996. **21**(7): p. 551-575.
- Iluore, O. E., et al. (2020). "Development of asset management model using real-time equipment monitoring (RTEM): case study of an industrial company." *Cogent Business & Management* 7(1): 1763649.
- Imene, F. and J. Imhanzenobe (2020). "Information technology and the accountant today: What has really changed?" *Journal of Accounting and Taxation* 12(1): 48-60.
- Indu I, Anand PR, Bhaskar V. Identity and Access Management in Cloud environment: Mechanisms and Challenges. *Engineering Science and Technology, an International Journal*. 2018 Aug 1;21(4):574-588.
- Inuwa, H. (2022). Industry 4.0 Implementation Challenges in the Nigerian Oil and Gas Industry: An Interpretive Structural Modeling Approach. *SPE Nigeria Annual International Conference and Exhibition*, SPE.
- Ion, I., Sachdeva, N., Kumaraguru, P. and Čapkun, S. Home is safer than the cloud! Privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*. *Association for Computing Machinery, New York, NY, USA, 2011 July 20, Article 13, 1–20*. <https://doi.org/10.1145/2078827.2078845>
- Islam, M. A., et al. (2018). "Basic Summary Statistics." *Foundations of Biostatistics*: 39-72.

- Ismail, U. M. and S. Islam (2020). "A unified framework for cloud security transparency and audit." *Journal of Information Security and Applications* 54: 102594.
- Ismail W.B and Yusof M. Mitigation strategies for unintentional insider threats on information leaks. *International Journal of Security and Its Applications*. 2018 Jan 1;12(1): pp.37-46.
- Iureva, R., et al. *Information security of Smart Factories*. in *Journal of Physics: Conference Series*. 2018. IOP Publishing.
- Jaatun, M. G., et al. (2020). "Enhancing accountability in the cloud." *International Journal of Information Management* 53: 101498.
- Jacobsen, D. I. (2002). *Vad, hur och varför: Om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen*. Studentlitteratur, Lund Sverige.
- Jacobs, F. Robert. "Enterprise resource planning (ERP)—A brief history." *Journal of Operations Management*, 25(2) (2007): 357-363.
- Jangjou, Mehrdad, and Mohammad Karim Sohrabi. "A comprehensive survey on security challenges in different network layers in cloud computing." *Archives of Computational Methods in Engineering* (2022): 1-22.
- Janiesch, C., et al. (2021). "Machine learning and deep learning." *Electronic Markets* 31(3): 685-695.
- Jansen, Wayne A., and Tim Grance. "Guidelines on security and privacy in public cloud computing." NIST Special Publication 800-144 (2011).
- Janulevičius, Justinas, et al. "Enterprise architecture modeling based on cloud computing security ontology as a reference model." *2017 Open Conference of Electrical, Electronic and Information Sciences (eStream)*. IEEE, 2017. (pp. 1-6)
- James, M.L., Wotring, C.E. and Forrest, E.J. An exploratory study of the perceived benefits of electronic bulletin board use and their impact on other communication activities. *Journal of Broadcasting & Electronic Media*. 1995, 39(1), pp.30-50.

- Jayeola, O., et al. (2022). "The mediating and moderating effects of top management support on the cloud ERP implementation–financial performance relationship." *Sustainability* 14(9): 5688.
- Jha, Jatinder Kumar, and Manjari Singh. "Who cares about ethical practices at workplace? A taxonomy of employees' unethical conduct from top management perspective." *International Journal of Organizational Analysis* (2021).
- Jin, H., et al. (2018). "A framework with data-centric accountability and auditability for cloud storage." *The journal of supercomputing* 74(11): 5903-5926.
- Jing, Xue, and Zhang Jian-Jun. "A brief survey on the security model of cloud computing." *2010 ninth international symposium on distributed computing and applications to business, engineering and science*. IEEE, 2010. (pp. 475-478).
- Johansson, B., et al. (2015). Cloud ERP adoption opportunities and concerns: the role of organizational size. 2015 48th Hawaii international conference on system sciences, IEEE.
- Johanson, G. A., & Brooks, G. P. (2010). Initial scale development: sample size for initial studies. *Educational and Psychological Measurement*, 70(3), 394-400.
- Johansson, Björn, et al. "Cloud ERP adoption opportunities and concerns: a comparison between SMES and large companies." *Pre-ECIS 2014 Workshop "IT Operations Management"(ITOM2014)*. 2014. (pp. 1-13)
- Johnson, R. A. and G. K. Bhattacharyya (2019). *Statistics: principles and methods*, John Wiley & Sons.
- Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, 33(7), 14-26.
- Johnson, R. D., et al. (2016). "The evolution of the field of human resource information systems: Co-evolution of technology and HR processes." *Communications of the Association for Information Systems* 38(1): 28.

- JPC Rodrigues, J., et al. (2013). "Analysis of the security and privacy requirements of cloud-based electronic health records systems." *Journal of medical Internet research* 15(8): e186.
- Jun Han, Rongbi Liu, Brandon Swanner and Shicheng Yang. "Enterprise resource planning." *Japansk produksjonsfilosofi, Toyota Production* (2010).
- Kabay, M., et al., *Using social psychology to implement security policies*. Computer security handbook, 2012: p. 50.1-25.
- Kabanda, Salah, and Seapei Nozimbali Mogoane. "A Conceptual Framework for Exploring the Factors Influencing Information Security Policy Compliance in Emerging Economies." *International Conference on e-Infrastructure and e-Services for Developing Countries*. Springer, Cham, 2022. (pp. 203-218).
- Kambatla, K., et al. (2014). "Trends in big data analytics." *Journal of parallel and distributed computing* 74(7): 2561-2573.
- Kaplan, Bonnie, and Dennis Duchon. "Combining qualitative and quantitative methods in information systems research: a case study." *MIS Quarterly* (1988): 12(4), pp. 571-586.
- Karadsheh, L. (2012). "Applying security policies and service level agreement to IaaS service model to enhance security and transition." *Computers & Security* 31(3): 315-326.
- Karimanzira, D. and T. Rauschenbach (2019). "Enhancing aquaponics management with IoT-based Predictive Analytics for efficient information utilization." *Information Processing in Agriculture* 6(3): 375-385.
- Karimi-Ghartemani, Samaneh, Naser Khani, and Ali Nasr Isfahani. "A qualitative analysis and a conceptual model for organizational stupidity." *Journal of Organizational Change Management* (2022). 35(3), pp. 441-462
- Katuu, S. (2020). "Enterprise resource planning: past, present, and future." *New Review of Information Networking* 25(1): 37-46.



- Kaur, B. and S. Sharma, *Parametric analysis of various cloud computing security models*. International Journal of Information and Computation Technology, ISSN, 2014: p. 0974-2239.
- Kaushik, Vibha, and Christine A. Walsh. Pragmatism as a Research Paradigm and Its Implications for Social Work Research. *Social Sciences* 2019. 8(9): pp.255. <https://doi.org/10.3390/socsci8090255>
- Kearns, G.S. and R. Sabherwal, *Strategic Alignment between Business and Information Technology: A knowledge based view of behaviours, outcome and consequences*. Journal of Management Information Systems, 2007. **23**(3): p. 129-162.
- Keatinge, R. R., et al. (1995). "Limited Liability Partnerships: The Next Step in the Evolution of the Unincorporated Business Organization." *The Business Lawyer*: 147-207.
- Kemper, G., *Improving employees' cyber security awareness*. Computer Fraud & Security, 2019. **2019**(8): p. 11-14.
- Khalil, M. H. M. "ERP Implementation in Large Organizations and its Challenges."
- Khan, S. U. and N. Ullah (2016). "Challenges in the adoption of hybrid cloud: an exploratory study using systematic literature review." *The Journal of Engineering* 2016(5): 107-118.
- Khando, K., et al. (2021). "Enhancing employees information security awareness in private and public organisations: A systematic literature review." *Computers & Security* 16: 102267.
- Kiran, T. and A. Reddy (2019). "Critical success factors of ERP implementation in SMEs." *Journal of Project Management* 4(4): 267-280.
- Klapper, L., et al. (2010). *Entrepreneurship and firm formation across countries. International differences in entrepreneurship*, University of Chicago Press: 129-158.
- Kline, R. R. (2015). *The cybernetics moment: Or why we call our age the information age*, JHU Press.

- Ključnikov, Aleksandr, Ladislav Mura, and David Sklenár. "Information security management in SMEs: factors of success." *Entrepreneurship and Sustainability Issues* 6 (4) (2019): 2081.
- Ko, R. K., et al. (2011). TrustCloud: A framework for accountability and trust in cloud computing. 2011 IEEE World Congress on Services, IEEE.
- Ko, R. K., et al. (2011). Towards achieving accountability, auditability and trust in cloud computing. *Advances in Computing and Communications: First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part IV 1*, Springer.
- Kong, Xiaoxi, and Zhanchuan Cai. "An Information Security Method Based on Optimized High-Fidelity Reversible Data Hiding." *IEEE Transactions on Industrial Informatics* (2022). 18(12), pp. 8529-8539.
- Kowalski, P., et al. (2013). "State-owned enterprises: Trade effects and policy implications."
- Kraemer, S.B., *An adversarial viewpoint of human and organizational factors in computer and information security*. 2006: University of Wisconsin at Madison. Madison ProQuest Dissertations Publishing, 2006. 3234846
- Kristiansen, Renate. "Tailoring of ERP user interfaces using a model-based approach." (2013). URL: <http://www.idi.ntnu.no/~renatek/ThesisProposal>
- Kritikos, K., et al. (2019). "A survey on vulnerability assessment tools and databases for cloud-based web applications." *Array* 3: 100011.
- Kshetri, N., *Cloud computing in developing economies*. *Computer*, 2010. **43**(10): p. 47-55.
- Kumar, M. R. and R. Sankar (2008). "An application for ordinal logistic (proportional odds) regression model using SPSS." *ResearchGate*,(January): 1-18.
- Kumar, M. S. (1985). "Growth, acquisition activity and firm size: evidence from the United Kingdom." *The Journal of Industrial Economics* 33(3): 327-338.
- Kumar, R. and Bhatia, M. P. S. A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability. In *2020 IEEE*

*International Conference on Computing, Power and Communication Technologies(GUCON)*, 2020, pp.334-337, doi: 10.1109/GUCON48875.2020.9231255.

Kumar, R. and R. Goyal (2020). "Modeling continuous security: A conceptual model for automated DevSecOps using open-source software over cloud (ADOC)." *Computers & Security* 97: 101967.

Kumar, R. and R. Goyal (2019). "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey." *Computer Science Review* 33: 1-48

Kumar, R. and R. Goyal (2019). "Assurance of data security and privacy in the cloud: A three-dimensional perspective." *Software Quality Professional* 21(2): 7-26.

Kumari, M. and R. Nath, *Data Security Model in Cloud Computing Environment*, in *Cyber Security*. 2018, Springer. p. 91-100.

Kunduru, A. R. "Industry Best Practices on Implementing Oracle Cloud ERP Security." *International Journal of Computer Trends and Technology* 71(6): 1-8.

Kuranga, A., et al. (2021). Critical Implementation Factors for Cloud-Based Enterprise Resources planning in the Nigerian Maritime Transport and Supply Chain. IOP Conference Series: Materials Science and Engineering, IOP Publishing.

Kurbel, K. E. and K. E. Kurbel (2013). "MRP II: Manufacturing Resource Planning." *Enterprise Resource Planning and Supply Chain Management: Functions, Business Processes and Software for Manufacturing Companies*: 61-93.

Lacey, David. *Managing the Human Factor in Information Security: How to win over staff and influence business managers*. John Wiley & Sons, 2009.

Lane, M., A. Shrestha, and O. Ali, *Managing the risks of data security and privacy in the cloud: a shared responsibility between the cloud service provider and the client organisation*. 2017.

- Lansing, J. and Sunyaev, A. Trust in cloud computing: Conceptual typology and trust-building antecedents. *ACM sigmis database: The database for advances in Information Systems*. 2016, 47(2), pp.58-96.
- Lee, M. J., et al. (2017). Next era of enterprise resource planning system review on traditional on-premise ERP versus cloud-based ERP: Factors influence decision on migration to cloud-based ERP for Malaysian SMEs/SMIs. 2017 IEEE Conference on Systems, Process and Control (ICSPC), IEEE.
- Lee, Nigel G. Fielding Raymond M. *Using computers in qualitative research*. 1991, (pp. 1-13). London: Sage
- Lee, S. M., et al. (2009). "Open process and open-source enterprise systems." *Enterprise Information Systems* 3(2): 201-209.
- Leedy, P. & Ormrod, J. *Practical research: Planning and design* (7th ed.). Upper Saddle River, NJ: Merrill Prentice Hall. Thousand Oaks: SAGE Publications (2001).
- Leidner, D. E. and J. J. Elam (1995). "The impact of executive information systems on organizational design, intelligence, and decision making." *Organization Science* 6(6): 645-664.
- Li, W., et al. (2008). "The choice of statistical models in road safety countermeasure effectiveness studies in Iowa." *Accident Analysis & Prevention* 40(4): 1531-1542.
- Li, X., J. Chen, and M. Luo. *A simple security model based on cloud reference model*. in *2011 10th International Symposium on Distributed Computing and Applications to Business, Engineering and Science*. 2011. IEEE.
- Liu, Feng, Weiping Guo, Zhi Qiang Zhao, and Wu Chou. "SaaS integration for software cloud." In *2010 IEEE 3rd International Conference on Cloud Computing*, pp. 402-409. IEEE, 2010.
- Liu, J.-L., et al. (2019). "Development of a cloud-based advanced planning and scheduling system for automotive parts manufacturing industry." *Procedia Manufacturing* 38: 1532-1539.

- Liu, Lan, and Xin Gao. "Effect mechanism of senior manger incentive and enterprise performance under vertical dyad linkage characteristics differences." *International Conference on Computer Application and Information Security (ICCAIS 2021)*. Vol. 12260. pp. 591-598, SPIE, 2022.
- Llave, M. R. (2017). "Business intelligence and analytics in small and medium-sized enterprises: A systematic literature review." *Procedia Computer Science* 121: 194-205.
- Locke, Edwin A. "Job satisfaction and job performance: A theoretical analysis." *Organizational behavior and human performance* 5 (5) (1970): 484-500.
- Lockyer, S. (2006). "Heard the one about... applying mixed methods in humour research?" *International Journal of Social Research Methodology* 9(1): 41-59.
- López, C. and A. Ishizaka (2017). "GAHPSort: A new group multi-criteria decision method for sorting a large number of the cloud-based ERP solutions." *Computers in Industry* 92: 12-25.
- Lukings, M. and A. Habibi Lashkari (2022). *Data Sovereignty. Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective*, Springer: 1-38.
- Luna-Reyes, L. F. and D. L. Andersen (2003). "Collecting and analyzing qualitative data for system dynamics: methods and models." *System Dynamics Review: The Journal of the System Dynamics Society* 19(4): 271-296.
- Luo, Xin, et al. "Social engineering: The neglected human factor for information security management." *Information Resources Management Journal (IRMJ)* 24.3 (2011): 1-8.
- Mabert, V. A., et al. (2001). "Enterprise resource planning: common myths versus evolving reality." *Business Horizons* 44(3): 69-69.
- Madni, A. M. and M. Sievers (2014). "Systems integration: Key perspectives, experiences, and challenges." *Systems Engineering* 17(1): 37-51.

- Mahmoud, R., et al. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. 2015 10th international conference for internet technology and secured transactions (ICITST), IEEE.
- Mailland, J. and K. Driscoll (2017). Minitel: Welcome to the internet, MIT Press.
- Malik, M. I., et al. (2018). "CLOUD COMPUTING-TECHNOLOGIES." International Journal of Advanced Research in Computer Science 9(2).
- Mallo, S. N. and F. N. Ogwueleka (2019). "Impacts and Challenges of Cloud Computing for Small and Medium Scale Businesses in Nigeria." Journal of Advances in Computer Engineering and Technology 5(3): 169-180.
- Mares, I. and Carnes, M.E. Social policy in developing countries. *Annual review of political science*. 2009, vol 12, p.93.
- Marinos, Alexandros, and Gerard Briscoe. "Community cloud computing." *IEEE international conference on cloud computing*. Springer, Berlin, Heidelberg, 2009. (pp. 472-484).
- Markus, M. Lynne, and Cornelis Tanis. "The enterprise systems experience-from adoption to success." *Framing the domains of IT research: Glimpsing the future through the past* 173.2000 (2000): 207-173.
- Marston, S., et al., *Cloud computing—The business perspective*. Decision Support Systems, 2011. **51**(1): p. 176-189.
- Martynov, A., Ensuring data security in enterprise networks. Language in the field of professional communication.—Yekaterinburg, 2020, 2020: p. 561-565.
- Mather, T., S. Kumaraswamy, and S. Latif, *Cloud security and privacy: an enterprise perspective on risks and compliance*. 2009: O'Reilly Media, Inc.
- Matrix, S. (2014). "The Netflix effect: Teens, binge watching, and on-demand digital media trends." *Jeunesse: young people, texts, cultures* 6(1): 119-138.
- Mayoral Pérez-Campos E, Fisher R, Anne Langer A, Lorenzo Pérez-Campos E, Pérez-Campos Mayoral L, Hernandez-Huerta MT, Matias-Cervantes CA. Leading Interview and Interrogation Techniques. Focus on Cognitive Interview. *European Polygraph*. 2022;16(1 (55)):45-63.

- McDaniel, M.A., F.L. Schmidt, and J.E. Hunter, *Job experience correlates of job performance*. *Journal of Applied Psychology*, 1988. **73**(2): p. 327.
- McLeod, Alexander, and Diane Dolezel. "Information security policy non-compliance: Can capitulation theory explain user behaviors?." *Computers & Security* 112 (2022): 102526.
- Melara, M. S., et al. (2015). {CONIKS}: Bringing key transparency to end users. 24<sup>th</sup> USENIX Security Symposium (USENIX Security 15).
- Mell, P. and T. Grance (2009). "Effectively and securely using the cloud computing paradigm." *NIST, Information Technology Laboratory* 2(8): 304-311.
- Mell, P. and T. Grance, *The NIST definition of cloud computing*. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930 September 2011
- Mell, P.M. and T. Grance, *Sp 800-145. the nist definition of cloud computing*. 2011. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930 September 2011.
- Merriam, S. B. and R. S. Grenier (2019). *Qualitative research in practice: Examples for discussion and analysis*, John Wiley & Sons.
- Metalidou E, Marinagi C, Trivellas P, Eberhagen N, Skourlas C, Giannakopoulos G. The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*. 2014 Aug 25;147:424-8.
- Mezgár, I. and U. Rauschecker (2014). "The challenge of networked enterprises for cloud computing interoperability." *Computers in Industry* 65(4): 657-674.
- Miles, M. B., & Huberman, A. M. *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Thousand Oaks, CA: Sage. chniques. Focus on Cognitive Interview. *European Polygraph*, (1994). 16(1), pp.45-63.
- Millet, I. and C. H. Mawhinney (1992). "Executive information systems: a critical perspective." *Information & Management* 23(2): 83-92.

- Mircea, Marinela. "Addressing data security in the cloud." *International Journal of Information and Communication Engineering* 6.6 (2012): 798-805.
- Mitropoulos, S., et al. (2006). "On Incident Handling and Response: A state-of-the-art approach." *Computers & Security* 25(5): 351-370.
- MJ, M. J., Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. (2021). "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews." 372: n71. Retrieved 01/082023, 2023, from <http://www.prisma-statement.org/>.
- Modi, C., et al., *A survey on security issues and solutions at different layers of Cloud computing*. The Journal of Supercomputing, 2013. **63**(2): p. 561-592.
- Mohabbatalab, E., et al. (2014). "The perceived advantages of cloud computing for SMEs." *GSTF Journal on Computing* 4(1): 61-65.
- Mohammed, A. S., et al. (2022). "Cybersecurity challenges in the offshore oil and gas industry: an Industrial Cyber-Physical Systems (ICPS) perspective." *ACM Transactions on Cyber-Physical Systems (TCPS)* 6(3): 1-27.
- Mohamed EM, Abdelkader HS, El-Etriby S. Enhanced data security model for cloud computing. In 2012 8th International Conference on Informatics and Systems (INFOS) 2012 May 14 (pp. CC-12). IEEE.
- Mohamed, E.M., H.S. Abdelkader, and S. El-Etriby, *Data security model for cloud computing*. Journal of Communication and Computer, 2013. **10**(08): p. 1047-1062.
- Mohammed, G., et al. (2023). "An Empirical Study on the Affecting Factors of Cloud-based ERP System Adoption in Iraqi SMEs." *International Journal of Advanced Computer Science and Applications* 14(1).
- Mohlameane, M.J. and Ruxwana, N.L. The potential of cloud computing as an alternative technology for SMEs in South Africa. *Journal of Economics, Business and Management*. 2013, 1(4), pp.396-400.
- Monk, E. and B. Wagner (2012). *Concepts in enterprise resource planning*, Cengage Learning.



- Morawiec, P. and A. Sołtysik-Piorunkiewicz (2022). "Cloud computing, big data, and blockchain technology adoption in ERP implementation methodology." *Sustainability* 14(7): 3714.
- Moreno-Vozmediano, R., et al. (2012). "IaaS cloud architecture: From virtualized datacenters to federated cloud infrastructures." *Computer* 45(12): 65-72.
- Morozan, I., *Multi-clouds database: A new model to provide security in cloud computing*. online) <https://www.researchgate.net/publication/273136522> (accessed on Apr. 1, 2015), 2014. Vrije Universiteit Amsterdam, The Netherlands.
- Mortazavi-Alavi, R., *A risk-driven investment model for analysing human factors in information security*. 2016, Doctoral dissertation, University of East London.
- Moussetis, R. and T. Cavenagh (2021). "Strategic, Legal, and Accounting Challenges for Social Enterprises." *JBM*: 23.
- Mungoli, N. (2023). "Scalable, Distributed AI Frameworks: Leveraging Cloud Computing for Enhanced Deep Learning Performance and Efficiency." arXiv preprint arXiv:2304.13738.
- Myers Michael David., and Avison, David E. "Qualitative research in information systems: a reader." *Qualitative Research in Information Systems* (2002): 1-312.
- Nandakumar, K., et al. (2021). "Securing data in transit using data-in-transit defender architecture for cloud communication." *Soft Computing* 25(18): 12343-12356.
- Nasim, R., et al. (2020). "A cloud-based enterprise resource planning architecture for women's education in remote areas." *Electronics* 9(11): 1758.
- National Research Council CO. *Computers at risk: Safe computing in the information age*. National Academy Press; 1991 Jan 1.
- Ndulue, Theresa.I. Impact of training and development on workers performance in an organization. In *Book of Proceedings, Proceedings of International Congress on Business and Economic Research (ICBER2012)*, International Association for Teaching and Learning, Granada. 2012, September (Vol. 1, pp. 135-148).

- Nednur, A. *The 5 Key Characteristics of Cloud Computing*. BlackBoard 2018. Cited 11-02-2019; Available from: <https://www.udemy.com/implementing-microsoft-azure-infrastructure-solutions-70533/?couponCode=LEARNIT>.
- Newman, M. and D. Gough (2020). "Systematic reviews in educational research: Methodology, perspectives and application." *Systematic reviews in educational research: Methodology, perspectives and application*: 3-22.
- Ng, K. K., et al. (2021). "A systematic literature review on intelligent automation: Aligning concepts from theory, practice, and future perspectives." *Advanced Engineering Informatics* 47: 101246.
- Ng'ethe, N. (1989). "In search of NGOs: towards a funding strategy to create NGO research capacity."
- Nguyen, H. and H. Doan (2020). "Driving change management strategy in ERP implementation project."
- Ni, Q., Lobo, J., Calo, S., Rohatgi, P. and Bertino, E. Automating role-based provisioning by learning from examples. In *Proceedings of the 14th ACM symposium on Access control models and technologies*. 2009 Jun 3 (pp. 75-84). <https://doi.org/10.1145/1542207.1542222>.
- Nick, J.M., Cohen, D. and Kaliski, B.S. Key enabling technologies for virtual private clouds. In *Handbook of Cloud Computing*. 2010 (pp. 47-63). Springer, Boston, MA. [https://doi.org/10.1007/978-1-4419-6524-0\\_3](https://doi.org/10.1007/978-1-4419-6524-0_3)
- Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, Bonacina S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*. 2021 Jul 28;21(15):5119.
- Niranjanamurthy, M., et al. (2013). "Analysis of e-commerce and m-commerce: advantages, limitations and security issues." *International Journal of Advanced Research in Computer and Communication Engineering* 2(6): 2360-2370.
- Niu, N., et al. (2013). "Enterprise information systems architecture—Analysis and evaluation." *IEEE transactions on industrial informatics* 9(4): 2147-2154.

- Nofal, M. I. and Z. M. Yusof (2013). "Integration of business intelligence and enterprise resource planning within organizations." *Procedia technology* 11: 658-665.
- Noraziah, A., et al. (2021). "BVAGQ-AR for Fragmented Database Replication Management." *IEEE Access* 9: 56168-56177.
- Nurse, J. R., et al. (2014). Understanding insider threat: A framework for characterising attacks. 2014 IEEE security and privacy workshops, IEEE.
- Nuss, M., et al. (2018). Towards blockchain-based identity and access management for internet of things in enterprises. Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings 15, Springer.
- Ogunsola, L. and W. Aboyade (2005). "Information and communication technology in Nigeria: Revolution or evolution." *Journal of Social Sciences* 11(1): 7-14.
- Okardi, B. and O. Asagba (2021). "Overview of distributed database system." *International Journal of Computer Techniques* 8(1): 83-100.
- Okeke, A. (2021). "Towards sustainability in the global oil and gas industry: Identifying where the emphasis lies." *Environmental and Sustainability Indicators* 12: 100145.
- Okoye Francis, A., et al. (2014). "Cloud Computing in Nigeria: Prospects, Challenges, and Operation Framework." *International Journal of Engineering Research & Technology (IJERT)* 3(6): 2107-2113.
- Olt, Christian M. "Information Security and Privacy in a Digital World: A Human Challenge." (2022). Ph.D. Thesis, Darmstadt, Technische Universitat, DOI: 10.26083/tuprints-00021138
- Olson, I., Abrams, Marshall D., Sushil G. Jajodia, and Harold J. Podell, eds. *Information security: an integrated collection of essays*. IEEE computer society press, 1995.
- O'Malley, G., Marseille, E. and Weaver, M.R. Cost-effectiveness analyses of training: a manager's guide. *Human Resources for Health*. 2013, 11(1), pp.1-9.

- Omar, L. S. (2019). "Using Ordinal Logistic Regression Analysis in Evaluating Teachers' Performance Level of High Schools (12th grades) in Kurdistan Regional Government." *Journal of University of Raparin* 6(2): 57-77.
- Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. *Sensors*. 2022 Jan 25;22(3):927.
- Oni, S., et al. (2019). E-government and the challenge of cybercrime in Nigeria. 2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG), IEEE.
- Onwuegbuzie, A.J. and R.B. Johnson, *The validity issue in mixed research*. Research in the Schools, 2006. **13**(1): p. 48-63.
- Onwuegbuzie, Anthony J., and Nancy L. Leech. "On becoming a pragmatic researcher: The importance of combining quantitative and qualitative research methodologies." *International journal of social research methodology* 8(5), (2005): 375-387.
- Oreščanin, D. and T. Hlupić (2021). Data lakehouse-a novel step in analytics architecture. 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), IEEE.
- Orosz I, A. Selmeçi and T. Orosz, "Software as a Service operation model in cloud-based ERP systems," *2019 IEEE 17th World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 2019, pp. 345-354, doi: 10.1109/SAMI.2019.8782739.
- Osborne, J.W., *Best practices in quantitative methods*. 2008: Sage.
- Osborne, Jason W. *Best practices in data cleaning: A complete guide to everything you need to do before and after collecting your data*. Sage, 2013.
- Otero, A.R. *Information Technology Control and Audit, Fifth Edition (5th ed.)*. Auerbach Publications (2018). <https://doi.org/10.1201/9780429465000>
- Ott, R. Lyman, and Micheal T. Longnecker. *An introduction to statistical methods and data analysis*. Cengage Learning, 2015.

- Otuonye, A. I. (2021). "CLOUD-BASED ENTERPRISE RESOURCE PLANNING FOR SUSTAINABLE GROWTH OF SMES IN THIRD WORLD COUNTRIES." *International Journal of Computer Science and Information Security (IJCSIS)* 19(5).
- Ozili, P. K. (2021). "Covid-19 pandemic and economic crisis: The Nigerian experience and structural causes." *Journal of Economic and Administrative Sciences* 37(4): 401-418.
- Özsu, M. T. and P. Valduriez (1999). *Principles of distributed database systems*, Springer.
- Panchal, S. and Cartwright, S. Group differences in post-merger stress. *Journal of Managerial Psychology*. (2001), 16(6), pp. 424-433. <https://doi.org/10.1108/02683940110402398>
- Panetto, H. (2007). "Towards a classification framework for interoperability of enterprise applications." *International Journal of Computer Integrated Manufacturing* 20(8): 727-740.
- Pandita, D. and Ray, S. Talent management and employee engagement – a meta-analysis of their impact on talent retention. *Industrial and Commercial Training*. (2018), 50(4), pp. 185-199. <https://doi.org/10.1108/ICT-09-2017-0073>
- Parker, D., *Security motivation, the mother of all controls, must precede awareness*. *Computer Security Journal*, 1999. **15**: p. 15-24.
- Parkin, S.E., A. van Moorsel, and R. Coles. *An information security ontology incorporating human-behavioural implications*. in *Proceedings of the 2nd International Conference on Security of Information and Networks*. 2009.
- Parmar, H. and A. Gosai (2015). "Analysis and study of network security at transport layer." *International Journal of Computer Applications* 121(13): 21604-24716.
- Pasquale, F. and T. A. Ragone (2013). "Protecting health privacy in an era of big data processing and cloud computing." *Stan. Tech. L. Rev.* 17: 595.
- Pasquier, T., et al. (2018). "Data provenance to audit compliance with privacy policy in the Internet of Things." *Personal and Ubiquitous Computing* 22: 333-344.

- Patel, H.B. and Kansara, N. Cloud Computing Deployment Models: A Comparative Study. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*. 2021 Mar 23. Available at SSRN: <https://ssrn.com/abstract=3832832>
- Patel, S. (2015). The research paradigm – methodology, epistemology and ontology – explained in simple language. Available at: "<http://salmapatel.co.uk/academia/the-research-paradigm-methodologyepistemology-and-ontology-explained-in-simple-language>"
- Paul, P.K., Karn, B. and Rajesh, R. Cloud computing and its deployment model: A short review. *International Journal of Applied Science and Engineering*. 2015, 3(1), p.29
- Paulk, Mark C., Bill Curtis, and Mary B. Chrissis. *Capability maturity model for software*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 1991.
- Pearlin LI, Menaghan EG, Lieberman MA, Mullan JT. The stress process. *Journal of Health and Social behavior*. 1981 Dec 1: pp. 337-56.
- Pearson, A., et al. (2015). "A mixed-methods approach to systematic reviews." *JBIEvidence Implementation* 13(3): 121-131.
- Pearson S. Privacy, Security and Trust in Cloud Computing. In: Pearson, S., Yee, G. (eds) *Privacy and Security for Cloud Computing*. Computer Communications and Networks. 2013 (pp. 3-42). Springer, London. [https://doi.org/10.1007/978-1-4471-4189-1\\_1](https://doi.org/10.1007/978-1-4471-4189-1_1)
- Peeters, J. (2009). "Early MRP Systems at Royal Philips Electronics in the 1960s and 1970s,". in *IEEE Annals of the History of Computing*. 31: 56-69.
- Peppers, K., et al. (2007). "A design science research methodology for information systems research." *Journal of management information systems* 24(3): 45-77.
- Pei, A.Q., M. Yang, and Y.B. Tang. *The Research Based on Security Model and Cloud Computing Strategy*. in *Advanced Materials Research*. 2014. Trans Tech Publ.

- Peirce, Charles Sanders, Nathan Houser, and Christian JW Kloesel. "How to make our ideas clear." *Charles S. Peirce: The Essential Writings* (1986): 137-57.
- Pekane, A. and M. Tanner. *A Systematic Literature Review on Cloud Computing and Small Medium Enterprises (SMEs) in Africa*. in *The European Conference on Information Systems Management*. 2017. Academic Conferences International Limited.
- Pollini A, Callari TC, Tedeschi A, Ruscio D, Save L, Chiarugi F, Guerri D. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*. 2022 May;24(2):371-90.
- Pollini, A., et al. (2022). "Leveraging human factors in cybersecurity: an integrated methodological approach." *Cognition, Technology & Work* 24(2): 371-390.
- Posthumus, R. *Data logging and monitoring for real-time systems*. 2007 (Master's thesis, University of Twente).
- Powell, R.R., *Evaluation research: An overview*. *Library Trends*, 2006. **55**(1): p. 102-120.
- Power, D. J. (2002). *Decision support systems: concepts and resources for managers*, Quorum Books.
- Prasad, S. (2023). *Correlation and Regression. Elementary Statistical Methods*, Springer: 241-279.
- Princewell, A.N. Church commercialization in Nigeria: Implications for public relations practice. *Journal of Philosophy, Culture and Religion*. 2017, 28(1), pp.1-11.
- Purohit, B. and P. P. Singh (2013). "Data leakage analysis on cloud computing." *International Journal of Engineering Research and Applications* 3(3): 1311-1316.
- Puth, M.-T., et al. (2015). "Effective use of Spearman's and Kendall's correlation coefficients for association between two measured traits." *Animal Behaviour* 102: 77-84.

- Putra, A.P.G., Humani, F., Zakiy, F.W., Shihab, M.R. and Ranti, B., 2020, October. Maturity Assessment of Cyber Security in The Workforce Management Domain: A Case Study in Bank Indonesia. In *2020 International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. 89-94). IEEE.
- Qadir, Suhail, and S. M. K. Quadri. Information availability: An insight into the most important attribute of information security. *Journal of Information Security* 7(3) (2016): 185-194.
- Qi, Q., et al. (2018). Modeling of cyber-physical systems and digital twin based on edge computing, fog computing and cloud computing towards smart manufacturing. *International Manufacturing Science and Engineering Conference*, American Society of Mechanical Engineers.
- Qian, J., et al. (2001). ACLA: A framework for access control list (ACL) analysis and optimization. *Communications and Multimedia Security Issues of the New Century: IFIP TC6/TC11 Fifth Joint Working Conference on Communications and Multimedia Security (CMS'01)* May 21–22, 2001, Darmstadt, Germany, Springer.
- Qiu MM, Zhou Y, Wang C. Systematic analysis of public cloud service level agreements and related business values. In *2013 IEEE International Conference on Services Computing 2013 Jun 28* (pp. 729-736). IEEE.
- Raczyńska, M. Definition of micro, small and medium enterprise under the guidelines of the European Union. *Review of Economic and Business Studies*. Alexandru Ioan Cuza University, Faculty of Economics and Business Administration 2019, (24), pp.165-190.
- Rai, Rashmi, G. Sahoo, and Shabana Mehruz. Securing software as a service model of cloud computing: Issues and solutions. In *2013 International Journal on Cloud Computing: Services and Architecture (IJCCSA)* ,Vol.3, No.4, August 2013. DOI : 10.5121/ijccsa.2013.3401.
- Rajaeian, M.M., Cater-Steel, A. and Lane, M. A systematic literature review and critical assessment of model-driven decision support for IT outsourcing. *Decision Support Systems*. 2017, vol 102, pp.42-56.



- Rajan, C. A. and R. Baral (2015). "Adoption of ERP system: An empirical study of factors influencing the usage of ERP and its impact on end user." *IIMB Management Review* 27(2): 105-117.
- Rani, D. and R. K. Ranjan (2014). "A comparative study of SaaS, PaaS and IaaS in cloud computing." *International Journal of Advanced Research in Computer Science and Software Engineering* 4(6).
- Rantos, K., K. Fysarakis, and C. Manifavas, *How effective is your security awareness program? An evaluation methodology*. *Information Security Journal: A Global Perspective*, 2012. 21(6): p. 328-345.
- Rao, T. R., et al. (2019). "The big data system, components, tools, and technologies: a survey." *Knowledge and Information Systems* 60: 1165-1245.
- Rasheed, H. (2014). "Data and infrastructure security auditing in cloud computing environments." *International Journal of Information Management* 34(3): 364-368.
- Rashid, M.A., L. Hossain, and J.D. Patrick, *The evolution of ERP systems: A historical perspective*, in *Enterprise resource planning: Solutions and management*. 2002, IGI global. p. 35-50.
- Ray, E.B. and Miller, K.I. The influence of communication structure and social support on job stress and burnout. *Management Communication Quarterly*. 1991, 4(4), pp.506-527.
- Raza, M.H., Adenola, A.F., Nafarieh, A. and Robertson, W., 2015. The slow adoption of cloud computing and IT workforce. *Procedia Computer Science*, 52, pp.1114-1119.
- Razzaq, A., et al. (2013). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), IEEE.
- Reason, J., & Hobbs, A. (2003). *Managing Maintenance Error: A Practical Guide* (1st ed.). CRC Press. <https://doi.org/10.1201/9781315249926>

- Rebollo, O., Mellado, D., Fernández-Medina, E. and Mouratidis, H. Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*. 2015, 58, pp.44-57.
- Richings D. Rethinking endpoint management for the modern age. *Network Security*. 2022 Oct;2022(10).
- Romero, D. and F. Vernadat (2016). "Enterprise information systems state of the art: Past, present and future trends." *Computers in Industry* 79: 3-13.
- Rose, K., et al. (2015). "The internet of things: An overview." *The internet society (ISOC)* 80: 1-50.
- Rossman GB, Wilson BL. Numbers and words: Combining quantitative and qualitative methods in a single large-scale evaluation study. *Evaluation review*. 1985 Oct; 9(5):627-43.
- Rowsell-Jones, A. and B. Gomolski, *Executive Summary: Optimizing IT Assets: Is Cloud Computing the Answer*. Gartner Research. ID, 2011(G00211420).
- Rozenberg, Y. (2012). "Challenges in PII data protection." *Computer Fraud & Security* 2012(6): 5-9.
- Rubin, Herbert J., and Irene S. Rubin. *Qualitative interviewing: The art of hearing data*. sage, 2011.
- Rudner, M. (2013). "Cyber-threats to critical national infrastructure: An intelligence challenge." *International Journal of Intelligence and CounterIntelligence* 26(3): 453-481.
- Ruparelia, N. B. (2010). "Software development lifecycle models." *ACM SIGSOFT Software Engineering Notes* 35(3): 8-13.
- Saa P, Moscoso-Zea O, Costales AC, Luján-Mora S. Data security issues in cloud-based Software-as-a-Service ERP. In 2017 12th Iberian Conference on Information Systems and Technologies (CISTI) 2017 Jun 21 (pp. 1-7). IEEE. doi: 10.23919/CISTI.2017.7975779.

- Saa, P., Costales, A.C., Moscoso-Zea, O. and Lujan-Mora, S. (2017). Moving ERP Systems to the Cloud - Data Security Issues. *Journal of Information Systems Engineering & Management*, 2(4), 21. <https://doi.org/10.20897/jisem.201721>
- Saeed, I., et al. (2012). "Cloud enterprise resource planning adoption: Motives & barriers." *Advances in Enterprise Information Systems II* 429.
- Saidu, A., *Security Threats and Challenges in Cloud Computing Application. International Journal of Computer Science and Mathematical Theory*. 5 (2) (2019), pp. 46-55.
- Saigushev, N., et al. *Information Systems at Enterprise. Design of Secure Network of Enterprise*. in *Journal of Physics: Conference Series*. 2018. IOP Publishing.
- Saini, I., et al. (2014). Cloud and traditional ERP systems in small and medium enterprises. 2014 International Conference on Information Systems and Computer Networks (ISCON), IEEE.
- Saks, M. and J. Allsop, *Researching health: Qualitative, quantitative and mixed methods*. 2012: Sage.
- Salim, S. A., et al. (2015). "Moving from evaluation to trial: How do SMEs start adopting cloud ERP?" *Australasian Journal of Information Systems* 19.
- Sarathy, V., et al. (2010). Next generation cloud computing architecture: Enabling real-time dynamism for shared distributed physical infrastructure. 2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises, IEEE.
- Saripalli, P. and B. Walters. *Quirc: A quantitative impact and risk assessment framework for cloud security*. in *2010 IEEE 3rd international conference on cloud computing*. 2010. IEEE.
- Saritha, Lingam, and K. Salivahana Reddy. "A Project On Secure Cloud Storing And Sharing Of Big Data Using Data Chunks." *Journal Of Resource Management And Technology* (2020), 11 (3), , p.378-383.

- Sarkar, K.R., *Assessing insider threats to information security using technical, behavioural and organisational measures*. Information Security Technical Report, 2010. **15**(3): p. 112-133.
- Saunders, M., Lewis, P. and Thornhill, A., 1997. *Research Methods for Business Students* (Pitman, London).
- Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (5th Eds) Essex: Pearson Education Ltd.
- Saunders, M.N.K. and Tosey, P.C., 2013. The layers of research design. *Rapport*, (Winter), pp.58-59.
- Schaffer H. E, S. F. Averitt, M. I. Hoit, A. Peeler, E. D. Sills and M. A. Vouk. NCSU's Virtual Computing Lab: A Cloud Computing Solution. In *Computer*, vol. 42, no. 7, pp. 94-97, July 2009, doi: 10.1109/MC.2009.230.
- Schein, E. (1992). *Organisational Culture and Leadership* (2nd edn). San Francisco, CA: Jossey-Bass Publishers.
- Schraagen, J.M. and van de Ven, J. Human factors aspects of ICT for crisis management. *Cognition, Technology & Work*. 2011, 13(3), pp.175-187.
- Sears, R. and C. van Ingen (2006). "Fragmentation in large object repositories." arXiv preprint cs/0612111.
- Seethamraju, R. (2015). "Adoption of software as a service (SaaS) enterprise resource planning (ERP) systems in small and medium sized enterprises (SMEs)." *Information systems frontiers* 17: 475-492.
- Seethamraju, R. and D. K. Sundar (2013). "Influence of ERP systems on business process agility." *IIMB Management Review* 25(3): 137-149.
- Sehgal, N. K., et al. (2020). "Cloud computing with security." *Concepts and practices*. Second edition. Switzerland: Springer.
- Sen, J., *Security and privacy issues in cloud computing*, in *Architectures and protocols for secure information technology infrastructures*. 2014, IGI Global. p. 1-45.

- Sengupta, S. and K. Annervaz (2014). "Multi-site data distribution for disaster recovery—A planning framework." *Future Generation computer systems* 41: 53-64.
- Sengupta, S., et al. (2011). *Cloud computing security--trends and research directions*. 2011 IEEE World Congress on Services, IEEE.
- Shaheen S, Abrar M, Saleem S, Shabbir R, Zulfiqar S.. Linking organizational cronyism to deviant workplace behavior: Testing the mediating role of employee negligence in Pakistani higher education institutions. *International Journal of Leadership in Education* (2021): 1-23.
- Shahid, M.A. and M. Sharif, *Cloud computing security models, architectures, issues and challenges: A survey*. SmartCR, 2015. 5(6): p. 602-616.
- Shahraki, A., et al. (2022). "A comparative study on online machine learning techniques for network traffic streams analysis." *Computer Networks* 207: 108836.
- Shaikh, R. and M. Sasikumar (2015). "Data classification for achieving security in cloud computing." *Procedia Computer Science* 45: 493-498.
- Shang, S. and P. B. Seddon (2002). "Assessing and managing the benefits of enterprise systems: the business manager's perspective." *Information systems journal* 12(4): 271-299.
- Sharma, D. H., et al. (2016). "Identity and access management as security-as-a-service from clouds." *Procedia Computer Science* 79: 170-174.
- Sharma, P.K., et al. *Issues and challenges of data security in a cloud computing environment*. in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*. 2017. IEEE.
- Shatat, A. S. and A. S. Shatat (2021). "Cloud-based ERP systems implementation: major challenges and critical success factors." *Journal of Information & Knowledge Management* 20(03): 2150034.
- Shaw, B. (2021). "UK businesses broken down by legal status, industry, region, employment and turnover size bands." *UK business; activity, size and location*:

2021. Retrieved 30/09/2023, 2023, from <https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/bulletins/ukbusinessactivitysizeandlocation/2021>.

Shawish, A. and M. Salama (2013). Cloud computing: paradigms and technologies. Inter-cooperative collective intelligence: Techniques and applications, Springer: 39-67.

She, W. and B. Thuraisingham (2007). "Security for enterprise resource planning systems." *Information Systems Security* 16(3): 152-163.

Shokrollahi Yancheshmeh, A. Multi-Tenancy Security in Cloud Computing: Edge Computing and Distributed Cloud. School of Electrical Engineering and Computer Science (EECS). Independent thesis Advanced level (degree of Master) 2019. DiVA, id: diva2:1412847.

Shoniwa, T. R. (2021). Developing a framework for adoption of cloud computing by small medium enterprises in Zimbabwe.

Shuttleworth, M. (2008). Quantitative and Quantitative Research Design. Available Online at: [HYPERLINK https://explorable.com/quantitative-research-design](https://explorable.com/quantitative-research-design).

Silverman, D. (2010). *Doing qualitative research: a practical handbook* (3rd ed.). Thousand Oaks, CA: Sage Publications Ltd.

Simmon, E. Evaluation of Cloud Computing Services based on NIST SP 800-145. *NIST Special Publication 500-322*. (2018).

Singh, S., et al. (2016). "A survey on cloud computing security: Issues, threats, and solutions." *Journal of Network and Computer Applications* 75: 200-222.

Smith, Andrew R., John M. Colombi, and Joseph R. Wirthlin. "Rapid development: A content analysis comparison of literature and purposive sampling of rapid reaction projects." *Procedia Computer Science* 16 (2013): 475-482.

Smith, A., Bhogal, J. and Sharma, M. August. Cloud computing: adoption considerations for business and education. In *2014 International Conference on Future Internet of Things and Cloud*. 2014 (pp. 302-307). IEEE. doi: 10.1109/FiCloud.2014.54.

- Snedaker, S., 2013. Business continuity and disaster recovery planning for IT professionals. Newnes.
- Snedaker S. Business continuity and disaster recovery planning for IT professionals. Newnes; 2013 Sep 10. Newnes, 2013, ISBN 0124114512, 9780124114517
- Sofaer, S., *Qualitative methods: what are they and why use them?* Health Services Research, 1999. **34**(5 Pt 2): p. 1101.
- Sokol, A.W. and M.D. Hogan. NIST Cloud Computing Standards Roadmap Version 2. NIST Cloud Computing Standards Roadmap Working Group. In NIST Special Publications 500–291 2013 (pp. 1-113). NIST.
- Sokol, A. and Hogan, M. (2013), NIST Cloud Computing Standards Roadmap, Special Publication 500–291 2013 (pp. 1-113), National Institute of Standards and Technology, Gaithersburg, MD, [online], <https://doi.org/10.6028/NIST.SP.500-291r2> (Accessed December 7, 2022)
- Solove, D. J. (2004). The digital person: Technology and privacy in the information age, NyU Press.
- Spencer-Oatey H, Franklin P. What is culture. A compilation of quotations. GlobalPAD Core Concepts. 2012;1:22.
- Spring, J., *Monitoring cloud computing by layer, part 1*. IEEE Security & Privacy, 2011. **9**(2): p. 66-68.
- Sreemathy, J., et al. (2021). Overview of etl tools and talend-data integration. 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE.
- Stake, R. E. (2010). "Qualitative research: Studying how things work."
- Stavrou, V., et al. *Business Process Modeling for Insider threat monitoring and handling*. in *International Conference on Trust, Privacy and Security in Digital Business*. 2014. Springer.
- Stake, R.E. (1994) Case Studies. In: Denzin, N.K. and Lincoln, Y.S., Eds., Handbook of Qualitative Research, Sage, Thousand Oaks, 236-247.

- Stepanov, L., et al. Approach to estimation of level of information security at enterprise based on genetic algorithm. in *Journal of Physics: Conference Series*. 2018. IOP Publishing.
- Stephanou, M. and M. Varughese (2021). "Sequential estimation of Spearman rank correlation using Hermite series estimators." *Journal of Multivariate Analysis* 186: 104783.
- Stuckenberg, Sebastian; Fielt, Erwin; and Loser, Timm. The Impact Of Software-As-A-Service On Business Models Of Leading Software Vendors: Experiences From Three Exploratory Case Studies (2011). *PACIS 2011 Proceedings*. 184. <https://aisel.aisnet.org/pacis2011/184>.
- Subashini, S. and V. Kavitha (2011). "A survey on security issues in service delivery models of cloud computing." *Journal of Network and Computer Applications* 34(1): 1-11.
- Subramanian, N. and A. Jeyaraj, *Recent security challenges in cloud computing*. Computers & Electrical Engineering, 2018. **71**: p. 28-42.
- Sun, Y., Gong, B., Meng, X., Lin, Z. and Bertino, E., 2009. Specification and enforcement of flexible security policy for active cooperation. *Information Sciences*, 179(15), pp.2629-2642.
- Su, Y.-f. and C. Yang (2010). "Why are enterprise resource planning systems indispensable to supply chain management?" *European Journal of Operational Research* 203(1): 81-94.
- Sundareswaran, S., et al. (2012). "Ensuring distributed accountability for data sharing in the cloud." *IEEE transactions on dependable and secure computing* 9(4): 556-568.
- Surbiryala, J. and C. Rong (2019). *Cloud computing: History and overview*. 2019 IEEE Cloud Summit, IEEE.
- Suthaharan, S. (2016). "Machine learning models and algorithms for big data classification." *Integr. Ser. Inf. Syst* 36: 1-12.



- Sveiby, K.E., *The new organizational wealth: Managing & measuring knowledge-based assets*. 1997: Berrett-Koehler Publishers.
- Tabrizchi, H. and M. Kuchaki Rafsanjani (2020). "A survey on security challenges in cloud computing: issues, threats, and solutions." *The journal of supercomputing* 76(12): 9493-9532.
- Tahboub, R. and Y. Saleh (2014). Data leakage/loss prevention systems (DLP). 2014 World Congress on Computer Applications and Information Systems (WCCAIS), IEEE.
- Tahmid, M. (2020). "Accounting in the Cloud: A New Era of Streamlining Accounting with Cloud Technology." ID: 1902018. Department of Education, Bangabandhu Sheikh Mujibur Rahman Digital University, Bangladesh. 1902018@icte.bdu.ac.bd. researchgate.net
- Takabi, H., J.B. Joshi, and G.-J. Ahn, *Security and privacy challenges in cloud computing environments*. IEEE Security & Privacy, 2010. **8**(6): p. 24-31.
- Tambare, P., et al. (2021). "Performance measurement system and quality management in data-driven Industry 4.0: A review." *Sensors* 22(1): 224.
- Tang, B., R. Sandhu, and Q. Li, *Multi-tenancy authorization models for collaborative cloud services*. *Concurrency and Computation: Practice and Experience*, 2015. **27**(11): p. 2851-2868.
- Tashakkori, Abbas, Charles Teddlie, and Charles B. Teddlie. *Mixed methodology: Combining qualitative and quantitative approaches*. Vol. 46. sage, 1998.
- Taylor, A. (2021). "Standing by for data loss: Failure, preparedness and the cloud." *ephemera: theory & politics in organization* 21(1).
- Taymaz, E. Are Small Firms Really Less Productive?. *Small Bus Econ*, 2005. 25, 429–445. <https://doi.org/10.1007/s11187-004-6492-x>
- Thitme, S. and V. K. Verma (2016). "A recent study of various encryption and decryption techniques." *International Research Journal of Advanced Engineering and Science* 1(3): 92-94.
- Thomas, S. A. (2000). *SSL & TLs Essentials*, United States of America.

- Thunnissen, M. Talent management: For what, how and how well? An empirical exploration of talent management in practice. *Employee Relations*, 2016, 38(1), pp. 57-72. <https://doi.org/10.1108/ER-08-2015-0159>
- Tob-Ogu, A., et al. (2018). "ICT adoption in road freight transport in Nigeria—A case study of the petroleum downstream sector." *Technological Forecasting and Social Change* 131: 240-252.
- Tongsuksai, S., et al. (2023). "Influential characteristics and benefits of cloud ERP adoption in New Zealand SMEs: a vendors' perspective." *IEEE Access* 11: 23956-23979.
- Trček, D., et al., *Information systems security and human behaviour*. Behaviour & Information Technology, 2007. **26**(2): p. 113-118.
- Trost J, Lee CP, Gibbs N, Beyah R, Copeland JA. Visual firewall: real-time network security monitor. In *IEEE Workshop on Visualization for Computer Security*, 2005.(VizSEC 05). 2005 Oct 26 (pp. 129-136). IEEE.
- Tsai, W.-T., Q. Shao, and J. Elston. *Prioritizing service requests on cloud with multi-tenancy*. in *7th International Conference on E-Business Engineering*. 2010. IEEE.
- Tulinayo, F. P., et al. (2018). "Digital technologies in resource constrained higher institutions of learning: a study on students' acceptance and usability." *International Journal of Educational Technology in Higher Education* 15(1): 1-19.
- Uchenna, C. P., et al. (2015). "Overcoming the barriers to enterprise cloud adoption within Nigerian consumer constituency." *British Journal of Mathematics & Computer Science* 8(1): 39-56.
- Ukwandu, E., et al. (2023). *Assessing Cyber-Security Readiness of Nigeria to Industry 4.0*. Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales, Springer.

- Undheim, A., A. Chilwan, and P. Heegaard. *Differentiated availability in cloud computing slas*. in *Proceedings of the 2011 IEEE/ACM 12th International Conference on Grid Computing*. 2011. IEEE Computer Society.
- Unger, J.M., Rauch, A., Frese, M. and Rosenbusch, N. Human capital and entrepreneurial success: A meta-analytical review. *Journal of Business Venturing*. 2011, 26(3), pp.341-358.
- Usman, U. M. Z., et al. (2019). "The determinants of adoption of cloud-based ERP of Nigerian's SMEs manufacturing sector using TOE framework and DOI theory." *International Journal of Enterprise Information Systems (IJEIS)* 15(3): 27-43.
- Utting, P. (2005). "Corporate responsibility and the movement of business." *Development in practice* 15(3-4): 375-388.
- Valavala, M. and W. Alhamdani (2020). "A Survey on Database Index Tuning and Defragmentation." *International Journal of Engineering Research & Technology* 9(12): 317-321.
- Valentine, J.A., *Enhancing the employee security awareness model*. *Computer Fraud & Security*, 2006. **2006**(6): p. 17-19.
- Van der Molen, F. (1970). *Get ready for cloud computing*, Van Haren Publishing, 2010.p.5-8
- Van Niekerk, B. and P. Jacobs (2013). *Cloud-based security mechanisms for critical information infrastructure protection*. 2013 *International Conference on Adaptive Science and Technology*, IEEE.
- Varshney, S., et al. (2020). *Big data privacy breach prevention strategies*. 2020 *IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, IEEE.
- Vasiljeva, T., S. Shaikhulina, and K. Kreslins, *Cloud computing: business perspectives, benefits and challenges for small and medium enterprises (case of Latvia)*. *Procedia Engineering*, 2017. **178**: p. 443-451.

- Venkatraman, S. and K. Fahd (2016). "Challenges and success factors of ERP systems in Australian SMEs." *Systems* 4(2): 20.
- Verma, J. and A.-S. G. Abdel-Salam (2019). *Testing statistical assumptions in research*, John Wiley & Sons.
- Vis, B., Van Kersbergen, K. and Hylands, T. To what extent did the financial crisis intensify the pressure to reform the welfare state?. *Social Policy & Administration*. 2011, 45(4), pp.338-353. <https://doi.org/10.1111/j.1467-9515.2011.00778.x>.
- Vorakulpipat C, Sirapaisan S, Rattanalerdnusorn E, Savangasuk V. A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. *Security and Communication Networks*. 2017 Jan 1;2017.
- Vroom, C. and R. Von Solms, *Towards information security behavioural compliance*. *Computers & security*, 2004. **23**(3): p. 191-198.
- Waddock, S. A. (1988). "Building successful social partnerships." *MIT Sloan Management Review* 29(4): 17.
- Wall, David S., *Crime, Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing* (July 20, 2017). Available at SSRN: <http://dx.doi.org/10.2139/ssrn.3005872>
- Wanasinghe, T. R., et al. (2020). "The internet of things in the oil and gas industry: a systematic review." *IEEE Internet of Things Journal* 7(9): 8654-8673.
- Wanasinghe, T. R., et al. (2021). "Human centric digital transformation and operator 4.0 for the oil and gas industry." *IEEE Access* 9: 113270-113291.
- Wang, H., *Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-health Record*. *IEEE Access*, 2018.
- Wang, Q., et al. (2010). "Enabling public auditability and data dynamics for storage security in cloud computing." *IEEE transactions on parallel and distributed systems* 22(5): 847-859.

- Wankhade, M., et al. (2022). "A survey on sentiment analysis methods, applications, and challenges." *Artificial Intelligence Review* 55(7): 5731-5780.
- Warkentin, M. and Beranek, P.M. Training to improve virtual team communication. *Information Systems Journal*. 1999, 9(4), pp.271-289. <https://doi.org/10.1046/j.1365-2575.1999.00065.x>
- Wei, C.-C. (2008). "Evaluating the performance of an ERP system based on the knowledge of ERP implementation objectives." *The International Journal of Advanced Manufacturing Technology* 39: 168-181.
- Wei, Y. and M.B. Blake, *Service-oriented computing and cloud computing: Challenges and opportunities*. IEEE Internet Computing, 2010. 14(6): p. 72-75.
- Weir, G., et al. (2017). Cloud accounting systems, the audit trail, forensics and the EU GDPR: how hard can it be? British Accounting & Finance Association (BAFA) Annual Conference 2017.
- Weitzner, Daniel J., et al. "Information accountability." *Communications of the ACM* 51.6 (2008): 82-87.
- Weli W. Re-examination and expanding the EUCS Model on Cloud-based ERP system. *Journal of information and organizational sciences*. 2021 Jun 15;45(1):115-35.
- Weng, F. and M.-C. Hung (2014). "Competition and challenge on adopting cloud ERP." *International Journal of Innovation, Management and Technology* 5(4): 309.
- Werlinger, R., K. Hawkey, and K. Beznosov, *An integrated view of human, organizational, and technological challenges of IT security management*. *Information Management & Computer Security*, 2009. 17(1): p. 4-19.
- Wikipedia (2014). "Sony Pictures hack." Retrieved May 20, 2023, 2023, from [https://en.wikipedia.org/w/index.php?title=Sony\\_Pictures\\_hack&oldid=1154381581](https://en.wikipedia.org/w/index.php?title=Sony_Pictures_hack&oldid=1154381581).

- Williams, P. (2001). Information Security Governance. Information Security Technical Report, 6(3), 60-70.
- Williams, P. (2007). Information Governance: A Model for Security in Medical Practice. Journal of Digital Forensics, Security and Law. Vol 2(1): 57-73.
- Wilson, M. and J. Hash, *Building an information technology security awareness and training program*. NIST Special publication, 2003. **800**(50): p. 1-39.
- Winter Jr, R. K. (1977). "State law, shareholder protection, and the theory of the corporation." The Journal of Legal Studies 6(2): 251-292.
- Wood T, Shenoy P.J, Gerber A, van der Merwe J.E and Ramakrishnan K.K. The Case for Enterprise-Ready Virtual Private Clouds. In HotCloud 2009 Jun 14.
- Wu, D., et al. (2015). "Cloud-based design and manufacturing: A new paradigm in digital manufacturing and design innovation." Computer-aided design 59: 1-14.
- Wu, W.-W., *Mining significant factors affecting the adoption of SaaS using the rough set approach*. Journal of Systems and Software, 2011. **84**(3): p. 435-441.
- Xiaochao, Z., Y. Lihong, and P. Li. *An Alternative Approach to Confidentiality Analysis*. in *Computational Intelligence and Security, 2006 International Conference on*. 2006. IEEE.
- Xin Z, Song-qing L, Nai-wen L. Research on cloud computing data security model based on multi-dimension. In 2012 International Symposium on Information Technologies in Medicine and Education 2012 Aug 3 (Vol. 2, pp. 897-900). IEEE.
- Xue, C.T.S. and Xin, F.T.W. Benefits and challenges of the adoption of cloud computing in business. International Journal on Cloud Computing: Services and Architecture. 2016, 6(6), pp.01-15.
- Yassin, A.A., Jin, H., Ibrahim, A., Qiang, W., Zou, D. (2013). Cloud Authentication Based on Anonymous One-Time Password. In: Han, YH., Park, DS., Jia, W., Yeo, SS. (eds) Ubiquitous Information Technologies and Applications. Lecture

Notes in Electrical Engineering, (pp. 423-431). vol 214. Springer, Dordrecht.  
[https://doi.org/10.1007/978-94-007-5857-5\\_46](https://doi.org/10.1007/978-94-007-5857-5_46)

- Yeboah-Boateng, E. O. (2013). Cyber-security challenges with smes in developing economies: Issues of confidentiality, integrity & availability (CIA), Institut for Elektroniske Systemer, Aalborg Universitet.
- Younis, Y. A., et al. (2014). "An access control model for cloud computing." *Journal of Information Security and Applications* 19(1): 45-60.
- Yin R. K. (2014). *Case Study Research: Design and Methods*, 5th edition, Los Angeles, CA: Sage.
- Yu, S., et al. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. 2010 Proceedings IEEE INFOCOM, Ieee.
- Zacharewicz, G., et al. (2017). "Model-based approaches for interoperability of next generation enterprise information systems: state of the art and future challenges." *Information Systems and e-Business Management* 15: 229-256.
- Zeinab, K. A. M. and S. A. A. Elmustafa (2017). "Internet of things applications, challenges and related future technologies." *World Scientific News* 67(2): 126-148.
- Zhang, H., et al. (2015). "In-memory big data management and processing: A survey." *IEEE Transactions on Knowledge and Data Engineering* 27(7): 1920-1948.
- Zhang Y, Zhang C, Liu M. Effects of Top-Down, Bottom-Up, and Horizontal Communication on Organizational Commitment: Evidence from Chinese Internet Firms. *IEEE Transactions on Professional Communication*. 2022 Jun 24; 65(3): p.411-426.
- Zhang, Q., L. Cheng, and R. Boutaba, *Cloud computing: state-of-the-art and research challenges*. *Journal of Internet Services and Applications*, 2010. 1(1): p. 7-18.
- Zhou, M., et al. (2010). Services in the cloud computing era: A survey. 2010 4th International Universal Communication Symposium, IEEE.
- Zhu, L. and D. F. Spidal (2015). "Shared integrated library system migration from a technical services perspective." *Technical Services Quarterly* 32(3): 253-273.

Zissis, D. and D. Lekkas, *Addressing cloud computing security issues*. Future Generation Computer Systems, 2012. **28**(3): p. 583-592.

Zmud, R. W. (1980). "Management of large software development efforts." MIS quarterly: 45-55.



# Appendix

This session of the thesis gives a summary of other research activities that did not form the main content of the thesis but was an important exercise in our research and research findings. Here we talked about the Ethics documents used during data collection in Appendix 1. The Appendix 2 shows the initial study interviews questions and a sample of the initial study transcript. The Appendix 3 shows the main study survey questions draft and a sample of the main study transcript as generated from the Qualtrics software used. This session also shows the default main study report as generated from the Qualtrics before data cleaning and classification was done. The Appendix 4 shows the research communication exercises, show samples of paper, abstract, poster and research image publication. The Appendix 5 shows the initial study participating enterprise profile.

## 8.1. Appendix 1. Research Ethics documentation

### **Title of research:**

The impact of cloud computing on enterprise system security; *with emphasis on the role of the human factor in enhancing the enterprise system security.*

“An End-User Centred Framework for Data Access Management and Security in the Enterprise Public Cloud”

### **Summary of research (short overview of the background and aims of this study):**

This is a proposed series of interviews and surveys that is aimed to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. This study goal

is accomplished by analysing the present status of cloud computing security models. It also examines the essential human factor elements that influence the adoption of a cloud-based ERP systems in such organisations. To discover how the human factor affects the data security management process within the enterprise, especially with respect to cloud-based enterprise information systems and to validate the views of our proposed framework. The interviews will be conducted by a PhD researcher from the University of Strathclyde.

Enterprise systems give coordinated and summarized information to all the activities in an organization. These systems fill in as a key resource for any organization and as such, it is necessary to guarantee the security of the data in these systems. At the same time, innovation is vital for the application of modern-day computing technology. Considering the large sums that many organizations spend on computing systems and infrastructure, and the need to reduce these costs, this had led many organizations to consider implementation of a cloud-based solution. Cloud computing is becoming popular because of its benefits and its strongest point of reducing the computing cost for most enterprises. The small to medium enterprise would readily go for cloud solutions as this makes computing more affordable and highly scalable, giving enterprises the impression that they pay for only what they use and can always increase the size of the usage as the enterprise grows in their ventures. But there are major concerns about the adoption of cloud computing, which largely has to do with the security of data in the cloud.

The aim of this research is to investigate end-user security responsibility in ensuring enterprise data security in public cloud, in order to discover meaning and aid the formulation of explanations for deficiencies in the culture of information security inside SMEs organisations in Nigeria. To determine to what extent cloud computing poses a risk to the data security in the enterprise system; and the role of human factors (*where human factor here refers to the employee of an enterprise that is using cloud computing*) in ensuring a better enterprise data security in the Cloud. This research will help to propose a cloud computing data security management framework approach; for an enterprise that is or hoping to adopt cloud computing in the future; with the intention of understanding if the employees carried out their activities in a particular way, would it pose a risk or enhance the security of their data in the cloud?

### **How will participants be recruited?**

The participating enterprises will be recruited by officially inviting them via email and a hardcopy letter from the researcher; upon their acceptance to participate in the research, the company will give consent to the researcher. With this approval, individual employees of the participating enterprise will be contacted directly by speaking to them or we could work with the enterprise schedule to make their staff available for the research activity. We also hope to use social media platforms like LinkedIn to directly contact IT professionals across the globe to take part in the survey. We hope to recruit 2-3 enterprises and a minimum of 40 participants across the different enterprises.

**What will the participants be told about the proposed research study? Either upload or include a copy of the briefing notes issued to participants. In particular, this should include details of yourself, the context of the study and an overview of the data that you plan to collect, your supervisor, and contact details for the Departmental Ethics Committee.**

**PDF File:** [View the document](#)

Dear...Participant

You are invited to participate in research being conducted by Eya Nwanneka a PhD researcher at the University of Strathclyde. The research is on the impact of cloud computing on enterprise system security; *with emphasis on the role of human factor in enhancing the enterprise system security. (end-user security responsibility in ensuring enterprise data security in public cloud.)*

This information sheet describes the research to be undertaken. Please read this sheet carefully and be confident that you understand its contents before deciding whether

to participate or not. If you have any questions about the research, please ask the researcher.

Thank you for participating in this research activity. First, I would like to let you know that the interview will take about 30 minutes. I will give you a draft of the questions to read before we start. The interview will contain questions about the background information of the interviewee, awareness of security risks associated with cloud computing, data management policies in their enterprise, training policies in their enterprise, general knowledge of cloud computing, enterprise information systems and data management security models. You will be identified by the ID number (e.g. P01). Your name and other contact details will never be used in this research so you cannot be recognised from the interview data. The collected data from the interview will be used for research purposes only and will be stored and kept strictly confidential. An anonymised version of the data will be made available for research purposes only.

Thank you for participating in this Survey. I would like to let you know that survey will take about 10 minutes. The survey contains questions about the background information of the participant, awareness of security risks associated with cloud computing, cloud computing security models and end-user security responsibility in ensuring enterprise data security in public cloud. You will be identified by ID number (e.g. P01). Your name and other contact details will never be used in this research so that you cannot be recognised from the survey response. The collected data from the survey will be used for research purposes only and will be stored and kept strictly confidential. An anonymised version of the data will be made available for research purposes only. Click on this link to start

[https://qfreeaccountssjc1.az1.qualtrics.com/jfe/form/SV\\_71A1fZabkW8lk21](https://qfreeaccountssjc1.az1.qualtrics.com/jfe/form/SV_71A1fZabkW8lk21)

Though there are direct benefits to those participating in the study, this interview is also an opportunity for you to share insights on the best data management security model that could be adopted widely to improve the use of cloud computing in enterprise systems. The aim of this study is to learn more about the behaviour of staff

that could impact data management security in a Cloud environment. For the enterprises that participate in the research, upon their request a functional requirement document (FRD document) could be prepared for them which will give the company an insight into the As Is procedures in the company with respect to enterprise information systems. Your participation in this research is voluntary and you are free to withdraw at any time without giving a reason. I am happy to make the anonymised results available to anyone who takes part and wishes to see them. I will give you a consent form to read and sign.

To protect participants, the following steps will be taken with regards to anonymity and confidentiality of information:

- 1) The audio recording will be kept on my personal computer for transcription, and then will be deleted after the research has been completed. An interview transcript will be stored on the Strathclyde H drive and external hard drive to be analysed.
  - 2) Digital copies of interview data will be included in the University Knowledge Base. These copies will not contain any information which could possibly identify any participant.
  - 3) The consent form will be kept in my supervisor's office at the University of Strathclyde for five years. When this period is over, this form will be shredded.
- Please read the consent form carefully and be confident that you understand its contents before signing it. If you have any questions about the research, please feel free to contact the researcher or any of her supervisors.

Researcher

██████████

Computer and Information Sciences,

PhD Researcher

████████████████████

Primary Supervisor

██████████

Computer and Information Sciences

[REDACTED]

[REDACTED]

This study is approved by the Departmental Ethics Committee and if there are any concerns you should contact the Departmental Ethics Committee using

[REDACTED]

**How will consent be demonstrated? Either upload or include here a copy of the consent form/instructions issued to participants. It is particularly important that you make the rights of the participants to freely withdraw from the study at any point (if they begin to feel stressed for example), nor feel under any pressure or obligation to complete the study, answer any particular question, or undertake any particular task. Their rights regarding associated data collected should also be made explicit.**

**PDF File:** [View the document](#)

Consent Form for Interview

Researcher:

[REDACTED]

[REDACTED]

Department of Computer and Information Sciences.

Supervisors:

[REDACTED]

Department of Computer and Information Sciences.

[REDACTED]

Department of Computer and Information Sciences.

Title of the study: The impact of cloud computing on enterprise system security; *with emphasis on the role of human factor in enhancing the enterprise system security.*

*(end-user security responsibility in ensuring enterprise data security in public cloud,)*

By signing below, I confirm that I have read and understand the following points:

1. I confirm that I have read and understand the information sheet for the above study and have had the opportunity to ask any questions.
2. I understand that my permission is voluntary and that I am free to withdraw at any time, without giving any reason, without my legal rights being affected.
3. I consent to being a participant in the above study.
4. I consent for anonymised data gathered from this interview which does not contain my identity information to be made available for research purposes.

Name of Participant Date:

Signature of Participant

Name of Researcher Date:

Signature of Researcher

**What will participants be expected to do? Either upload or include a copy of the instructions issued to participants along with a copy of or link to the survey, interview script or task description you intend to carry out. Please also confirm (where appropriate) that your supervisor has seen and approved both your planned study, and this associated ethics application.**

I expect participants to answer all the interview/survey questions from their experience or give their opinions or withdraw from the interview any time.

I confirm that my supervisor has seen and approved both my planned study, and this associated ethics application.

**What data will be collected and how will it be captured and stored? In particular indicate how adherence to the Data Protection Act and the General Data Protection Regulation (GDPR) will be guaranteed and how participant confidentiality will be handled.**

The data that will be collected is the background information of the interviewee, their awareness level with respect to security risks associated with cloud computing, data management policies in their enterprise, training policies in their enterprise, general knowledge of cloud computing, enterprise information systems and data management security models. (Their behaviour, experience, knowledge, and attitudes towards cloud computing usage). The data will be captured as an audio recording for the interview and online data collection for the survey.

To protect participants, the following steps will be taken with regards to anonymity and confidentiality of information:

- 1) The audio recording will be kept on my personal computer for transcription, and then will be deleted after the research has been completed. An interview transcript will be stored on the Strathclyde H drive and external hard drive to be analysed.
- 2) Digital copies of interview data and survey data will be included in the University Knowledge Base. These copies will not contain any information which could possibly identify any participant.
- 3) The consent form will be kept in my supervisor's office at the University of Strathclyde for five years. When this period is over, this form will be shredded.

**How will the data be processed? (E.g., analysed, reported, visualised, integrated with other data, etc.) Please pay particular attention to describing how personal or sensitive data will be handled and how GDPR regulations will be met.**



Since the aim of this study is to investigate the end-user security responsibility in ensuring enterprise data security in public cloud, and to discover how identified human factors affect the data security management process within the enterprise especially with respect to cloud-based enterprise information system and validate the concepts of our proposed implementation framework. The results from the interview and survey (the mixed method approach) will be analysed to support and gain more insights on the best data management security model for a cloud-based enterprise information system. The obtained findings will thereafter be reported as part of my thesis. All processing will adhere to the Data Protection Act and no personal data that identifies individuals will be published.

**How and when will data be disposed of? Either upload a copy of your data management plan or describe how data will be disposed.**

**PDF File:** None.

The data will be destroyed comprehensively and securely when the researcher finishes her study.

1) The audio recording will be kept on my personal computer for transcription purpose only, and then will be deleted after the research has been completed. The interview transcript and survey data will be stored on the Strathclyde H drive and external hard drive to be analysed.

2) Digital copies of interview data and survey data will be included in the University Knowledge Base. These copies will not contain any information which could possibly identify any participant.

3) The consent form will be kept in my supervisor's office at the University of Strathclyde for five years. When this period is over, this form will be shredded.

Dear Sir/Madam,

My name is Eya Nwanneka and I am a PhD student from the Department of Computer and Information Sciences at the University of Strathclyde. I am currently conducting research on the impact of cloud computing on enterprise system security; with emphasis on the role of the human factor in enhancing the enterprise system security [REDACTED]

I am currently looking for participating enterprises. This involves allowing your employees to take part in an interview and online survey that address questions about background information of the interviewee, awareness of security risks associated with cloud computing, data management policies in the enterprise, training policies in their enterprise, general knowledge of cloud computing, enterprise information systems and data management security models. An interview will take about 30 minutes and all gathered data are kept confidential and used only for the purpose of this study. The study will take place at the enterprise premises at a time to be arranged to ensure that there is minimal impact upon normal working activities.

Individual participants will be eligible to enter a draw for a £10 Amazon voucher while the participating enterprise will be eligible to request a functional requirement documents of their current 'As Is' procedures with respect to the enterprise information system.

If you have any questions about the research, please feel free to contact the researcher or her supervisors.

Researcher	Supervisor
[REDACTED] Computer and Information Sciences, PhD student [REDACTED]	[REDACTED] Computer and Information Sciences [REDACTED]

This study is approved by the Departmental Ethics Committee and if there are any concerns you should contact the Departmental Ethics Committee using [REDACTED]  
Ethics approval no.: 836.

We do hope for a favourable response from you.

Kind Regards,  
[REDACTED]

-----  
PhD Student  
Department of Computer and Information Sciences University of Strathclyde, Glasgow, UK  
[REDACTED]

## **8.2. Appendix 2. Initial Study Interviews Questions and Initial Study Transcripts.**

### **A. Initial Study Interview Question and justification for each question.**

**Question 1:** What role do you play in the design and implementation of EIS in your organization? Technology, Risk Assessment, Business.

This question will help us establish how the participant role is related or critical to influencing the implementation of a cloud-based ERP system. This question will also help us to establish if the person's role is Technical, Risk Analysis or Business inclined. This question also will help us understand what influences the choice of a cloud-based ERP system based on their understanding.

**Question 2:** The training program in your enterprise, does it cover all the areas of EIS regulations? If Yes, can you give example of how it covers recognized threats in cloud computing?

This question is to establish the training gaps that exists within the enterprise, especially with respect to recognised treats of cloud computing. This question will help us to understand current or exiting EIS regulations; and how they are applying within the enterprise. This question can also give us some insights of recognised treats of cloud computing with the enterprise.

**Question 3a:** Do you have any EIS awareness programme in your organization and do you find them efficient and effective?

**Question 3b:** Does it response to your needs in dealing with cloud based EIS issues?

This question will help us determine if EIS awareness programmes will help mitigate against identified treats in cloud computing ERP. If it is established that this is positive; then it will help us have an elaborate example on the type of awareness programme that works best within a peculiar enterprise. A close look on how to incorporate Awareness programme when developing DMS model for a cloud-based ERP.

**Question 4:** How do you communicate DMS policies to ensure that employees understood, and the policy do not adversely affect the business.

This question will help us understand strategies organisations use in communicating DMS policies to ensure a great understanding by their employees. This question will also help us understand how the employees of an enterprise are involved in DMS policy implementation. Where possible, we are to determine the importance of this communication strategy and then implement in the DMS model we develop.

**Question 5a:** How would you describe your knowledge of a cloud-based ERP system?

**Question 5b:** How would you describe your enterprise data security in cloud, could you give an example?

This question will help us to establish the knowledge level for a cloud-based ERP system. Also how knowledgeable are the enterprise employees about data security in cloud. We also hope to use this question to gain an insight into the data security approaches in cloud-based ERP systems.

**Question 6:** Do you feel that you are encouraged to respond to DMS policies within the enterprise; or do you feel reluctant to implement them?

This question intends to associate how the employees perceive DMS policies within their enterprise with the success rate of such policies. It will identify factors like stress; human error etc. will influence an already existing DMS policy of an enterprise.

**Question 7:** Do you have any incentive policy in your organization to reward your engagement in adhering to DMS policies of a cloud-based ERP system?

This question is to establish how incentives can encourage employees to adhere to DMS policies and see how this improves data security of a cloud-based ERP system.

**Question 8:** What is the impact of a cloud-based ERP on your enterprise system data security?

This question intends to address our main research question. We hope that experts' participants will give us on insight on the perceived impacts of cloud-based ERP systems on their enterprise security. With the identified impacts in mind, we can shape our research on addressing the major impacts.

**Question 9:** Do you find it a difficult deciding to move your enterprise data to cloud?  
If yes, please can you elaborate?

This question will help us to justify the perceived concerns associated with adoption of cloud-based ERP system from the literature. Speaking to experts in the field is an opportunity to understand the general views about a cloud-based ERP system.

**Question 10:** How do you or your enterprise mitigate the risk associated with the use of a cloud-based ERP systems?

This question hopes to identify two things; the identified risks of a cloud-based ERP systems; and how enterprises manage these risks. This will help our research to focus on developing a model that will be impactful especially in addressing the commonly identified risks.

**Question 11:** What is the current DMS approach currently used in your enterprise?

This question will help us understand the various data management security (DMS) approaches within an enterprise; and its effectiveness with a cloud-based ERP system.

**Question 12a:** Do you feel that there are actions of employees that poses a risk to data security?

**Question 12b:** Is this applicable also in cloud data security in cloud?

This question will assist us to identify the critical attributes or actions of an employee that poses a risk to cloud based ERP systems. Our research can focus more on the main identified human factors from the interview result.

**Question 13a:** What skills do you look for in an employee, when considering data security in the cloud?

**Question 13b:** How would you say the IT skills of your employees influence or affect your data security?

This question will enable us to determine the importance of IT skills in ensuring data security in cloud. We may also gain an insight on how the skills are used within the enterprise.

**Question 14:** What is the number of staff currently work in your enterprise?

This question will help us to determine the category of the enterprise as either micro, small, medium, or large.

**Question 15:** Do you feel that adopting cloud-based ERP system, that your enterprise would loss the security control of your enterprises data.

This question will help us justify our point in the literature review, with the challenges of software as a service model is; service users feel they have loss the secured control of their data. Either this could be true or false, the findings will give us an insight on the real situations.

## **B. Initial Study Interview Transcript for just one Participant MTP02**

**Researcher:** Hello Ma, Good afternoon,

**Participant:** Yea good afternoon.

**R:** Yea it is my pleasure to meet you here today, thank you for agreeing to take part in this interview. So am just going to explain a little more about the research.

**P:** ok

**R:** This is research on the role of human factor and how it imparts cloud computing security especially an enterprise system that is based in cloud. So, I understand that you have a wide range of experience when it comes to ERP and enterprise systems and am quite happy to be speaking with you today. So please this is the participants information sheet, if you can go through it and if you are willing to go ahead with the interview then I can give you the consent form.

**P:** Alright, just give me few minutes let me go through it.

**R:** Alright that is fine

**P:** Ok that is fine, am alright

**R:** Alright that is the consent form then, if you can sign it, this is trying to explain how the data will be processed and what it will be used for.

**P:** ok

**R:** If you can sign it then that will be fine.

**P:** All right, my name, signature, and the dates, right?

**R:** yes yes.

**P:** All right, that is it.

**R:** All right thank you; I will just sign mine too. Thank you very much. All right, so now this is a copy of the interview questions so that you can have a scan through before we start. If there is any question you do not want to attend to just now, you can just point at it and we will just have to skip that question, but if you are confident to give answers to all the questions, then we can proceed immediately.

**P:** All right, I think I will try my best to answer all your questions. So, let us get cracking.

**R:** Ok that is fine Ma, thank you. Ok so am a PhD researcher from the University Strathclyde as you already know, this interview is about trying to discover the role of human factor in enterprise system security with respect to cloud computing, so there are few questions we just want to ask you, so now the first question is.

**R:** What role do you play in the design and implementation of EIS in your organization? Technology, Risk Assessment, Business.

**P:** I would consider my role to be business oriented.

**R 2:** The training program in your enterprise, does it cover all the areas of EIS regulations? If Yes, can you give example of how it covers recognized threats in cloud computing?

**P:** Well, we have some trainings, but I cannot say there is no room for improvement. Of course, there is room for improvement. I would say the training on introductory cyber security touches some aspect of staying safe online, which I do believe is part of cloud systems.

**R 3a:** Do you have any EIS awareness programme in your organization, and do you find them efficient and effective?

**P:** Yea we do have some couple of trainings in our company, although different groups or department get different at different times to serve their respective needs. But in general, I feel the trainings available serves our current need, although there is room for improvement.

**R 3b:** Does its response to your needs in dealing with cloud based EIS issues?

**P:** This I would not know much about as am not directly dealing with I.T issues or challenges of the company. My role is more focus on the business side of thing, selling machinery to clients.

**R 4:** How do you communicate DMS policies to ensure that employees understood, and the policy do not adversely affect the business.

**P:** I am not in the position to do that. But most communication within our company is done through emails.

**R 5a:** How would you describe your knowledge of a cloud-based ERP system?

**P:** I only know the basis, like that it exists and is an advancement to the traditional computing.

**R 5b:** How would you describe your enterprise data security in cloud, could you give an example?

**P:** I do not know much about this. I just believe we are safe that IT security guys are on top of their games.

**R 6:** Do you feel that you are encouraged to respond to DMS policies within the enterprise; or do you feel reluctant to implement them?

**P:** Well, I believe there still needs to be more done especially in terms of how the policies are communicated and spread. This will ensure a wider understanding of the policy.

**R 7:** Do you have any incentive policy in your organization to reward your engagement in adhering to DMS policies of a cloud-based ERP system?

**P:** None that am aware of.

**R 8:** What is the impact of a cloud-based ERP on your enterprise system data security?



**P:** Am not aware of any impact, maybe the ICT department may be more informed about the impact we might be facing right now as a company, if any.

**R 9:** Do you find it a difficult deciding to move your enterprise data to cloud? If yes, please can you elaborate?

**P:** It was not my decision, and I do not know much about that.

**R 10:** How do you or your enterprise mitigate the risk associated with the use of a cloud-based ERP systems?

**P:** Well, the last I checked, you were required to change to a new password quite frequently, like say every three to four months intervals.

**R 11:** What is the current DMS approach currently used in your enterprise?

**P:** We have quarterly departmental audits and annual company audits. The auditors check that all data files are correct.

**R 12a:** Do you feel that there are actions of employees that poses a risk to data security?

**P:** Yes of course

**R 12b:** Is this applicable also in cloud data security in cloud?

**P:** Yes maybe, but I believe the cloud guys should be able to manage their data security well.

**R 13a:** What skills do you look for in an employee, when considering data security in the cloud?

**P:** Am not in the HR but I guess they might want technical IT skills.

**R 13b:** How would you say the IT skills of your employees influence or affect your data security?

**P:** IT skills is everything, when you have the right skills, security would not be a major concern.

**R 14:** What is the number of staff currently work in your enterprise?

**P:** We have above eighty employee or colleagues of mine.

**R 15:** Do you feel that adopting cloud-based ERP system, that your enterprise would lose the security control of your enterprises data.

**P:** Is possible since you are outsourcing the data to another party. But if you are confident in the other party, why not. It is not an automatic loss if you trust the other party like your own employees.

### **8.3. Appendix 3. Main Study Survey Questions Draft and Main Study Transcript generated from Qualtrics software.**

#### **A. Main Study Survey first draft**

##### **Survey Questions and Justification. First Draft**

---

Q1 Is Data Security in Cloud a major concern when an Enterprise is adopting a Cloud-based ERP software system?

- Definitely a major concern (1)
- Probably a major concern (2)
- Might or might not be a major concern (3)
- Probably not a major concern (4)
- Definitely not a major concern (5)

**Reason:** This question will enable us to ascertain from our participants, if cloud data security is still a major concern when adopting a cloud-based ERP solution or not. If it is still a major concern, some of the current Cloud Security Models CSM are yet to fully address these security issues and there are major room for improvement.

Q2 Does Cloud Computing Technology have any impact on Enterprise Systems Data Security?

- Definitely have an impact (1)
- Probably have an impact (2)
- Might or might not have an impact (3)
- Probably have no impact (4)
- Definitely have no impact (5)

**Reason:** This question addresses one of our major research goals, to ascertain if the adoption of a cloud-based ERP solution by Enterprises has an impact on the Enterprise data security as a whole.

Q3 The security responsibility of a cloud system should be shared between the Cloud Service Provider [CSP] and the Cloud Service End-users. How do you agree with the above statement?

- Definitely Agree (1)
- Probably Agree (2)
- Might or might not Agree (3)
- Probably Disagree (4)
- Definitely Disagree (5)

**Reason:** Our new proposed framework proposes a shared security responsibility between the End-user enterprise and the Cloud Service Provider (CSP). This question will help us to understand if our participants agree or disagree with such division of security responsibilities.

Q4 In your opinion, is it okay to ensure that no single system end-user (for instance CEO or the System Administrator) to have access to all the Enterprise data set in the cloud storage at once?

- Definitely Okay (1)
- Probably Okay (2)
- Might or might not be Okay (3)
- Probably not Okay (4)
- Definitely not Okay (5)

**Reason:** The proposed framework ensured that through data fragmentation, no single end-user is able to have access to all the enterprise data set, thereby minimizing the level of data set exposure should there be a successful malicious insider attack or cyber-attack incident.

Q5 How important is an End-user role and responsibility, in the determining the level / type of system access given to them in their enterprise system?

- Extremely important (1)
- Very important (2)
- Moderately important (3)
- Slightly important (4)
- Not at all important (5)

**Reason:** Since our proposed framework considered the end-user role and responsibilities as a key factor in determining the level of access; we intend to use this question to affirm this position or disprove it.

Q6. Do you agree that, when a single system end-user have access to all the Enterprise data set in cloud, this may increase the Enterprise chances of having a successful cyber-attack?

- Definitely Agree (1)
- Probably Agree (2)
- Might or might not Agree (3)
- Probably Disagree (4)
- Definitely Disagree (5)

**Reason:** We intend to understand how our participants associates a successful cyber-attack incident with access level of the system end-users. This question will either affirm our position on end-user access level control or disprove it.

Q7 End-users of a cloud-based ERP software systems should hold some security responsibilities of ensuring the security of their Enterprise data in cloud. Do you agree with the above statement?

- Definitely Agree (1)

- Probably Agree (2)
- Might or Might not Agree (3)
- Probably Disagree (4)
- Definitely Disagree (5)

**Reason:** This question will verify our claim that end-users should have more involvement in the securing of their Enterprise data in a cloud-based ERP system.

Q8 How important is End-user Access Control in ensuring Enterprise data security in cloud?

- Extremely important (1)
- Very important (2)
- Moderately important (3)
- Slightly important (4)
- Not at all important (5)

**Reason:** This question enables us to determine how the participants agree the “Access Control” is a key feature in managing data security in cloud.

Q9 To manage the Access Control, cloud service providers keep a directory known as "CSP Access Directory"; this is a database of all the cloud end-users and their passwords which is used in validating each time an end-user is accessing data in cloud.

Do you agree that the "CSP Access Directory" would improve access control management in cloud?

- Definitely Agree (1)
- Probably Agree (2)
- Might or might not Agree (3)
- Probably Disagree (4)
- Definitely Disagree (5)

**Reason:** This question enables us to determine how the participants agree that "CSP Access Directory" improves access control in a cloud-based ERP system.

Q10 Enterprise data set classification; should happen as an integral process of the enterprise preparations to move the enterprise data to cloud.

Do you agree with the above statement?

- Definitely Agree (1)
- Probably Agree (2)
- Might or might not Agree (3)
- Probably Disagree (4)
- Definitely Disagree (5)

**Reason:** The proposed framework main feature is the Enterprise Access Directory (EAD) which is a form of data classification within the Enterprise before moving dataset to cloud. The Enterprise dataset is to be classified against key roles and responsibilities of their end-users, which will determine the level of access each end-user will have and the dataset they can access in cloud. The above question will help us determine

from our participants opinion the importance of such data classification before moving the enterprise data to cloud.

Q11 Enterprise Database Fragmentation is a feature of a cloud security model that suggests that cloud service providers should store the enterprise data set in fragments and implement access control for each fragment of the database.

Do you agree that Enterprise Database Fragmentation in cloud would improve enterprise data security of a cloud-based ERP software system.

- Definitely Agree (1)
- Probably Agree (2)
- Might or might not Agree (3)
- Probably Disagree (4)
- Definitely Disagree (5)

**Reason:** This question enables us to determine how the participants agree with the concept that, Enterprise Database Fragmentation in cloud, is a way of improving data security in cloud.

Q12 An Enterprise system that prompt the Enterprise System Administrator when there is an unsuccessful login attempt, is more likely to promote Enterprise data security in cloud.

Do you agree with the above statement?

- Definitely Agree (1)
- Probably Agree (2)
- Might or might not Agree (3)
- Probably Disagree (4)
- Definitely Disagree (5)



**Reason:** This question helps us to justify if End-user Access Queries will improve enterprise data security in cloud

Q13 The current cloud security model available in my Enterprise meets all our Enterprise needs for data security in cloud.

- Definitely Yes (1)
- Probably Yes (2)
- Neutral (3)
- Probably No (4)
- Definitely No (5)

**Reason:** This is to get our participants opinion on the need to improve current cloud security model or framework in their enterprise.

Q14 How many years have you worked in your current role?

- Few months up to 1 year (1)
- 2 years up to 4 years (2)
- 5 years up to 7 years (3)
- 8 years up to 10 years (4)
- 11 years and above (5)

**Reason:** This question will give us an idea on how experienced our participant is, the more experienced participants may have more valuable responses and can be contacted for further studies like an interview.

**B. End-user Access Control Model Survey used for data collection.**

Q1 How many years have you worked in your current role?

- Few months up to 1 year (1)
- 2 years up to 4 years (2)
- 5 years up to 7 years (3)
- 8 years up to 10 years (4)
- 11 years and above (5)

Q2 Do you currently work with a Cloud-based ERP system in your enterprise?

- Yes, we are using a Cloud-based ERP system (1)
- No, we are not using a Cloud-based ERP system (2)

Q3

Cloud Computing has an impact on Enterprise system data security. To what extent do you agree with the above statement?

- Definitely has an impact (1)
  - Probably has an impact (2)
  - Might or might not have an impact (3)
  - Probably has no impact (4)
  - Definitely has no impact (5)
  - Can you tell us in your words why you choose the option you did above (6)
-

Q4 The security responsibility for a Cloud system within an enterprise; should be a shared responsibility between the Cloud Service Provider [CSP] and the Cloud Service End-users. (Cloud Service End-user are the enterprise employees who uses the enterprise system to work.) To what extent do you agree with the above statement?

- Definitely Agree (1)
  - Probably Agree (2)
  - Might or might not Agree (3)
  - Probably Disagree (4)
  - Definitely Disagree (5)
  - Can you tell us in your words why you choose the option you did above (6)
- 

Q5 In your opinion, is it okay to ensure that no single system end-user (including the CEO and the System Administrator) has access to all the Enterprise data set in the Cloud storage?

- Definitely Okay (1)
  - Probably Okay (2)
  - Might or might not be Okay (3)
  - Probably not Okay (4)
  - Definitely not Okay (5)
  - Can you tell us in your words why you choose the option you did above (6)
-

Q6 How important is your job description and responsibility, in determining the level or type of system access given to you in your enterprise system?

- Extremely important (1)
  - Very important (2)
  - Moderately important (3)
  - Slightly important (4)
  - Not at all important (5)
  - Can you tell us in your words why you choose the option you did above (6)
- 

Q7. Do you agree that, when a single system end-user has access to all the Enterprise data set in the Cloud, this may increase the Enterprise chances of suffering a successful cyber-attack?

- Definitely Agree (1)
  - Probably Agree (2)
  - Might or might not Agree (3)
  - Probably Disagree (4)
  - Definitely Disagree (5)
  - Can you tell us in your words why you choose the option you did above (6)
-

Q8 End-users of a Cloud based ERP software system, should hold some security responsibilities to ensure the security of their Enterprise data in the Cloud. Do you agree with this statement?

- Definitely Agree (1)
  - Probably Agree (2)
  - Might or Might not Agree (3)
  - Probably Disagree (4)
  - Definitely Disagree (5)
  - Can you tell us in your words why you choose the option you did above (6)
- 

Q9 How important is End-user Access Control in ensuring Enterprise data security in the Cloud?

- Extremely important (1)
- Very important (2)
- Moderately important (3)
- Slightly important (4)
- Not at all important (5)
- Can you tell us in your words why you choose the option you did above (6)

Q10 To manage Access Control, Cloud service providers keep a directory known as "CSP Access Directory"; this is a database of all the Cloud end-users and their passwords which is used in authentication each time an end-user accesses data in the Cloud.

Do you agree that the "CSP Access Directory" would improve access control management in the Cloud?

Definitely Agree (1)

Probably Agree (2)

Might or might not Agree (3)

Probably Disagree (4)

Definitely Disagree (5)

Can you tell us in your words why you choose the option you did above (6)

Q11

Enterprise data set classification is a process of classifying enterprise data set against key roles and responsibilities of their end-user, which will determine the level of access each end-user will have and the data that they can access in Cloud.

Enterprise data set classification: should happen as an integral process of the enterprise preparations to move the enterprise data to the Cloud.

Do you agree with the above statement?

Definitely Agree (1)

Probably Agree (2)

Might or might not Agree (3)

Probably Disagree (4)

Definitely Disagree (5)

Can you tell us in your words why you choose the option you did above (6)

---

Q12 Enterprise Database Fragmentation is a feature of a Cloud security model that suggests that Cloud service providers should store the enterprise data set in fragments and implement access control for each fragment of the database.



Do you agree that Enterprise Database Fragmentation in the Cloud would improve enterprise data security of a Cloud-based ERP software system?

- Definitely Agree (1)
  - Probably Agree (2)
  - Might or might not Agree (3)
  - Probably Disagree (4)
  - Definitely Disagree (5)
  - Can you tell us in your words why you choose the option you did above (6)
- 

Q13 An Enterprise system that prompts the Enterprise System Administrator when there is an unsuccessful login attempt, is more likely to promote Enterprise data security in the Cloud.

Do you agree with the above statement?

- Definitely Agree (1)
- Probably Agree (2)
- Might or might not Agree (3)
- Probably Disagree (4)
- Definitely Disagree (5)
- Can you tell us in your words why you choose the option you did above (6)

---

Q14

The set of policies, procedures, technology, and controls that functions jointly to safeguard the Cloud-based system, infrastructure and data are known as Cloud Computing Security Model.

Based on the above definition, Does the current Cloud Security Model available in your Enterprise meets all your Enterprise needs for data security in the Cloud?

Definitely Yes (1)

Probably Yes (2)

Neutral (3)

Probably No (4)

Definitely No (5)

Can you tell us in your words why you choose the option you did above (6)

---

Q15 From your experience, do you consider data security a major concern when your enterprise is adopting a cloud-based ERP software system?

Definitely a major concern (1)

Probably a major concern (2)

Might or might not be a major concern (3)

Probably not a major concern (4)

Definitely not a major concern (5)

Can you tell us in your words why you choose the option you did above (6)

End of Block: Default Question Block

C. Main Study Survey Transcript as generated from Qualtrics for our participant MS P14.

Q1. How many years have you worked in your current role?

- Few months up to 1 year
- 2 years up to 4 years
- 5 years up to 7 years
- 8 years up to 10 years
- 11 years and above

Q2. Do you currently work with a Cloud-based ERP system in your enterprise?

- Yes we are using a Cloud-based ERP system
- No we are not using a Cloud-based ERP system

Q3. Cloud Computing has an impact on Enterprise system data security. To what extent do you agree with the above statement?

- Definitely has an impact
- Probably has an impact
- Might or might not have an impact
- Probably has no impact
- Definitely has no impact
- Can you tell us in your words why you choose the option you did above

because, the data are stored in someone's computer

Q4. The security responsibility for a Cloud system within an enterprise; should be a shared responsibility between the Cloud Service Provider [CSP] and the Cloud Service End-users. (Cloud Service End-user are the enterprise employees who uses the enterprise system to work.) To what extent do you agree with the above statement?

- Definitely Agree
- Probably Agree
- Might or might not Agree
- Probably Disagree
- Definitely Disagree
- Can you tell us in your words why you choose the option you did above

This would probably reduce the risk of data theft

Q5 In your opinion, is it okay to ensure that no single system end-user (including the CFO and the System Administrator) has access to all the Enterprise data set in the Cloud storage?

- Definitely Okay
- Probably Okay
- Might or might not be Okay
- Probably not Okay
- Definitely not Okay
- Can you tell us in your words why you choose the option you did above

Q6. How important is your job description and responsibility, in determining the level or type of system access given to you in your enterprise system?

- Extremely important
- Very important
- Moderately important
- Slightly important
- Not at all important
- Can you tell us in your words why you choose the option you did above

---

Q7. Do you agree that, when a single system end-user has access to all the Enterprise data set in the Cloud, this may increase the Enterprise chances of suffering a successful cyber-attack?

- Definitely Agree
- Probably Agree
- Might or might not Agree
- Probably Disagree
- Definitely Disagree
- Can you tell us in your words why you choose the option you did above

As this end-user may be highly compromised

Q8. End-users of a Cloud based ERP software system, should hold some security responsibilities to ensure the security of their Enterprise data in the Cloud. Do you agree with this statement?

- Definitely Agree
- Probably Agree
- Might or Might not Agree
- Probably Disagree
- Definitely Disagree
- Can you tell us in your words why you choose the option you did above

Q9. How important is End-user Access Control in ensuring Enterprise data security in the Cloud?

- Extremely important
- Very important
- Moderately important
- Slightly important
- Not at all important
- 

---

Can you tell us in your words why you choose the option you did above

Q10. To manage Access Control, Cloud service providers keep a directory known as "CSP Access Directory"; this is a database of all the Cloud end-users and their passwords which is used in authentication each time an end-user accesses data in the Cloud.

Do you agree that the "CSP Access Directory" would improve access control management in the Cloud?

- Definitely Agree
- Probably Agree
- Might or might not Agree
- Probably Disagree
- Definitely Disagree
- Can you tell us in your words why you choose the option you did above

as unauthorized users would not have access

Q11.

Enterprise data set classification is a process of classifying enterprise data set against key roles and responsibilities of their end-user, which will determine the level of access each end-user will have and the data that they can access in Cloud.

Enterprise data set classification; should happen as an integral process of the enterprise preparations to move the enterprise data to the Cloud.

Do you agree with the above statement?

- Definitely Agree
- Probably Agree
- Might or might not Agree
- Probably Disagree
- Definitely Disagree
- 

---

Can you tell us in your words why you choose the option you did above

Q12. Enterprise Database Fragmentation is a feature of a Cloud security model that suggests that Cloud service providers should store the enterprise data set in fragments and implement access control for each fragment of the database.

Do you agree that Enterprise Database Fragmentation in the Cloud would improve enterprise data security of a Cloud-based ERP software system?

- Definitely Agree
- Probably Agree
- Might or might not Agree
- Probably Disagree
- Definitely Disagree
- Can you tell us in your words why you choose the option you did above

As such, in case of a cyber attack,  
then, not data would be compromised

Q13. An Enterprise system that prompts the Enterprise System Administrator when there is an unsuccessful login attempt, is more likely to promote Enterprise data security in the Cloud.

Do you agree with the above statement?

- Definitely Agree
- Probably Agree
- Might or might not Agree
- Probably Disagree
- Definitely Disagree
- Can you tell us in your words why you choose the option you did above

---

Q14.

The set of policies, procedures, technology and controls that functions jointly to safeguard the Cloud-based system, infrastructure and data are known as Cloud Computing Security Model.

Based on the above definition, Does the current Cloud Security Model available in your Enterprise meets all your Enterprise needs for data security in the Cloud?

- Definitely Yes
- Probably Yes
- Neutral
- Probably No
- Definitely No
- Can you tell us in your words why you choose the option you did above

I cant say

Q15. From your experience, do you consider data security a major concern when your enterprise is adopting a cloud-based ERP software system?

- Definitely a major concern
- Probably a major concern
- Might or might not be a major concern
- Probably not a major concern
- Definitely not a major concern
- Can you tell us in your words why you choose the option you did above



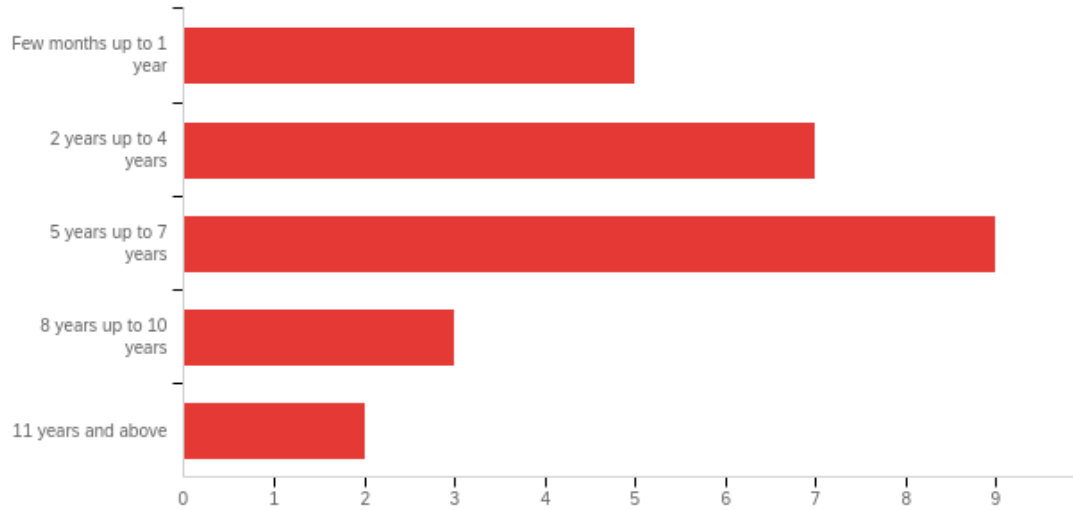
**D. Default Main Study Report as generated from Qualtrics.**

Default Report

End-user Access Control Model Survey

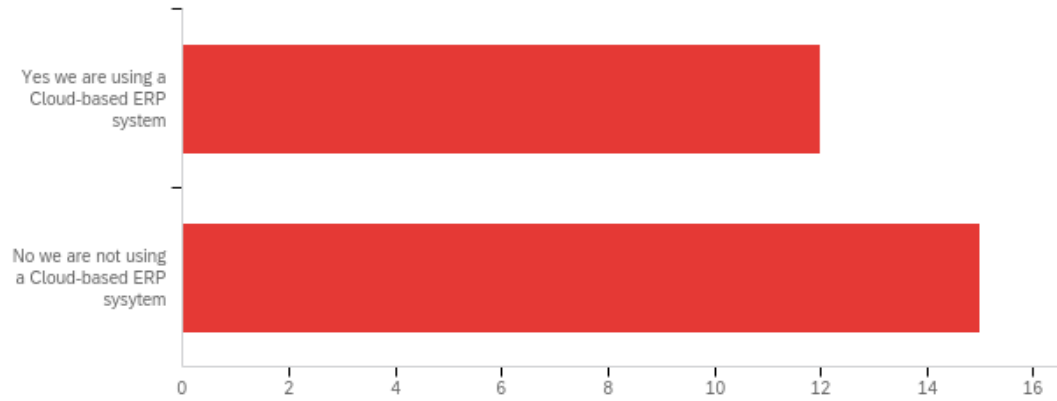
October 19th, 2020, 2:18 pm MDT

**Q1 - How many years have you worked in your current role?**



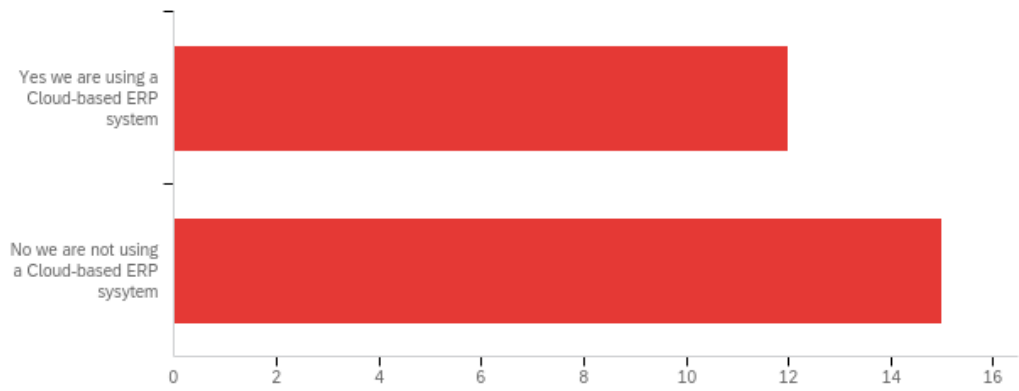
#	Answer	%	Count
1	Few months up to 1 year	19.23%	5
2	2 years up to 4 years	26.92%	7
3	5 years up to 7 years	34.62%	9
4	8 years up to 10 years	11.54%	3
5	11 years and above	7.69%	2
	Total	100%	26

**Q2 - Do you currently work with a Cloud-based ERP system in your enterprise?**

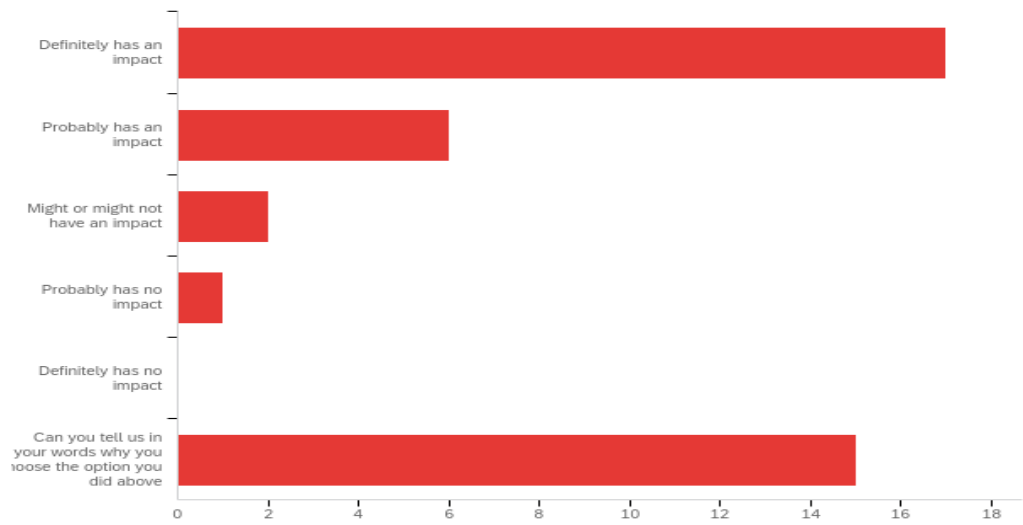


#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Do you currently work with a Cloud-based ERP system in your enterprise?	1.00	2.00	1.56	0.50	0.25	27

#	Answer	%	Count
1	Yes, we are using a Cloud-based ERP system	44.44%	12
2	No, we are not using a Cloud-based ERP system	55.56%	15
	Total	100%	27



**Q3 - Cloud Computing has an impact on Enterprise system data security. To what extent do you agree with the above statement?**



#	Answer	%	Count
1	Definitely has an impact	41.46%	17
2	Probably has an impact	14.63%	6
3	Might or might not have an impact	4.88%	2
4	Probably has no impact	2.44%	1
5	Definitely has no impact	0.00%	0
6	Can you tell us in your words why you choose the option you did above	36.59%	15
	Total	100%	41

Q3\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

---

Because it is the best and has in impart in the society.

---

Yes, because the traditional computing method have become changed to outsourcing of computing resources because of cloud computing.

---

Because I do not know much about it

---

Because cloud storage means storing valuable data in someone's computer

---

Because my neighbour uses computer to store many information that helps in his business

---

Effectiveness in data repository and access to many software applications

---

Things not on site and not seen gives room to possible remote attack vectors

---

Being one of the highest online storage systems, the impact is enormous. The vast space it possesses can support the expanded version of the organisation's security. Also, it has a strong coding system that cannot be easily decoded by online cyber thieves. There is also amazing space for data

---

It depends on the model used, for example in Software as a Service, the overall security lies with the vendor.

---

I really do not understand the level of effects it has on an enterprise security.

---

The ERP system could have unresolved bugs and because it is cloud based, this makes it vulnerable to external attempts to access and exploit the hidden vulnerabilities.

---

Type of cloud platform and provider

---

Cloud Computing most importantly keeps data safe from robbery or disasters like fire outbreak. That alone shows that it Cloud Computing greatly aids in security.

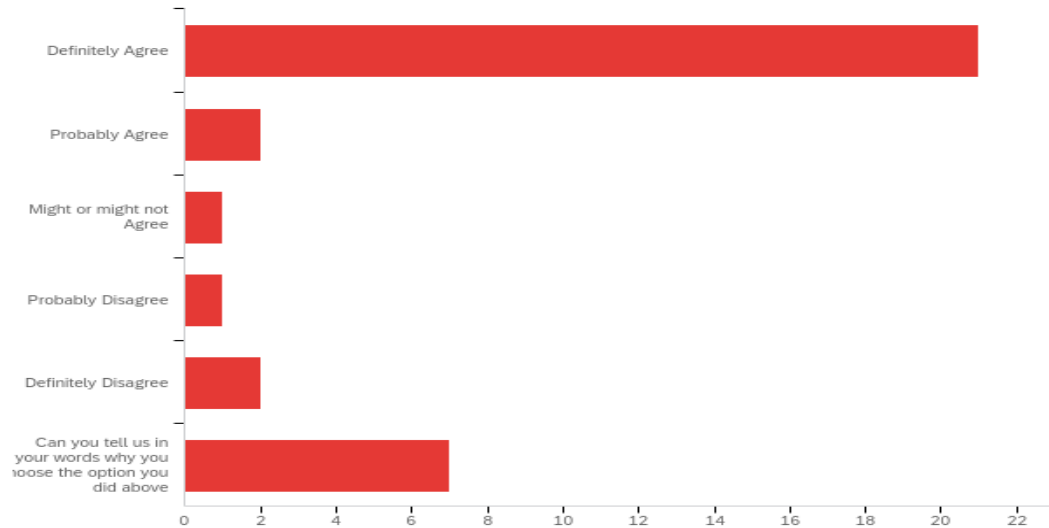
---

It changes how security policies are viewed and implemented

---

Data is more secured in the cloud than it will ever be on a standalone, LAN or MAN.

**Q4 - The security responsibility for a Cloud system within an enterprise; should be a shared responsibility between the Cloud Service Provider [CSP] and the Cloud Service End-users. (Cloud Service End-user are the enterprise employees who uses the enterprise system to work.) To what extent do you agree with the above statement?**



#	Answer	%	Count
1	Definitely Agree	61.76%	21
2	Probably Agree	5.88%	2
3	Might or might not Agree	2.94%	1
4	Probably Disagree	2.94%	1
5	Definitely Disagree	5.88%	2
6	Can you tell us in your words why you choose the option you did above	20.59%	7
	Total	100%	34

Q4\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

Because every stakeholder has a role to play for the security of a cloud system. It takes a weak link from any part of the system for the cloud system to be compromised.

So, everyone would get to know about it. And would reduce labour. To make work earlier for cloud service user and producer, which makes the work going.

if it is your responsibility, you will be more reasonable in dealing with data security incidents.

Because both parties should shoulder the responsibility of protect the data

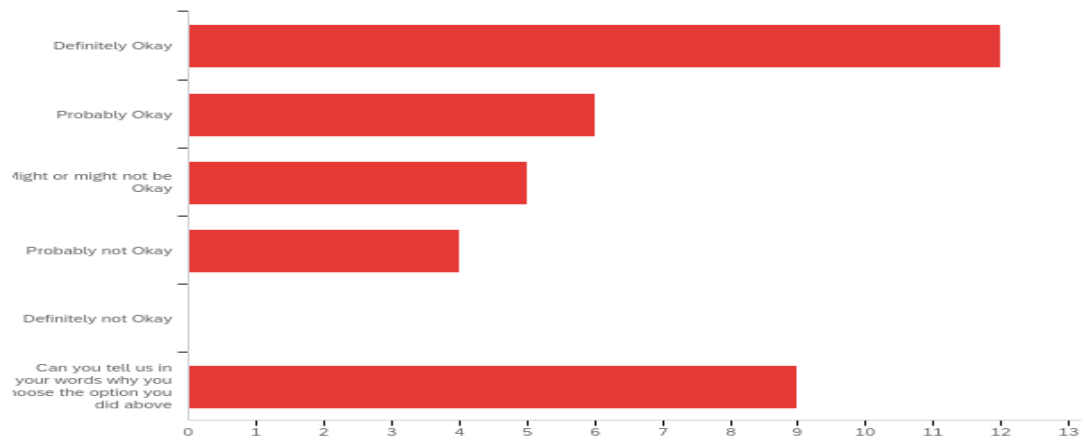
I believe it should be a shared responsibility and majorly that of the service provider; this is because they are the custodian of the database knowing all it involves regarding its functionality and technicality. The end-users can now minimise the kind of information they store that will not infect the database (cloud) with viruses.

It signals censorship of information and privacy.

If employees don't ensure they take measures to secure their data in the cloud, it could be hacked into, and that could destroy the company. If companies continue to crumble for such reason, cloud computing will lose its edge. So, the providers have to ensure they put serious security measures in place.

**Q5 - In your opinion, is it okay to ensure that no single system end-user (including the CEO and the System Administrator) has access to all the Enterprise data set in the Cloud storage?**

+



#	Answer	%	Count
1	Definitely Okay	33.33%	12
2	Probably Okay	16.67%	6
3	Might or might not be Okay	13.89%	5

4	Probably not Okay	11.11%	4
5	Definitely not Okay	0.00%	0
6	Can you tell us in your words why you choose the option you did above	25.00%	9
	Total	100%	36

Q5\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

Although allowing such access may help top management and data consultants effectively discharge their duty. However, avoiding total access by any group will reduce the possibility of gaining access to more personal private data reduce to possibility of a total security compromise of a cloud system.

Cause that is the best option

it depends largely on the company policy am not sure this will impact data security much.

To mitigate the prospect of identity theft or BEC attacks. There's need for limiting access to infrastructure for safety purposes.

From consideration and way to make it better

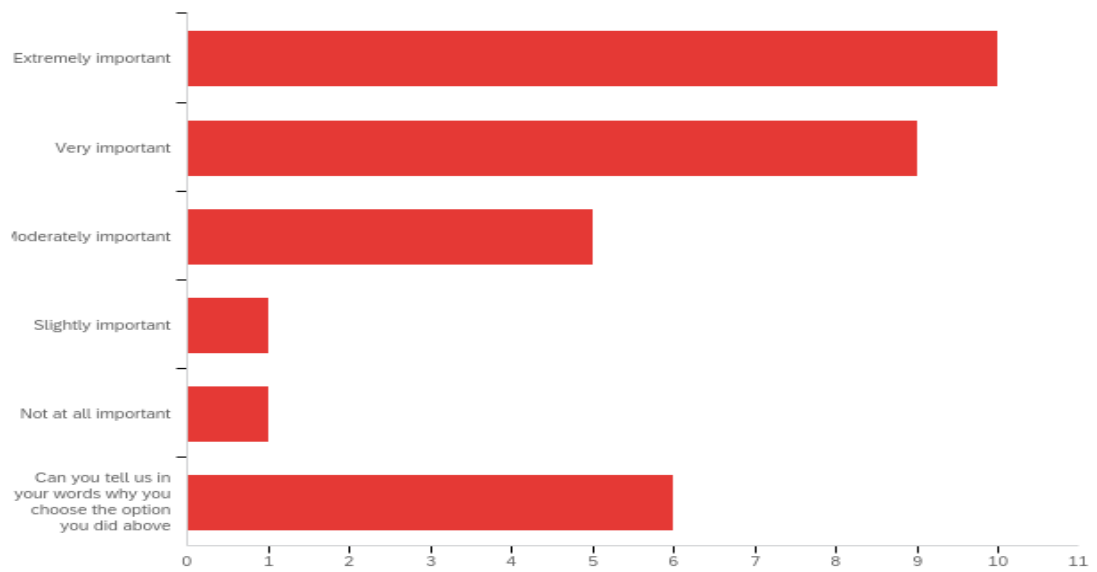
Because it requires shared responsibility, so trusted members should be given access. In that case, in the event of uncertainty, there would be continuity

It depends on the consensus reached.

If one person has access to every data, then if by any chance the person gets compromised, that could lead to the destruction of the company.

Data is more secured that way, as humans are prone to mistakes, error, and other factors.

**Q6 - How important is your job description and responsibility, in determining the level or type of system access given to you in your enterprise system?**



#	Answer	%	Count
1	Extremely important	31.25%	10
2	Very important	28.13%	9
3	Moderately important	15.63%	5
4	Slightly important	3.13%	1
5	Not at all important	3.13%	1
6	Can you tell us in your words why you choose the option you did above	18.75%	6
	Total	100%	32

Q6\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

---

Your role and responsibility determine what aspect of the system one really need.

---

Because it is helps everyone around me.

---

you cannot afford to ignore the role an individual is to play while using the system.

---

I am the project mgr. and the procurement specialist of the organisation. Enormous responsibility is vested on me to deliver on the mandate of the organisation, so without full access my job will suffer.

---



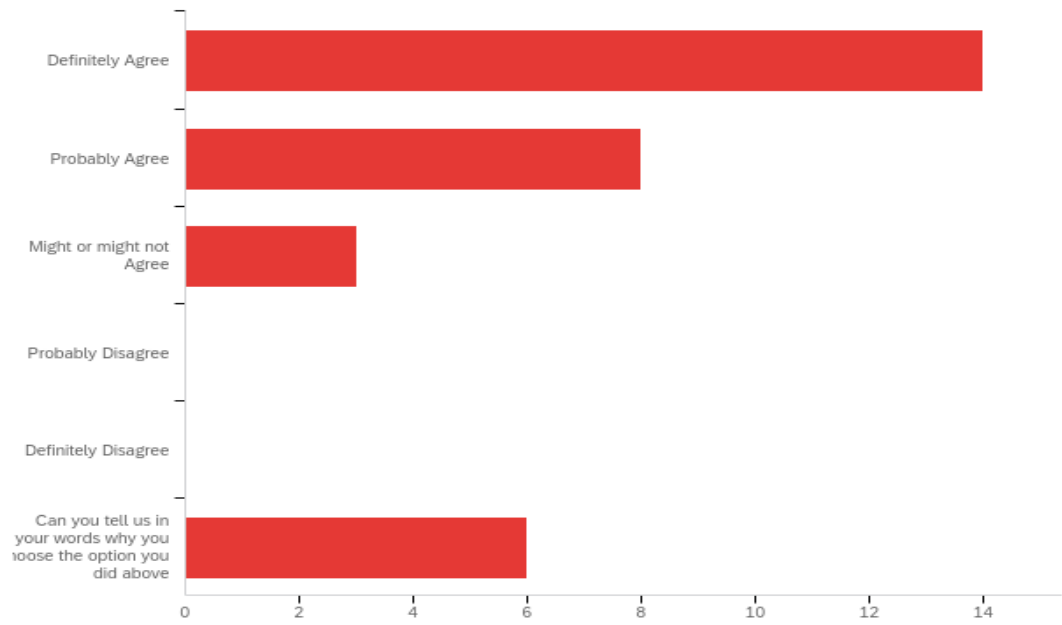
---

All Jobs are important and all information and data should be treated with respect.

---

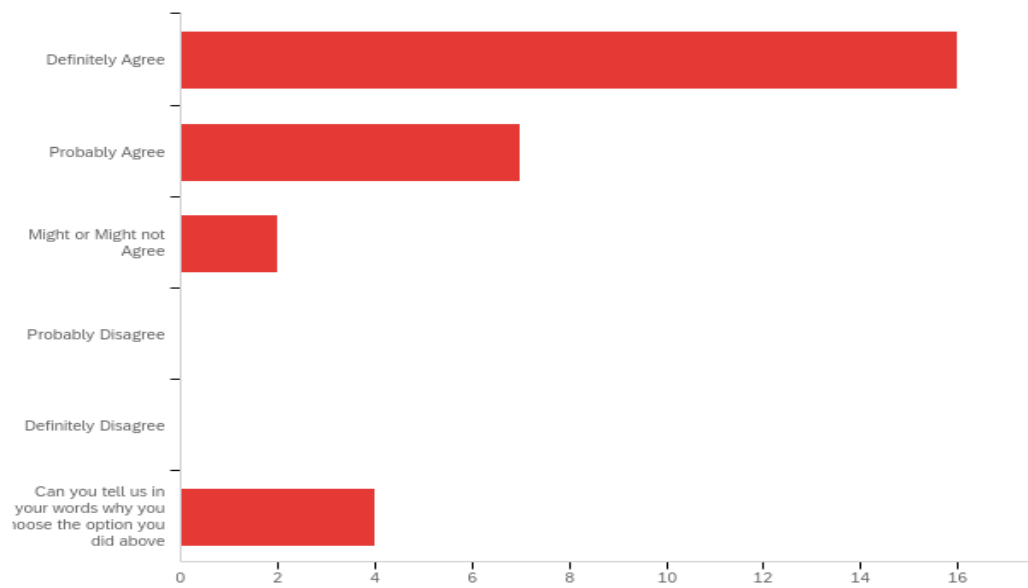
Because if I am to be accountable for something, then I need to have a degree of control over it.

**Q7 - Do you agree that, when a single system end-user has access to all the Enterprise data set in the Cloud, this may increase the Enterprise chances of suffering a successful cyber-attack?**



#	Answer	%	Count
1	Definitely Agree	45.16%	14
2	Probably Agree	25.81%	8
3	Might or might not Agree	9.68%	3
4	Probably Disagree	0.00%	0
5	Definitely Disagree	0.00%	0
6	Can you tell us in your words why you choose the option you did above	19.35%	6
	Total	100%	31

**Q8 - End-users of a Cloud based ERP software system, should hold some security responsibilities to ensure the security of their Enterprise data in the Cloud. Do you agree with this statement?**



#	Answer	%	Count
1	Definitely Agree	55.17%	16
2	Probably Agree	24.14%	7
3	Might or Might not Agree	6.90%	2
4	Probably Disagree	0.00%	0
5	Definitely Disagree	0.00%	0
6	Can you tell us in your words why you choose the option you did above	13.79%	4
	Total	100%	29

Q8\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

---

So, it would be co-ordinated

---

I can understand that it enhances the security of the end-users' data and possibly increases productivity

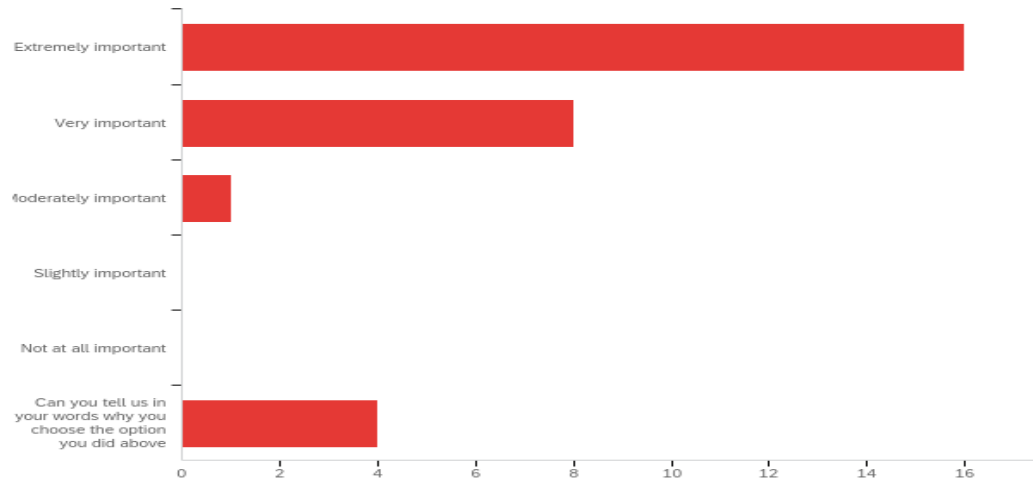
---

Security is an everyone's duty.

---

Security is a joint effort.

**Q9 - How important is End-user Access Control in ensuring Enterprise data security in the Cloud?**



#	Answer	%	Count
1	Extremely important	55.17%	16
2	Very important	27.59%	8
3	Moderately important	3.45%	1
4	Slightly important	0.00%	0
5	Not at all important	0.00%	0
6	Can you tell us in your words why you choose the option you did above	13.79%	4
	Total	100%	29

Q9\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

Best option to choose

Better dissemination of information. Increases the power of ownership. Establishes trust amongst players of the industry. Stronger control

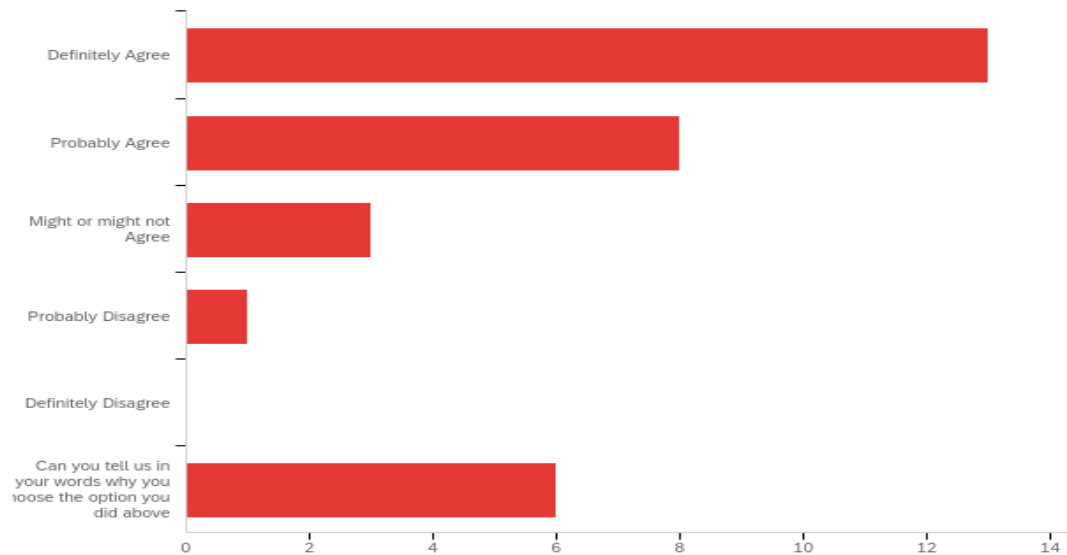
---

They get to manage and secure their data access.

---

They need control and easy access to their data.

**Q10 - To manage Access Control, Cloud service providers keep a directory known as "CSP Access Directory"; this is a database of all the Cloud end-users and their passwords which is used in authentication each time an end-user accesses data in the Cloud. Do you agree that the "CSP Access Directory" would improve access control management in the Cloud?**



#	Answer	%	Count
1	Definitely Agree	41.94%	13
2	Probably Agree	25.81%	8
3	Might or might not Agree	9.68%	3
4	Probably Disagree	3.23%	1
5	Definitely Disagree	0.00%	0
6	Can you tell us in your words why you choose the option you did above	19.35%	6
	Total	100%	31

Q10\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

This enables prompt observation and identification of loopholes within the system.

Cause it improves controls

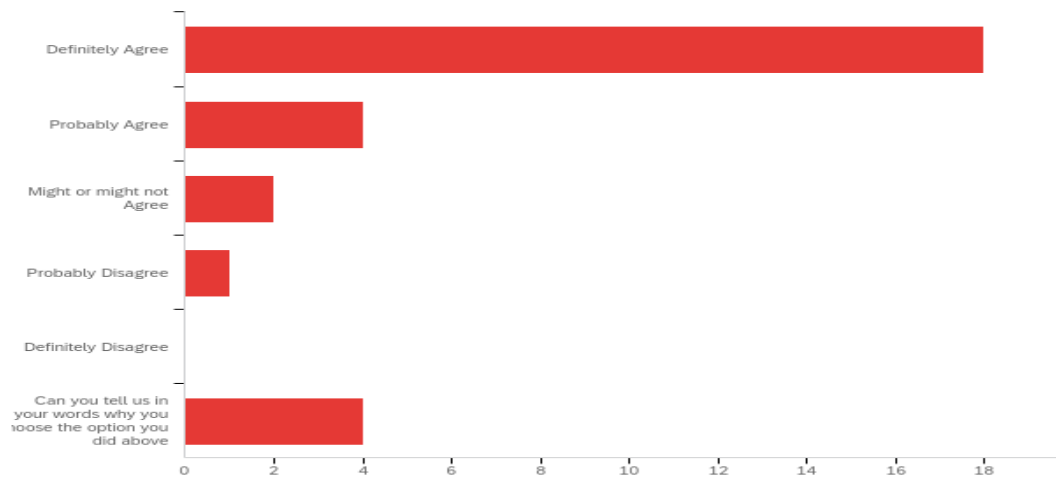
Then on a data bridge, the culprit would be known

Being aware if access control and its responsibility, control should not be made available to everyone, but few trusted members

Well, the data has to be stored in order to make its access easy.

Agree

**Q11 - Enterprise data set classification is a process of classifying enterprise data set against key roles and responsibilities of their end-user, which will determine the level of access each end-user will have and the data that they can access in Cloud. Enterprise data set classification: should happen as an integral process of the enterprise preparations to move the enterprise data to the Cloud. Do you agree with the above statement?**



#	Answer	%	Count
1	Definitely Agree	62.07%	18
2	Probably Agree	13.79%	4
3	Might or might not Agree	6.90%	2
4	Probably Disagree	3.45%	1
5	Definitely Disagree	0.00%	0
6	Can you tell us in your words why you choose the option you did above	13.79%	4
	Total	100%	29

Q11\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

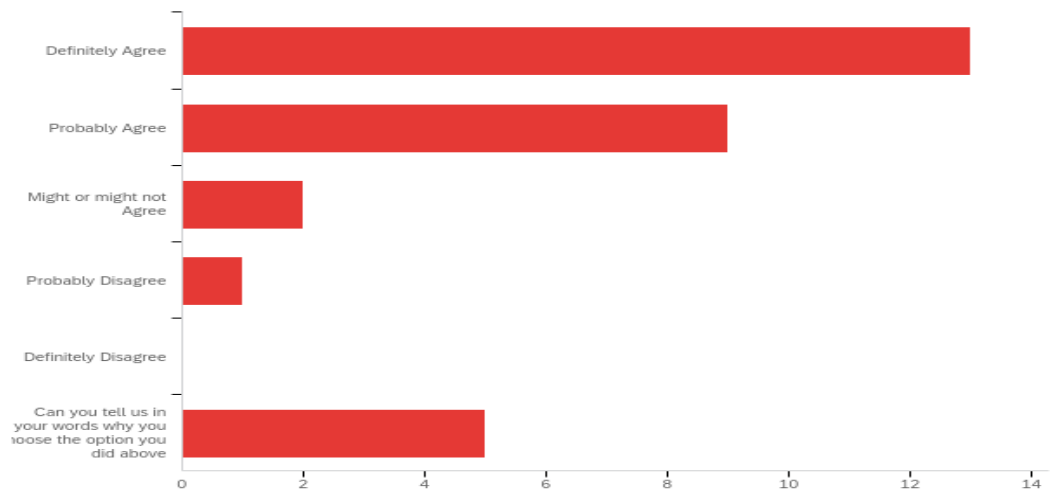
Best option

I do agree as certain classification should be achieved based integral mode for ease and to avoid muddling of data

Yes, I do agree with this because it helps to protect other end user's data.

Agree

**Q12 - Enterprise Database Fragmentation is a feature of a Cloud security model that suggests that Cloud service providers should store the enterprise data set in fragments and implement access control for each fragment of the database. Do you agree that Enterprise Database Fragmentation in the Cloud would improve enterprise data security of a Cloud-based ERP software system?**



#	Answer	%	Count
1	Definitely Agree	43.33%	13
2	Probably Agree	30.00%	9
3	Might or might not Agree	6.67%	2
4	Probably Disagree	3.33%	1
5	Definitely Disagree	0.00%	0
6	Can you tell us in your words why you choose the option you did above	16.67%	5
	Total	100%	30



Q12\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

Best options

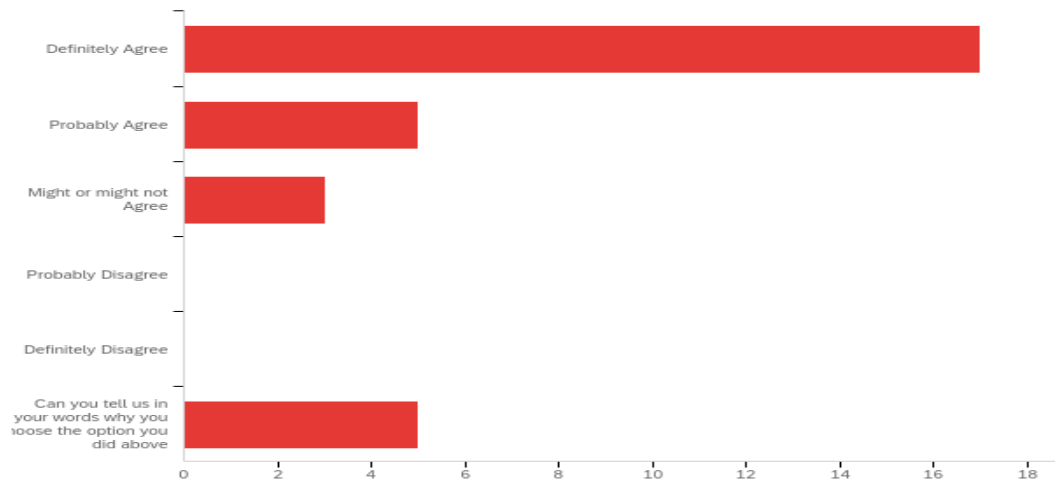
Because then more delicate data are stored differently from the rest

Yes, this can offer stronger data security to the enterprise which can deny cyber attackers from taking full control in the event of an attempt

Cannot really say much here.

It makes cyber-attacks less successful.

**Q13 - An Enterprise system that prompts the Enterprise System Administrator when there is an unsuccessful login attempt, is more likely to promote Enterprise data security in the Cloud. Do you agree with the above statement?**



#	Answer	%	Count
1	Definitely Agree	56.67%	17
2	Probably Agree	16.67%	5
3	Might or might not Agree	10.00%	3
4	Probably Disagree	0.00%	0
5	Definitely Disagree	0.00%	0
6	Can you tell us in your words why you choose the option you did above	16.67%	5
	Total	100%	30

Q13\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

Prompting an inability to login will help but it may also need to identify unauthorised access.

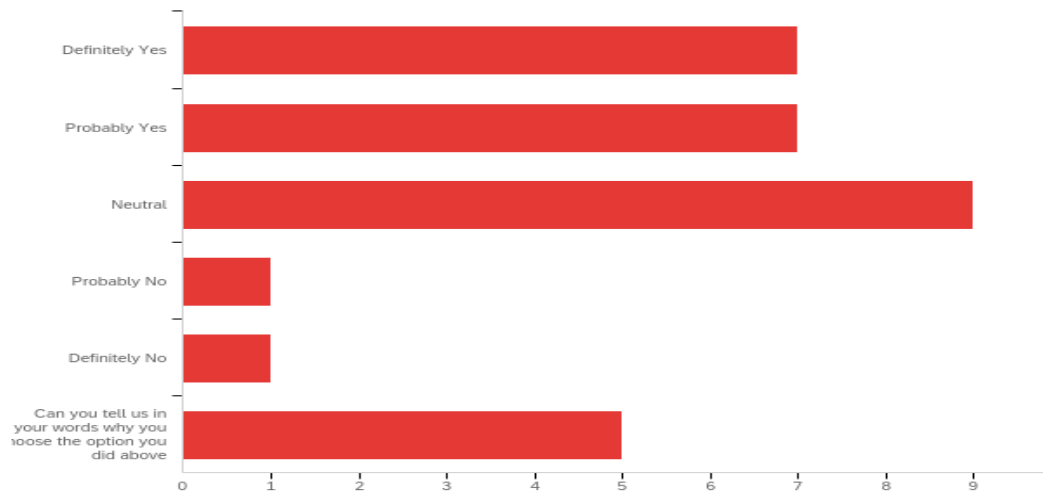
Cause that is the best option

This is an alert system in a way that notifies end-users of interference. By this, there is consciousness, and relaxed mind that attackers are always on the watch.



Because it makes administrators know when an unauthorized person is trying to access their system.

**Q14 - The set of policies, procedures, technology, and controls that functions jointly to safeguard the Cloud-based system, infrastructure and data are known as Cloud Computing Security Model. Based on the above definition, Does the current Cloud Security Model available in your Enterprise meets all your Enterprise needs for data security in the Cloud?**



#	Answer	%	Count
1	Definitely Yes	23.33%	7
2	Probably Yes	23.33%	7
3	Neutral	30.00%	9
4	Probably No	3.33%	1
5	Definitely No	3.33%	1
6	Can you tell us in your words why you choose the option you did above	16.67%	5
	Total	100%	30

Q14\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

Best option

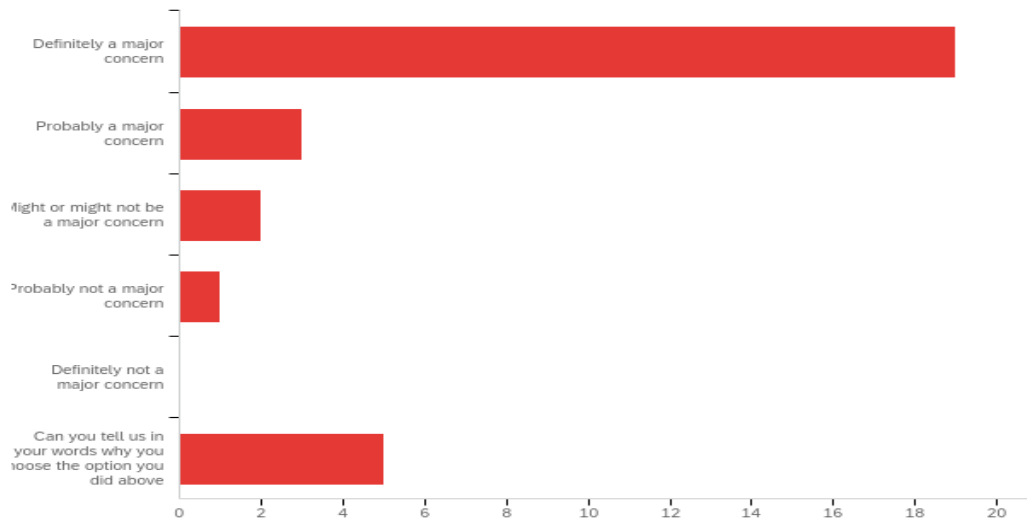
we do not use cloud in my enterprise

But there might still be other areas for improvement

To the extent I understand, I will say my current case has not disappointed.

I do not use it at work.

**Q15 - From your experience, do you consider data security a major concern when your enterprise is adopting a cloud-based ERP software system?**



#	Answer	%	Count
1	Definitely a major concern	63.33%	19
2	Probably a major concern	10.00%	3
3	Might or might not be a major concern	6.67%	2
4	Probably not a major concern	3.33%	1
5	Definitely not a major concern	0.00%	0
6	Can you tell us in your words why you choose the option you did above	16.67%	5
	Total	100%	30

Q15\_6\_TEXT - Can you tell us in your words why you choose the option you did above.

Can you tell us in your words why you choose the option you did above - Text

---

It makes work earlier and simple. Without much suffering

---

Of course, data security is the first thing we take into consideration

---

Without data security is like a house without a roof. Data should be protected at all times. Efforts should be made to enforce the security of data at all times

---

Data security of all sorts is a major concern.

---


Security is a major concern for every organization

## 8.4. Appendix 4. Research Communications


### Research Communications

#### A. Paper

# End-User Authentication Control in Public ERP System in Cloud : A Proposed End-user Centric Model\*

 1<sup>st</sup> Nwanneka Eya  
*Department of Computer and  
Information Science  
University of Strathclyde  
Glasgow, United Kingdom  
nwanneka.eya@strath.ac.uk*



 2<sup>nd</sup> George R S Weir  
*Department of Computer and  
Information Science  
University of Strathclyde  
Glasgow, United Kingdom  
george.weir@strath.ac.uk*

**Abstract**—Cloud Security is the use of latest technology and security techniques to safeguard your data, application and infrastructure associated with Cloud Computing. The set of policies, procedures, technologies, and controls that functions jointly to safeguard cloud-based systems, infrastructures and data are known as Cloud Computing Security Model. This paper reviewed the various identified Cloud Computing Security Model with a close look at the model that addresses data security challenges of a cloud-based ERP systems. The paper is proposing an End user Authentication Control Model for Cloud-based ERP systems. This is a cloud computing security model that uses Enterprise Access Directory, Enterprise Data Fragmentation in cloud and End-user Access Quires, to ensure that End users share a greater security responsibility. The proposed model when compared with other exiting model will encourage more end-user participation in their enterprise data security in cloud. The proposed model also mitigates the impact a malicious insider will have on the enterprise cloud data set in cloud, since no single user can get access to the whole enterprise database in cloud at the same time. The proposed model considered end-user role and responsibility within the enterprise to determine the level of access and the set of data to access in the cloud.

**Keywords**—Data Security, Cloud Computing, End-User, Model

#### INTRODUCTION

Cloud Computing is an emerging IT technology that provides on-demand services to end-user with a high scalability in an efficient way over the internet. S.Bhardwaj et al (2010) [1]. M.Kumari and R.Nath (2018) [2] Defined cloud computing as mainly outsourcing of computing resources over the internet. Computing resources here can main any feature of the traditional computing like servers, networks, data etc. J.Janulevicius et al (2017) [3] Stated that computing cost is

greatly reduced by enterprises who adopts cloud computing, although noting that data security is a major concern. [3-5]. S.H. Abbdal et al (2016) [6] identified that unreliable CSP is a security treat to cloud computing. M.Kumari and R.Nath (2018) [2] Believed that data integrity checks and end-user authorization is done by the enterprise who are the data owners. This will prevent the issues that arises from human factors from the cloud service provider (CSP) centre. Z. Xin et al (2012) [7] Noted that to build a cloud computing data security system is the foundation of building a secured cloud system. It is very important for enterprises that utilize cloud systems for commercial purposes to safeguard their sensitive data, for instance trade secrets.[7]. M.Kumari and R.Nath (2018) [2] Identified that although there have being many developed data security models for cloud computing, that these models did not extensively meet the needs of the end-users of the cloud system. Many scholars have researched and developed models that tried to address different challenges of cloud computing. There are many security challenges of cloud computing which can be categorized into four: infrastructure challenges, data challenges, end-user/CSP challenges and policy challenges. For this research, we have selected some cloud security model that are addressing any of the cloud challenges categories mention above, we took a closer look at Multiple Cloud Database Model which addresses data challenges because it proves most efficient but lacks the integration of end-user/CSP challenges.

This paper proposes an end-user centred model called "end-user authentication control model" for an ERP system in public cloud. The model will address the security gap created by lack of end-user involvement in their enterprise data security in cloud. This paper is organized with section II describing the identified cloud security model, section III using different parameter to compare the different cloud security model and looking at the strengths and weaknesses of the cloud security models. Section IV talks about the attributes

# A REPORT EVALUATING THE FACTORS THAT SUPPORTS AND INHIBITS THE CREATION OF AN INFORMATION SECURITY CULTURE WITHIN ORGANIZATIONS-SMEs.

<sup>1</sup>EYA NWANNEKA, <sup>2</sup>AHMAD RUFAl

<sup>1,2</sup>Computer and Information Science Department University of Strathclyde Glasgow  
Email: <sup>1</sup>nwanneka.eya@strath.ac.uk, <sup>2</sup>rufai.ahmad@strath.ac.uk

**Abstract:** The recent increase in vulnerability of information within an organization due to mobile technologies, online presence, data storage medium and BYOD has raised the concerns on the important of having a good information security culture in the organization. Culture has everything to do with human behaviours and a little changes in the human behaviours could have a tremendous effect on the information security culture [1]. This is why it is important for SMEs to create a good information security culture. The factors that supports and inhibits the creation of an information security culture and their dependability relationship was established. The report analysed the stages of formation of an information security culture within an organization. Milestones for creating and managing a good information security culture is emphasized in this report. The reports offers a recommendation for future research into creating a standard for measuring the financial losses resulting from poor information security culture.

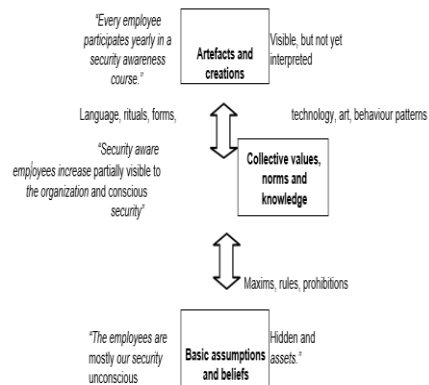
**Keywords:** Information Security, Organization Culture, Small Medium Enterprise.

## 1. INTRODUCTION

Businesses stands to lose a lot of their profit on annual basis due to lack of a good information security in the organisation [2]. Research has shown that many information security breaches are caused by employees of the enterprise; either knowingly or unknowingly[2]. [3] argued that companies' employees poses a greater treat to security of information especially if the organizational security culture is poor. Therefore is critical for any organization that want to implement a good information security to work to have a good security culture in the organization, in order to reduce the risk posed by employees to information security. However, for an organization to achieve this, the need to consider different types of controls and not just focusing on the technical controls; as well as having in place an effective IT governance, trusted internal procedures and a good measures of addressing employees behaviours [3].

The creation of an information security culture within an organization is a very important phase in the implementation of information security and has many factors that supports and inhibits the creation process. Information security culture started because of how the employees of an organization utilize the information security controls within the organization [1]. This information controls could be the different levels of access to different information, the password protection and different anti-virus software. An Organizational culture can be defined as the collective values, norms, and knowledge of an organization,

which is usually based on beliefs and assumptions growing over time that is the way the employees perceive the firm [2]. The Information security culture of an organization is the way processes are done in the firm to protect information which is considered a subculture to the main cooperate culture and it does not belong to any particular department as most system functions has a level of security. The information security culture has three stages and there interaction is shown in the **Fig.1**. The aim of creating a good information security culture is that at the last stage, it will overcome the negative belief employees may have about information security into positive beliefs and assumptions.



**Fig.1. The three Stages of Information Security Culture [2].**

C. Certificate of Conference Attendance and Presentation



# The impact of cloud computing on enterprise system security.

The role of human factor in enhancing the enterprise system security.

Nwanneka Gethrude Eya

Department of Computer and Information Science

University of Strathclyde

Glasgow, Scotland, United Kingdom

nwanneka.eya@strath.ac.uk

## ABSTRACT

Enterprise systems give coordinated and summarized information to all the activities in an organization. These systems fill in as a key resource for any organization and as such, it very necessary to guarantee the security of the data in these systems. Considering the large sum that many organization spend on computing systems and infrastructure, and the need to considerable reduce these cost, this had led to many organization to try reduce their computing cost through implementation of a cloud based solution s. Cloud computing is generally becoming easily adoptable because of its benefits and its strongest point of reducing the computing cost for most enterprise. The small medium enterprises would readily go for cloud solutions as it makes computing affordable and highly scalable. But there are major concerns about the adoption of cloud computing, which largely has to do with the security of data in the cloud. This research focused on determining to what extent the cloud computing poses a risk to the enterprise system data security; and the role of human factors ( *where human here refers to: the employee of an enterprise that is using cloud computing* ) in ensuring a better enterprise data security in cloud. The research proposed a cloud computing data security management a pproach; for an enterprise that adopts the use of cloud computing ; with the intention of understanding if the employees carried out their activities in a particular way, would it pose a risk or enhance the security of their data in the cloud

## KEYWORDS

Enterprise, Enterprise security, Information security, Data security, Cloud, Cloud computing; Emerging computing technology, Access management and Identity management.

## 1 Introducing the views

In the modern era or what many will call the information age; enterprise have an increased need to maximise productivity across all functional areas in order to remain competitive and reliance in their market niche. The need to respond to growing trend in the market have necessitate an over dependency of an average enterprise on technologies that would enable them achieve this. The adoption of an enterprise resource planning (ERP) solutions by enterprise can be dated back to 1990 when Gartner Group first developed material requirement planning (MRP) as well as

computer integrated manufacturing (CIM) to help with product production process in the manufacturing industry. ERP applications are unique software application developed to integrat all functional areas of an enterprise; for instance the finance, proj management, sales, inventory management etc.; which encourages transparent flow of information within the enterprise and therefor boosting the effectiveness. The ERP software applications adoption rate over the last decade can be described as impressive as many enterprises have not only adopted the ERP application bu also have an absolute dependency on these soft-wares to provide the information needed when making major business decisions.

The major challenges faced by enterprise with the implementation of an ERP software application is the associated infrastructure and maintenance cost which made the application unfordable for small medium enterprises (SME). Although there are a lot of ERP software applications developed to target the SME but still; when the return on investment (ROI) is measured against the cost of the ERP software application implementation cost, the result is mostly lean. [1]stated that as at 1998; a large sum of \$17 billion was the annual estimated expenses associated with the implementation of ERP software application in United States enterprises. It was argued that this was a direct result of the 30% 50% growth rate experienced by ERP vendors in US in 1998. By the end of year 200 0; the figure had gone up to \$ 21.5 billion representing a growth rate of 13.1%. This figure continues to grov as the year pass by and with more enterprises continued patronage of the ERP software applications.

The computing technology have experience a major shift with the introduction of the internet. This have changed the way many individual access their information and even the enterprises are no left out. The enterprises are experiencing a move from the traditional computing which invo lved a lot of infrastructures to more responsive internet based computing technology that can handle the rapid demand of realtime information to make busines decisions and remain competitive in the market. The enterprise have experienced a lot of these emerging computing technologies but cloud computing appears to be more intriguing as it promises decent economic gain. Cloud computing can be defined as the computing technology that allows an enterprise access to a set of networked servers using the internet. This simply means that with cloud computing an enterprise do not require a physical server located on their premises. Any IT service that is provided by a clo service provider to an enterprise over the cloud is known as a clo



University of Strathclyde Glasgow

# Understanding the human factor in enterprise data security in the cloud

\*Eya Gethrude, Dr. George Weir  
 Department of Computer & Information Science, University of Strathclyde, Glasgow, G1 1XH  
 \* nwanneka.eva@strath.ac.uk.

**Abstract**

Enterprise systems give coordinated and summarised information to all the activities in an organisation. In order to reduce costs, many organisations have moved to cloud-based solutions, but there are major concerns about the security of data in the cloud. As a key resource for any organisation, it is essential to secure enterprise data that employ such systems. This research focuses on determining the extent to which cloud computing poses a risk to enterprise data security, with particular reference to the role of enterprise employees in using cloud computing. The research proposes a cloud computing data security management approach with the intention of understanding how employee behaviour may pose risks or enhance the security of their data in the cloud.

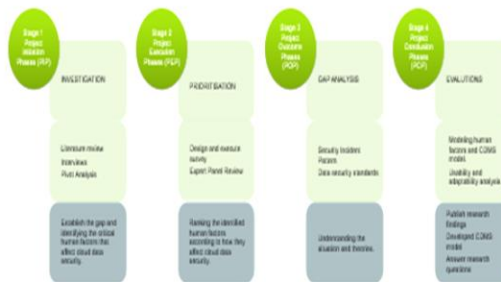
**Research Aim**

The main objective of this research is to develop a data management security model for an enterprise data in cloud, putting into consideration the role of the enterprise employee, which can be used in promoting of data security in cloud and the adoption rate of a cloud-based enterprise system.

**Research Objectives**

- The review of existing literature on cloud data management security models that can measure the impact of direct or indirect human factor on cloud data security.
- Evaluate the critical attributes of an employee that poses a risk to data security in cloud
- The development of a data management security model for an enterprise data in cloud, putting into consideration the role of the direct and indirect human factor.
- The evaluation of the developed framework with respect to its usability and adaptability in an enterprise.

**Methodology**



Each circle represent a single stage in the research. The first box represents what the stage is all about, the second box shows the activities needed to be carried out in the stage, while the last grey box represents the expected outcome of the stage.

The first pivot study was been done with seventeen participants who were considered experts in enterprise system data security, using a structured thirty piece interview question. The aim was to identify the enterprise assumed challenges of adoption of a cloud-based ERP system and the critical human factors that play a role in it.

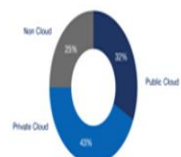
**Research Summary**



It is about you and the enterprise where you earn a living. It is centred on you because it involves your data which gives a very unique information about you and your work. You are concerned that your little secrets are not safe anymore, but your work place believes is not their responsibility; you believe is not yours either; scholars gladly blames the cloud service providers for our enterprise data lost. Do you think your actions or that of your colleagues may have contributed?

**Findings**

% Enterprise Workloads in Cloud



Source: RightScale 2013 State of the Cloud Report

Available data on cloud computing shows that enterprises are adopting cloud computing technology even though there are concerns about data security in cloud. It also shows that there are many enterprise data security models, many of which take the form of ISO standards. The findings show that the ISO standards are perceived as checklist and do not in many occasion transcends to the working ethics within an enterprise.

The responses from the pivot studies showed a general trend in identifying the critical human factor. Trust was mostly identified by the participants as the most critical human factors when considering data security in cloud. We intend to establish if the lack of trust on the cloud service providers is as a result of other underlying factors like poor knowledge, poor skill, poor customer relationship management etc.

**Conclusion**

The trust relationship between cloud service providers and service users was examined. The study intends to establish if the current enterprise data security models considered the cloud technology and the role of the enterprise employee. This study should provide an insight on the impact of enterprise employee on the enterprise data security in the cloud. Researchers could do a further research on the cloud computing architecture as an emerging IT technology, where possible develop a cloud architecture that can limit the identified risks that enterprise employees can pose to the data security in the cloud.

F. Image of Research



## **8.5. Appendix 5. Initial Study Participating Enterprise Profile.**

**Tonimas Nigerian Limited:** Tonimas Nigeria Limited, founded in 1982, has established itself as a market leader in the marketing and distribution of refined petroleum products throughout the country. Additionally, they manufacture and market high-quality lubricants. Additionally, their business group includes a manufacturing facility for aluminium roofing sheets and nails (Tonimas Aluminium), Tonimas Drinking Water, a haulage and shipping company, and the prestigious White Castle Hotels. Tonimas Nigeria Ltd. has conducted extensive research in a variety of fields, which has resulted in the development of dynamic product lines in Nigeria. Their products have become household names as a result of their relentless pursuit of high-quality standards across all their product lines and brands to provide the best quality to their customers. With a large operation and numerous branches, they are constantly looking for new ways to provide high-quality products at affordable prices for the benefit of their customers, which has resulted in the implementation of several ERP solutions over the last decade, the most recent being Microsoft Dynamic AX 2016. On November 16th, 2018, we paid a visit to Tonimas Nigeria Ltd at its headquarters in Aba, Abia State in Nigeria's South-Eastern region. Over a hundred staff members of various ethnic origins oversee the operations of the various business lines and their associated staff located in our numerous branches throughout the country. The meeting with one of the directors and the human resources manager went extremely well, and they expressed an eagerness to participate in the research at the time. Tonimas Group's website is located at <http://www.tonimasgroup.com>.

**Nestoil Limited** was founded in 1991 as the oil and gas division of the Obijackson Group. Local participation in Nigeria's oil and gas sector was extremely limited at the time. Nestoil's initial focus was on blending and marketing petroleum products, but the new company was forced to rethink its strategy in light of established foreign competitors with easier access to capital. Nestoil took a risk and reinvented itself as an Engineering, Procurement, Construction, and Commissioning (EPCC) services provider to the Oil and Gas and Energy industries, and this spirit has defined the

company to this day. Nestoil boldly identified an opportunity within the sector and reinvented itself as an Engineering, Procurement, Construction, and Commissioning company, motivated by a desire to create real value as a Nigerian Oil and Gas company (EPCC). Nestoil persevered through several setbacks and near-misses, guided by a conviction that it was on the right track, despite doubts about an all-Nigerian company's capacity and organisation to deliver on technically complex projects or the ability to amass the best talent to aid its cause. Six years later, in 1997, Shell awarded Nestoil a contract to rebuild its waste treatment plant in Edjeba, Delta State. Nestoil exceeded all expectations with the project's completion—both in terms of work quality and timeliness. It was quickly followed by two additional contracts: the Opokushi Flowstation Upgrade Works and the Otumara Flowstation Debottlenecking Train 3 Works. Nestoil thus began a legacy of success and never looked back. Nestoil has grown to become the region's leading EPCC firm over the last two decades and is the first choice for industry leaders such as Shell, Mobil, and the Nigerian National Petroleum Corporation (NNPC). Nestoil has grown into a successful enterprise with over 1,500 employees capable of executing world-class projects and ranks first among indigenous companies of its type. By completing one project after another, Nestoil has developed a reputation for living up to its operating philosophy – "we deliver results, not just reasons." A visit to the Nestoil Corporate Head Office at Nestoil Towers, 41-42 Akin Adesola Street, Victoria Island, Lagos State on the 29th of November 2018 was uninteresting because I was unable to meet with any of the managers. However, I was advised to submit my proposal to the Executive Director and they would contact me if it is of interest. I have not heard back from them. The company's website is located at <http://nestoil-ltd.com>.

**Intels Nigeria Limited:** Intels Nigeria Limited was founded in 1982 with the vision of developing an integrated logistics solution capable of providing a comprehensive package of facilities and services to Nigeria's oil and gas industry. Intels Nigeria has established itself as a leading supplier of oil and gas logistic support services throughout West Africa, particularly Nigeria, in collaboration with Intels West Africa (Intels) and Orleans Invest West Africa. Intels pioneered the concept of the integrated 'one-stop-shop' oil service centre, bringing together terminal operations, logistics,

transit, and supply services, first in Nigeria and then in other countries. Intels also provides dedicated manpower and equipment hire, secure residential housing, and commercial office space to supplement the services offered at oil service centres and to provide a more comprehensive logistics package. This benefits operators by allowing them to focus on their core business rather than on peripheral activities. Intels Nigeria employs between 1001 and 5000 people, making it the largest employer in south-eastern Nigeria. At the moment, they are using two different ERP solutions: Microsoft Navision 2016 and Microsoft AX 2012. We paid a visit to Intels Nigeria's headquarters in Onne Port Complex on the 15th of November 2018. The meeting with the ERP manager, whom I consider to be my boss, was successful because he expressed his complete support and promised to engage any staff members who could ensure the research was successful during that period. Intel Services' website is located at <http://www.intelservices.com>.

**Frank Advanced Engineering Tech Limited** is a self-contained corporation that is capable of meeting the engineering and construction needs of the oil and gas industries, both onshore and offshore. It was incorporated as an engineering and construction firm in 2015 under the company allied matters decree of 1990. Frank Advanced Engineering Tech Limited was founded to bring together a diverse group of highly qualified professionals to work in the fields of mechanical, civil, electrical, and instrumentation construction services, installation, project management, maintenance, and supplies. Their personnel can work independently or under the supervision of the owner-company to ensure that each phase of each operation is properly inspected and supervised, and that work is performed and documented by the owner's specifications and standard requirements. They are capable of providing highly skilled personnel in nearly every phase of the oil and gas industry. Despite being a subsidiary of Dachiafor Industries Nigeria Limited, one of Nigeria's first structural engineering firms specialising in structural steel fabrication for bridges, factories, and warehouses, Frank Advanced Engineering Tech Ltd has completed numerous contracts for major and independent oil and gas companies throughout the country. In 1999, the company merged with Prime Integrated Engineering Works Ltd. to form FrankTech Limited, which now provides a much broader range of products, including water and fuel tanks,

plant hire, and commercial buildings. From the 1970s to the 1980s, the company was instrumental in the general industrial development of Nigeria. In 2014, the company changed its name to Frank Advanced Engineering Tech Limited. On November 16, 2018, we paid a visit to their headquarters in Aba, Abia State. Although they sounded optimistic during the meeting with their branch manager, I am concerned about their suitability as they currently lack an ERP solution. They currently maintain business records in Microsoft Excel and communicate via standard email accounts. They agreed to participate in the research because they believed it would educate them about the benefits of ERP solutions for their business. Frank Technology's website address is <http://www.franktechnology.com>. These two other companies we could not visit due to distance and time constraints but sent a letter to them and waiting for their response at that time. LADOL- Lagos Deep Offshore Logistics Base and AGIP Energy and Natural Recourses Nigeria. We did not get any response from these two companies.