SECURE CLOUD COMPUTING ADOPTION: A STUDY OF THE ROLE OF CYBERSECURITY CONCERNS IN MEDIUM-SIZED ENTERPRISES IN INDIA

by

Jasmeet Bajaj

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

FEBRUARY, 2026

SECURE CLOUD COMPUTING ADOPTION: A STUDY OF THE ROLE OF CYBERSECURITY CONCERNS IN MEDIUM-SIZED ENTERPRISES IN INDIA

by

Jasmeet Bajaj

Supervised by

Monika Singh

APPROVED BY

Vassiliki Grougiou

Dissertation chair

RECEIVED/APPROVED BY:

Renee Goldstein Osmic

Admissions Director

Dedication

This dissertation is dedicated to my family, whose constant support, patience, and encouragement made this journey possible. Their belief in my pursuit of knowledge and professional growth provided the motivation to persevere through the challenges of doctoral research

Acknowledgements

I would like to express my sincere gratitude to my dissertation supervisor for the guidance, academic insight, and constructive feedback provided throughout the course of this research. Their expertise and direction were instrumental in shaping the study and maintaining academic rigor.

I also acknowledge the support and cooperation of all participants who contributed their time and responses to this research. Their input made this study possible.

ABSTRACT

SECURE CLOUD COMPUTING ADOPTION: A STUDY OF THE ROLE OF CYBERSECURITY CONCERNS IN MEDIUM-SIZED ENTERPRISES IN INDIA

Jasmeet Bajaj

2026

The study examines how cybersecurity issues are relevant in shaping the use of cloud computing (CC) among the medium-sized enterprises (MSEs) in India. Although cloud technologies have significant benefits like reduction of costs, scalability, flexibility, and resource effectiveness, the perceived security risk, a lack of trust in service providers, and resource limitations of the organisation often prove to be a barrier to their adoption. The research design relies on a descriptive study in which primary data were summarised through structured surveys and secondary data were summarised through scholarly and industrial sources to examine the effects of cybersecurity issues, organisational

preparedness, environmental influences, perceived risks and benefits, and trust in service providers on the decisions on adopting a CC. To determine the predictors that are significant in predicting the adoption behaviour, statistical analyses, including regression modelling, were used. The results indicate that the adoption is highly motivated by technological readiness, financial capacity, trust towards service providers, and perceived benefits, and vendor lock-in and availability concerns are the major obstacles. The research gives practical guidance to policy makers, cloud service providers, and business administrators to come up with safe, economically viable and confidence-building approaches to fast-tracking cloud adoption among Indian MSEs.

TABLE OF CONTENTS

List of Tables viii

List of Figures x

List of Abbreviations xiii

CHAPTER I: INTRODUCTION 1

1.1 Introduction 1

1.2 Cybersecurity Concerns Influencing Cloud Adoption 10

1.3 Intelligent Cloud Computing Reference Model for Cyber Security 11

1.4 Threat Reasons in Cloud Computing 13

1.5 Role of Organizational Factors in Addressing Cybersecurity Concerns 16

1.6 Perceived Risks and Barriers to Cloud Computing Adoption 18

1.7 Cloud adoption risk considerations and compensating controls 21

1.8 Perceived Usefulness and Benefits of Cloud Technologies 23

1.9 Role of Trust in Cloud Service Providers 26

1.10 Problem Statement 28

1.11 Research Objectives and Questions 29

CHAPTER II: REVIEW OF LITERATURE 31

2.1 Importance of Cloud Computing for Medium-Sized Enterprises (MSEs) in India 31

2.2 Concerns in Cloud Computing Adoption 39

2.3 Role of Organisational Factors in Cloud Computing Adoption 48

2.4 Environmental Factors Influencing Cloud Adoption 57

2.5 Impact of Geographical Location on Cloud Computing Accessibility 64

2.6 Perceived Risks and Barriers to Cloud Adoption 68

2.7 Perceived Usefulness and Benefits of Cloud Technologies 73

2.8 Role of Trust in Cloud Service Providers 78

2.9 Conclusion and Recommendations for Future Research 81

CHAPTER III: METHODOLOGY 88

3.1 Overview of the Research Problem 88

3.2 Operationalisation of Theoretical Constructs 89

3.3 Research Purpose and Questions 90

3.4 Research Design 90

3.5 Population and Sample 91

3.6 Participant Selection 91

3.7 Instrumentation 92

3.8 Data Collection Procedures 93

3.9 Data Analysis Procedures 93

3.10 Research Design Limitations 94

3.11 Conclusion 95

CHAPTER IV: RESULTS 97
4.1 Reliability Analysis 97
4.2 Findings of Demographic Details 97
4.3 Findings Related to Cybersecurity Concerns 103
4.4 Findings on Organisational Factors 111
4.5 Findings on Environmental Factors 118
4.6 Findings on Perceived Risks and Barriers 122
4.7 Findings on Perceived Usefulness and Benefits 127
4.8 Findings of Trust in Cloud Service Providers 132
4.9 Findings on Adoption of Cloud Computing 135
4.10 Descriptive Analysis 143
4.11 Hypothesis Testing 145
4.12 Summary of Findings 154
4.13 Conclusion 155
CHAPTER V: DISCUSSION 157
5.1 Discussion of Results 157
5.2 Discussion of Research Question One 158
5.3 Discussion of Research Question Two 160
5.4 Discussion of Research Question Three 163
5.5 Discussion of Research Question Four 165
5.6 Discussion of Research Question Five 167
CHAPTER VI: SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS 171
6.1 Summary 171
6.2 Implications 172
6.3 Recommendations for Future Research 173
6.4 Conclusion 175

References 178

Appendix A: Dataset 218

List of Tables

Table 4.1 Reliability Statistics 97

Table 4.2 Demographic details of respondents 97

Table 4.3 Cybersecurity Concerns 104

Table 4.4 Organisational Factors 112

Table 4.5 Environmental Factors 118

Table 4.6 Perceived Risks and Barriers 123

Table 4.7 Perceived Usefulness and Benefits 128

Table 4.8 Trust in Cloud Service Providers 133

Table 4.9 Adoption of Cloud Computing 136

Table 4.10 Descriptive Statistics 144

Table 4.11 Logistic Regression Model Fit and Goodness-of-Fit Statistics for Cloud Computing Adoption 145

Table 4.12 Parameter Estimates for Logistic Regression Predicting Cloud Computing Adoption 146

Table 4.13 Logistic Regression Model Fit and Goodness-of-Fit Statistics for Organisational Factors Affecting Cloud Computing Adoption 147

Table 4.14 Parameter Estimates for Logistic Regression of Organisational Factors on Cloud Computing Adoption 148

Table 4.15 Logistic Regression Model Fit and Goodness-of-Fit Statistics for Environmental Factors Affecting Cloud Computing Adoption 149

Table 4.16 Parameter Estimates for Logistic Regression of Environmental Factors on Cloud Computing Adoption 150

Table 4.17 Logistic Regression Model Fit and Goodness-of-Fit Statistics for Perceived Risks and Barriers Affecting Cloud Computing Adoption 150

Table 4.18 Parameter Estimates for Logistic Regression of Perceived Risks and Barriers on Cloud Computing Adoption 151

Table 4.19 Logistic Regression Model Fit and Goodness-of-Fit Statistics for Perceived Usefulness and Benefits Affecting Cloud Computing Adoption 152

Table 4.20 Parameter Estimates for Logistic Regression of Perceived Usefulness and Benefits on Cloud Computing Adoption 152

Table 4.21 Logistic Regression Model Fit and Goodness-of-Fit Statistics for Trust in Cloud Service Providers Affecting Cloud Computing Adoption 153

Table 4.22 Parameter Estimates for Logistic Regression of Trust in Cloud Service Providers on Cloud Computing Adoption 154

Table 5.1 Summary of Hypothesis 170

List of Figures

Figure 1.1 The cloud computing system's suggested reference model for cybersecurity. 12

Figure 4.1 Age 99

Figure 4.2 Gender 99

Figure 4.3 Employment Status 100

Figure 4.4 Education 101

Figure 4.5 Experience in AI/ML 101

Figure 4.6 AI/ML Techniques Used 102

Figure 4.7 Programming Languages 103

Figure 4.8 I am concerned about the privacy of sensitive data stored on cloud platforms. 105

Figure 4.9 Cloud service providers adequately address data privacy issues. 105

Figure 4.10 I worry about unauthorised access to confidential data in the cloud. 106

Figure 4.11 Cloud systems ensure sufficient measures to protect data confidentiality. 107

Figure 4.12 I perceive a high risk of data breaches when using cloud services. 107

Figure 4.13 Cloud providers effectively maintain data integrity. 108

Figure 4.14 I am concerned about the availability of my data when needed. 109

Figure 4.15 Cloud providers have robust mechanisms to ensure continuous access to data. 109

Figure 4.16 I perceive a high risk of data breaches when using cloud services. 110

Figure 4.17 Cloud providers take adequate measures to mitigate the risk of data breaches. 111

Figure 4.18 Our organisation is technologically prepared for cloud computing adoption**.** 113

Figure 4,19 We have the necessary IT infrastructure to support cloud adoption.113
Figure 4.20 The organisations has sufficient financial resources to invest in cloud solutions. 114
Figure 4.21 Budgetary constraints hinder our ability to adopt cloud computing. 115
Figure 4.22 Top management is actively involved in cloud adoption decisions. 115
Figure 4.23 Senior leadership supports the allocation of resources for cloud initiatives. 116
Figure 4.24 The organisation is aware of the potential benefits of cloud computing. 117
Figure 4.25 Employees understand how cloud computing can enhance business processes. 117
Figure 4.26 Competitive pressure drives our organisations to adopt cloud computing. 119
Figure 4.27 Competitors using cloud computing gain a significant competitive advantage. 119
Figure 4.28 Reliable internet connectivity is critical for adopting cloud computing. 120
Figure 4.29 Internet speed in our area is sufficient to support cloud computing adoption. 121
Figure 4.30 Our geographical location affects the availability of cloud service providers. 121
Figure 4.31 Location-specific challenges hinder our ability to adopt cloud technologies. 122
Figure 4.32 I am concerned about being locked into a specific cloud vendor's ecosystem. 123

Figure 4.33 Vendor lock-in limits our ability to switch providers without significant cost or effort. 124

Figure 4.34 Frequent downtime or outages are a major concern with cloud services. 125

Figure 4.35 The reliability of cloud services affects our willingness to adopt them. 125

Figure 4.36 I am concerned about losing control over data stored in the cloud. 126

Figure 4.37 Using cloud services compromises our ability to manage and secure our data effectively. 127

Figure 4.38 Cloud computing helps reduce overall IT costs for our organisation. 128

Figure 4.39 Adopting cloud services leads to better cost management. 129

Figure 4.40 Cloud computing provides the flexibility to scale resources as needed. 130

Figure 4.41 The scalability of cloud services enhances operational efficiency. 130

Figure 4.42 Cloud computing is easy to adopt and integrate into existing business operations. 131

Figure 4.43 Employees find cloud-based tools and services user-friendly and efficient. 132

Figure 4.44 The reputation of cloud service providers influences our trust in their services. 133

Figure 4.45 Compliance with industry security standards enhances trust in cloud providers. 134

Figure 4.46 Cloud service providers are transparent about how they handle and protect data. 134

Figure 4.47 Providers' clear communication about security policies builds trust. 135

Figure 4.48 Our organisation is actively considering adopting cloud computing. 137

Figure 4.49 The adoption of cloud computing will help us reduce IT infrastructure costs. 137

Figure 4.50 The adoption of cloud computing improves long-term IT cost efficiency. 138

Figure 4.51 Cloud computing services are reliable and meet our business needs. 139

Figure 4.52 We are concerned about data security when using cloud computing services. 139

Figure 4.53 The flexibility and scalability of cloud computing are important for our business. 140

Figure 4.54 Our staff has the necessary skills and knowledge to adopt cloud computing. 141

Figure 4.55 Cloud computing helps improve collaboration and communication within our organisation. 141

Figure 4.56 We trust cloud service providers to handle our sensitive data securely. 142

Figure 4.57 Our organisation's leadership is supportive of adopting cloud computing technologies. 143

List of Abbreviations

Abbreviations	Full Form
CC	Cloud Computing
MSEs	Medium-Sized Enterprises
IS	Information Systems
IS	Information Technologies
NIST	National Institute of Standards and Technology
CTI	Cyber Threat Intelligence
ISC	Information Security Culture
TPB	Theory of Planned Behaviour
TAM	Technological Acceptance Model
PLS	Partially Least Squares
MENA	Middle East and North Africa
SLAs	Service Level Agreements
EC2	Elastic Compute Cloud
SaaS	Software as a Service
PaaS	Platform as a Service
EaaS	Expert as a Service
IaaS	Infrastructure as a Service
EAP	Economically Active Population
SMBs	Small and Medium-Sized Businesses
MSMEs	Micro, Small, and Medium-Sized Enterprises
DL	Deep Learning's
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
SGN	Smart Grid Networks
FAR	False Alarm Rate
MAR	Missed Alarm Rate
MSE	Mean Squared Error
MAE	Mean Absolute Error
DBN	Deep Belief Networks
GRU	Gated Recurrent Units
Modbus TCP	Modbus-Transmission Control Protocol
GOOSE	Generic Object-Oriented Substation Events
MMS	Manufacturing Message Specification
MV-CAAE	Multi-View Combinatorial-Attentive Autoencoder
SEM	Structural Equation Modelling
ANN	Artificial Neural Network
ISM	Interpretive Structural Modelling
TOE	Technology Organisation Environment
PITR	Perceived IT Security Risk

MLR	Multiple Linear Regression
DIT	Diffusion of Innovation Theory
PU	Perceived Usefulness
PEOU	Perceived Ease of Use
ERP	Enterprise Resource Planning
CoT	Cloud of Things
HPC	High-Performance Computing
ROI	Return on Investment
CSE	Computer Self-Efficacy
CBBS	Cloud-Based Business Services
CSFs	Critical Success Factors
CSPs	Cloud Service Providers
SLR	Systematic Literature Review
VE	Virtual Enterprise
IRS	Internet Reliability and Speed
GL	Geographical Location
RCSS	Reputation and Complying with Security Standards
TDH	Data Handling Transparency

CHAPTER I:
INTRODUCTION

1.1 Introduction

Cloud computing technology has developed very fast, and has brought about efficiency and effectiveness in business operations due to flexibility and affordability (Attaran and Woods, 2019). As businesses progress in India, a large number of "Medium Enterprises" MEs are now opting for the third platform, cloud solutions especially in a bid to improve on their competitiveness as they adapt to the unpredictable global markets (Agrawal, Mustafi and Sharma, 2016). However, while the increase in cloud adoption presents a range of advantages, it simultaneously introduces significant cloud security challenges (Chauhan and Shiaeles, 2023). In particular, these concerns are a major drawback for enterprises of a medium size with a limited budget – the full-scale adoption of cloud technology does not seem possible given such conditions. Employers are currently on the risky side due to possible dangers like data theft, compliance, and data localisation, and therefore, the evaluation of safety measures is paramount in their consideration of the adoption (Swire et al., 2024).

Organisations can improve their efficiency and effectiveness and acquire a competitive edge by adopting the quickly expanding computer-based information systems (IS) (Thong, 1999). The IS procedures have been altered by the cloud computing revolution, which has transformed the way IT resources and services are delivered (Misra and Mondal, 2011). Cloud computing has grown in importance in IS development due to the rise of Internet and IT (Al Mudawi, Beloff and White, 2019). Organizations may improve their efficacy and effectiveness and gain a competitive edge using CC. (Lokuge and Sedera, 2017). According to Skafi, Yunis and Zekri (2020a) these benefits are available to both big organizations and SMEs. However, there are concerns about security of CC that are preventing its widespread use (Nagahawatta *et al.*, 2021). Consequently, this indicates that even small businesses are worried about the security of cloud computing. For huge companies, security measures, necessary infrastructure, and trained staff for planning may not be a big deal, but for most SMEs, these are major issues.

(Osborn and Simpson, 2018). According to (Mijnhardt, Baars and Spruit, 2016). SMEs are perceived as having fewer resources, a lower degree of validation, and an informal management style. According to Mijnhardt, Baars and Spruit (2016); Osborn and Simpson (2018b) organization theories and methods that work for big companies might not work for SMEs. Avoiding the usual relational view and instead studying the security needs of SMEs to use cloud computing is critical.

According to Hasan (2023) cloud-based products can significantly cut operational expenses and increase efficiencies for SMEs. There is a lower return on investment and lower costs with cloud computing. In terms of employment, tax income, and export profits, SMEs play a crucial role in any country's economy (Shetty and Rajesh, 2021). If they want to compete on a global scale, SMEs must use CC. The advantages of CC include cheap prices, elastic scalability, and agility. Unfortunately, Indian SMEs are missing out on cloud computing's growth-promoting and entrepreneurial-inspiring possibilities. Jain (2024) Cloud computing is an ideal solution for innovation-driven alliances between universities and companies, but there is a lack of qualified professionals. Before decision-making, it is crucial to consider benefits and drawbacks of cloud technology (Helaimia, 2023). SME cloud adoption is poor because of unresolved concerns, migration interfaces, service level agreements, vendor lock-ins, and a lack of confidence and interest. To address the factors that encourage and hinder cloud adoption, as well as security, financial metrics, and privacy issues, CC wants to be studied from a commercial and business perspective. Adoption, green advantages, and governance structure all depend on cloud computing (Bello *et al.*, 2021).

This research will seek to find out how issues of cybersecurity impact the usage of secure cloud computing among MEs in India. Concerning the perceptions, strategies and modified measures used by enterprises in the course of dealing with security issues, this study aims to find out extent to which these issues influence decision-making. It is important to address this problem since it can help to understand how willing medium enterprises are to implement cloud technologies for their business while preserving data

integrity and customer trust. Potential implications of this analysis for policy advice and guidelines for secure and sustainable cloud adoption in the Indian environment.

Cloud computing is meant to benefit organisations by improving performance, cutting costs, expanding storage capacity, and making it easily accessible from anywhere in the globe. The majority of SMEs in the early stages of their development may find this helpful. Even though these kinds of computer systems have been around for a while and are helpful for many services in Western nations, the concept of CC is relatively new in many developing nations, including India, where businesses are simply looking for more efficient developments and lower creation costs (Katsikatsou *et al.*, 2012). Malecki (1977) SMEs should keep their expenses under control because they are extremely cost-conscious. New technology adoption typically comes at a considerable cost, even though it gives SMEs a competitive edge. Costs of many kinds, including fixed, operating, and training costs, are typically included in every IT investment. However, frequently, the project's real cost exceeds the original projection (Whittaker, 1999; Jørgensen and Moløkken-Østvold, 2006). The high expenses and risks related with IT projects make it difficult for SMEs to invest in or quickly embrace new technology. SMEs are typically tiny businesses, which makes them less structured. Even though they may have a formal IT department, the majority of SMEs lack a systematic risk management procedure. CC is a new business theory that integrates a variety of experts to accomplish corporate business tasks in an internet-based setting, in addition to apps, architecture, and business models. CC has emerged in recent years as a solution to this IT issue due to the growth of new web and IT technologies. An unusual approach to IT is CC, which uses the Internet to store and distribute hardware and software resources. Without really owning these computer assets, it lets companies use a collection of IT resources and applications as services mostly via the Internet. Dutta, Peng and Choudhary (2013) Furthermore, the cloud has macroeconomic advantages. The cloud computing model's cost-cutting characteristic increases likelihood of business development, particularly for SMEs, which in turn suggests increased employment and national output (Keesookpun and Mitomo, 2014). Furthermore, the cloud has macroeconomic

advantages. The CC model's cost-cutting characteristic increases the likelihood of business development, particularly for SMEs, which in turn suggests increased employment and national output

In the modern digital year, “information technologies” (IT) have become a crucial component of organisational architecture of majority of knowledge-intensive organizations across all industries, nations, and institutions (such as manufacturing companies, banks, hospitals, colleges, and even governments). Traditionally, user organisations host and maintain IT resources (such as servers, memory cards, CPUs, software, and data) internally. But as business and technology continue to advance, modern organisations are bolstered by a growing number of IT applications and a constantly evolving IT infrastructure. Maintaining these growing internal IT resources and facilities has become increasingly expensive and time-consuming for businesses. As a result, and also because of the global economic crisis that began in 2008, organisations today frequently struggle to maintain a high level of use of cutting-edge IT applications to maintain competitiveness while also significantly lowering their IT operation and maintenance costs. CC has emerged in recent years as a solution to this IT conundrum due to the emergence of new web and IT technologies. A cutting-edge IT paradigm for hosting and sharing hardware and software resources online is called CC. It allows businesses to use a pool of IT resources and apps as services online without having to store these computer resources on-site. Buyya, Broberg and Goscinski (2011) Additionally, this novel cloud model makes it possible to pay for computing resources as needed. Because of this, using IT resources is comparable to using other everyday utilities like gas and water (Buyya, Broberg and Goscinski, 2011; Mell and Grance, 2012). The development of CC also makes it easier for IT standardization and commoditization to proceed, which is the method via which user companies can use information technology resources as common commodities without having to install, maintain, or build anything specific for them. This includes infrastructure resources like servers, storage, and networks. (Lee, 2010; Muhss, Neumann and Schmietendorf, 2011).

The most important consideration is not whether or not to adopt an innovative technology; rather, it has to do with when to make the decision, either initially or later. Following this, the focus is on the relationship between the unrecoverable expenses typically incurred at the time of adoption and the streams of revenues discovered during the adopted improvement's full life. The biggest difference with cloud technology in terms of enterprise adoption is that it offers a wider range of adoption tactics than certain previous enterprise solutions like ERP, SCM, and CRM. As a result, many businesses wish to adopt cloud technology to improve their performance to be more cost-effective in the current business environment. According to Gupta, Seetharaman and Raj (2013), some microbusinesses and SMEs are still unsure about whether or not to adopt CC trend. CC has several advantages over traditional computing, including scalability, reduced entry costs, device and location independence, and agility. Numerous cloud service providers have emerged as a result of the advantages, and users are increasing their use. In these situations, a CC service's quality can serve as a guide for consumers choosing a cloud service and for providers choosing a criterion or factor to improve their offerings. Choi and Lee (2012) The purpose of this empirical study is to confirm or disprove the conceptual framework's ability to capture adoption decisions and available adoption modalities by cloud stage and to identify factors that influence CC adoption. This framework has been widely used to explain initiative IT adoption. Consequently, they were able to determine, from the adopter's point of view, what factors influence th choice to utilize cloud deployment models and, more specifically, what factors impact the performance of the chosen cloud services (Hsu, Ray and Li-Hsieh, 2014).

Adopting computer-based “information systems” (IS), which are expanding quickly, gives businesses a competitive edge and increases productivity and effectiveness. Thong (1999) The distribution of IT resources and services has undergone a paradigm shift due to cloud computing, which has altered IS procedures. Misra and Mondal (2011b) As Internet and IT have developed, cloud computing has emerged as a crucial component of IS development(Al Mudawi, Beloff and White, 2019). Businesses can improve their efficacy and efficiency and obtain a competitive edge by utilizing CC.

Marston *et al.* (2011); Lokuge and Sedera (2017) These benefits are available to both SMEs and large organizations (Lacity and Reynolds, 2014; Lokuge and Sedera, 2018; Skafi, Yunis and Zekri, 2020). However, the adoption of cloud technology is being threatened by the security issues of CC (Varghese and Buyya, 2018). Thus, security of CC has raised issues for businesses of all kinds, including startups. For large organizations, security protocols, infrastructure, and trained staff needed for planning may not be major issues, but for the majority of SMEs, these are crucial issues. Osborn and Simpson (2018a) Many people have the impression that SMEs are less formalised, less well-funded, and run with a more hands-off approach to management. Therefore, SMEs might not benefit from organizational theories and methods that work for big companies. Mijnhardt, Baars and Spruit (2016) The security requirements for SMEs' adoption of cloud computing must be examined independently, as opposed to using the widely accepted relational paradigm. The study defines "security" as an organization's capacity to effectively manage its security to guarantee availability, confidentiality, and integrity of its cloud-based data and applications. Data availability, data transit, data storage, and data security are primary issues with CC security. Mahmood (2011), malevolent insiders, external assaults, and interruptions in service (Behl, 2011). According to Phaphoom *et al.* (2015) researchers have highlighted security concerns as major barriers to cloud computing adoption. Researchers like Oliveira, Thomas and Espadanal (2014); Nagahawatta, Warren and Yeoh (2020) contend that security concerns are essential to implementation of CC by businesses. Therefore, research on security-related issues and how they affect CC adoption intentions, especially among SMEs, is crucial. According to Nagahawatta, Warren and Yeoh (2020) Additionally, little is known about connection and interplay between adoption of CC and security considerations, as well as between adoption of CC and security needs of SMEs. Thus, this study's goal is to look into the main security-related elements that affect SMEs' adoption of CC.

The majority of firms in many nations and continents are SMEs, which are vital to their economies. They make up about 70% of Europe's workforce, nearly 60% of GDP,

and more than 99.99 percent of EU firms. Nowotarski and Paslawski (2017) Of all firms in the United States, 99% are small enterprises, and of all employees, 47.5% work for these companies (Small Business Administration, 2018). To remain competitive and improve their performance, SMEs must use readily available and inexpensive IT. Only then will they be able to continue contributing to the economy of the countries where they were established. On the list of these innovative and reasonably priced technologies for SMB operations is "cloud computing" (CC). More and more people are starting to pay attention to the CC model as a whole since it promises a radical change in the way IT resources and expertise are distributed (Rekik, Boukadi and Abdallah, 2019). CC offers several advantages to SMEs that choose to adopt and utilize it. It is affordable, doesn't require a lot of technical expertise, and can strengthen bilateral partnerships among businesses. Jäger *et al.* (2016); Moeuf *et al.* (2018) CC has developed into an innovative solution that allows businesses of any size to gain access to advanced IT services without the need for frequent maintenance, retraining of employees, or a large initial investment, regardless of their level of IT understanding. Vu, Hartley and Kankanhalli (2020) CC improves SMEs' performance and competitiveness by facilitating seamless communication across all activities (Xiao and Watson, 2019; Khayer *et al.*, 2020) Research has focused on understanding challenges associated with the implementation of CC since SMEs are unwilling to do so. Review studies are also a part of this field of study (Senyo, Addae and Boateng, 2018; Yu *et al.*, 2018).

Computers and cell phones have seen a meteoric rise in usage over the past several years. Due to this trend, worldwide competition is at an all-time high, and companies are realising they need to diversify their customer bases to survive. Making the most of available resources in pursuit of operational excellence is crucial for meeting this demand. One new development that aims to meet these demands is cloud computing. The concept of CC is not new, although it did not become commercially available until about the year 2000. Computing in the cloud is as easy as offering IT solutions over the Internet as a service instead of a physical product (Senyo, Effah and Addae, 2016). In 2020, over a trillion dollars will be spent on IT related to moving to cloud computing, as

predicted by Gartner (2016), Companies like Amazon, Microsoft, Salesforce, and Google, who offer cloud services, are competing fiercely for a cut of this anticipated profit. A rising number of academic research have focused on CC in the past few years. Literature reviews are part of this set of investigations (Venters and Whitley, 2012; Yang and Tate, 2012; Fernando, Loke and Rahayu, 2013; Bayramusta and Nasir, 2016). The necessity for more reviews arises from the fact that, despite the helpful insights provided by these assessments, there are still certain ignorance gaps about CC. First, some people are unfamiliar with the models, concepts, and theories that served as the foundation for the study of CC. Second, understanding the aspects of CC that have not gotten much attention from scholars is still incomplete. The third issue is that the methodologies that underpin CC research are not well understood. Finally, some people are unfamiliar with the breadth of study and worldwide scope of CC research. They propose that filling in these gaps in knowledge will help advance CC in practice, improve our overall grasp of topic, and serve as a framework for future research. Based on this, this study offers a comprehensive review of CC studies conducted between 2009 and 2015. With the hope of reviewing and shedding light on the state of CC research as well as its theoretical underpinnings, models, methodology, geographic emphasis, and trends throughout the past two decades.

One important market for cloud-based products to decrease operational costs and increase efficiencies is SMEs. The use of CC results in lower expenses and a lower ROI. SMEs play a crucial role in any country's economy because of the jobs, taxes, and export profits they generate. SMEs can't break into the global market without cloud computing. Quickness, elasticity, and cost-effectiveness are just a few of the numerous advantages of cloud computing. However, Indian SMEs are missing out on cloud computing's growth-promoting and entrepreneurial-encouraging capabilities since they aren't making use of the platform's affordable solutions (Garg, Jajodia and Singh, 2023). Cloud computing is an ideal solution for innovation-driven alliances between universities and companies, but there is a lack of qualified professionals. Technology assessment is essential to evaluate cloud technology's merits and demerits before decision-making.

Lack of interest and confidence, unresolved problems, vendor lock-ins, SLAs, and migration interfaces all contribute to SMEs' poor cloud adoption rates. Research on CC should focus on the practical and financial aspects of the topic to answer questions like privacy, security, and factors that influence rate of cloud adoption. The structure of governance, environmental advantages, and acceptance are all impacted by cloud computing.

1.2 Cybersecurity Concerns Influencing Cloud Adoption

At this time, cloud computing is seen as the most cutting-edge technology among the world's top nations, and it is also one of key elements of latest industrial revolution. (ONIK, KIM and YANG, 2019). Cybersecurity risks associated with cloud computing encompass vulnerabilities in its various architectural components (Nita and Mihailescu, 2018). The core concept of cloud computing is around specialised information processing technologies that, according to the demands of the users, expose the computing system's resources as an Internet service. One distinctive aspect of CC is isolation of its users from inner workings of the system, which allows for dynamic resource allocation. Data storage hardware, the hypervisor's ability to generate a virtual machine, and the services offered to end users are the three pillars upon which the cloud rests. The aforementioned aspects of cloud computing are all susceptible to cyber security risks (Khoda Parast et al., 2022). The cloud paradigm's diverse components—including its network, architecture, application software interface, and hardware—increasingly complicate security concerns. Because of this, both cloud service provider and customer run risk of encountering security flaws caused by different combinations of CC (Ghobaei-Arani, Jabbehdari and Pourmina, 2018). Creating a conceptual model is the first important step in securing cloud computing with a complicated framework (Alguliev and Abdullayeva, 2013). Here, we offer a new model for the intelligent cloud system's cyber security reference, built from the ground up using components from various CC layers. An assault model is constructed to ensure the safety of cloud systems, and cybersecurity concerns related to cloud service models are investigated. The cybersecurity of CC is explained by regulations and statutes. Based on security considerations, the ideas of cyber resilience

and cybersecurity in cloud systems are defined. Intelligent cloud systems' cyber resilience architecture is designed.

1.3 Intelligent Cloud Computing Reference Model for Cyber Security

A description of the cloud system's architecture is necessary for ensuring cyber cybersecurity of CC. In this area, major organisations, including Microsoft, IBM, and NIST, offer cloud computing reference models. In the standard model of CC information systems outlined by the "National Institute of Standards and Technology" (NIST), there are five main participants: cloud clients, cloud providers, cloud communication operators (cloud carriers), cloud auditors, and cloud brokers (Liu *et al.*, 2011). The layers that comprise the NIST reference model are Service, Orchestration, Resource Abstraction and Managing Cloud Services, Management, Physical Resources, and Security. The following concerns are taken into consideration while determining how to build a safe CC system in this context:

- Customer authentication and authorisation in the cloud;
- Making sure that resources are assigned for recovery, updates, and connecting new nodes;
- Preserving sight of digital assets;
- Executing performance reports based on tracked cloud activity;
- settling on the terms of the service guarantee;
- Following the specified security policy, keeping an eye on how SLA is being put into action.

A new cloud computing reference model has been put forth by IBM. (Pikaray, Mohapatra and Kumar Rath, 2015). Three parties— consumer, operator, and producer of cloud services—define the cloud computing system model described by IBM's reference model. Entities, groups of entities, or organisations can all fulfil these responsibilities. The hardware infrastructure, cloud management platform, and cloud services are all encompassed in this design, which takes performance, security, and resilience to failures as a common component. The virtualisation and service layers are crucial elements that

are overlooked by the present cloud computing security reference models, despite their importance in guaranteeing the security of CC. Additionally, they fail to consider the issues with cloud computing's cyber resiliency and the social media IoT sensor layer, which gathers text input that attacker's type to launch cyberattacks on cloud infrastructure. To do this, research suggests a new cybersecurity reference model for CC platforms, with components standing in for each layer of the cloud. The updated model is shown here (Figure 1.1).

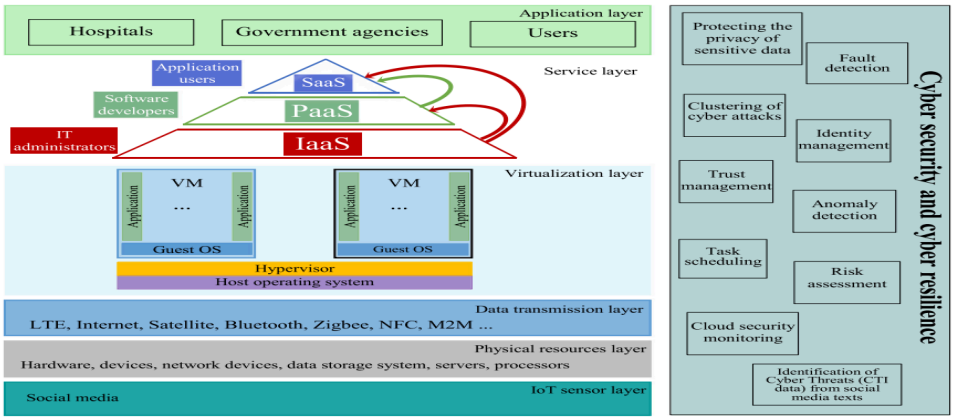

Figure 1.1

The cloud computing system's suggested reference model for cybersecurity.

The two primary components of CC system model that have been presented are the cloud customer and the cloud operator. Layers one through six make up this model: application, service, IoT social media sensors, physical resources, data transmission, virtualisation, cyber resilience, and cyber security, among others.

Considering these factors is essential to the suggested model of a secure cloud computing system:

- Identification of faults;
- Privacy of sensitive data;
- Cyberattack clustering;
- Identity administration;
- Management of trust;

- Identifying anomalies;
- Scheduling tasks;
- Evaluation of risk;
- Monitoring of cloud security;
- Recognising cyber dangers and extracting CTI (Cyber Threat Intelligence) through social media text analysis.

1.4 Threat Reasons in Cloud Computing

Security in the cloud ensures that all data, programs, and hardwwere used in cloud computing are safe. Public, private, or hybrid cloud security is mostly the same for all types of organisations. To safeguard data and the infrastructure supporting cloud computing, a wide range of innovations and controls have been assembled to constitute cloud security. kumar and Goyal (2019) A lot of groups in the business and academic sectors are wary of putting all their data security eggs in the cloud computing basket. Cybercriminals target both on-premises and cloud-based information technology systems. Cloud security requires proper protection, just like any other computing environment. As a result, both data and network are secure, and they can detect and respond to any strange activity or unexpected occurrences with lightning speed. Tu et al. (2020). Ensuring that cloud security measures are up-to-date and effective is crucial in preventing unauthorised access or disruptions. Shen et al. (2018) Service providers need to make sure their clients' data and resources are safe in the cloud if they want to avoid issues and problems. When designing multitenant systems, cloud providers should keep tenants separate and use the principles of segmentation. Verifying the risk associated with outsourced data should be the initial step in developing a strong model in a cloud environment. This can only be accomplished by first sorting data according to risks related to it. Important company data will be prioritised by the security model. Due to their versatility, there are many potential uses for them, including social networks, enterprise, implementation, services, and business tools; thus, it is important to identify the hazards. Ahmed et al. (2018); Mani and Malviya (2019) This study aims to shed light on security concerns that hinder the comprehension, scalability, and assessment of attacks tailored to cloud. With an eye

towards secure cloud computing, they take a look at some foundational studies that pit security explanations against one another. There has to be practical advice on how to secure data in these security explanations. Additionally, new security practices are required for cloud computing.

- **Cloud Computing Fundamentals**

Computing in the cloud is a revolutionary new way of providing consumers with access to shared, on-demand computer resources and services over Internet. The management and utilisation of IT infrastructure is going through a total paradigm change. The approach relies on the seamless collaboration of numerous software and hardware components to deliver a wide range of services. Cloud computing is all about making computing resources, such data storage and processing power, available on demand. It gets rid of the requirement for customers to operate their own dedicated infrastructure. Virtualised computer resources that are accessible whenever needed is the core idea behind cloud computing. As a result, consumers may get their hands on the necessary processing power and data storage without having to worry about maintaining their own specialised infrastructure. Among the many advantages of cloud computing are its scalability, reduced costs, more efficiency, better performance, and stringent security options. Mani and Malviya (2019); Waqas *et al.* (2020) Various models, including public, private, or hybrid ones, can be used to deploy CC. Businesses that operate in public cloud make their internet services available to many different types of customers, whilst those in the private cloud cater only to certain businesses or organisations. In a hybrid arrangement, the public and private clouds work together. The three main service models of CC—IaaS, PaaS, and SaaS—are a flexible way to distribute important data across the internet.

- **Cloud Security: Safeguarding Data and Resources**

The security of information and infrastructure is of utmost importance in the cloud computing ecosystem. Data, software, and the underlying technology are all shielded from harm in the cloud-by-cloud security. It makes no difference whether you're utilizing a public, or hybrid cloud system; private, security is always an issue. For issues

related to data security, several organisations, whether in the corporate or academic sectors, are hesitant to completely adopt cloud computing. Both on-premises and cloud-based IT systems are vulnerable to security breaches. As a result, cloud security is crucial for protecting data and networks adequately and for being able to react quickly to any strange or unexpected occurrences. To keep ahead of prospective hackers, effective security solutions for cloud must improve regularly. Preventing unauthorised access or interruptions requires proactive measures and timely updates. Cloud providers need to take strong precautions to safeguard their data and resources while still providing dependable and secure services if they want to allay fears and worries surrounding cloud security. One strategy makes use of the ideas of segmentation and isolation inside cloud systems that support multiple tenants. Dawood *et al.* (2023) Conducting a risk assessment of outsourced data is a crucial first step in developing a solid cloud security model. Data should be classified according to the danger it represents, and a security model should make sure that the most important data is protected first. Enterprise, social networks, service implementation, and business tools are only a few areas that could be affected by these dangers, thus it's crucial to identify and comprehend them. With this knowledge of potential dangers, we can build security solutions that are specific to cloud computing and its peculiarities. In addition, we will streamline our comprehension of cloud-specific assaults, scaling security solutions, and assessing their efficacy by delving deeper into this literature study and exploring particular security concerns. They will also take a look at new security trends that are pertinent to this ever-changing industry and ongoing research that tries to improve cloud computing security solutions.

1.5 Role of Organizational Factors in Addressing Cybersecurity Concerns

The typical expense of a security issue caused by cyber-attacks exceeding $8.64 million in recent years has catapulted cybersecurity into the forefront of IT study and practice. Johnson (2022) Although there is some research on the topic, it is unclear how factors like company culture and IT use governance affect people's intentions to implement security measures. By providing procedures, frameworks, and mechanisms for making informed IT decisions, IT usage governance mitigates security risks during IT

deployment and maximises resource utilisation. Lunardi *et al.* (2014); Lunardi et al. (2014); Weill and Ross (2004) There is evidence that certain IT usage governance techniques also encourage the desired actions. Bowen, Cheung and Rohde (2007) In addition to IT usage governance, information security culture is essential in establishing a setting that fosters common security goals, values, and procedures throughout a company. Niekerk and Solms (2010) Employees' intentions towards information security behaviours are more positively influenced by companies with a strong culture of information security, according to researchers. Parsons *et al.* (2015) Organizational sanctions, which are the official punishments forced by employers, also work well discourage individuals from participating in inappropriate or unacceptable conduct. Vance, Siponen and Straub (2020) A strong framework for improving security behaviours and reducing risks can be formed by combining IT use governance with an information security culture that is both strong and sanctioned by organization.

In this digital age, organizations must be more vigilant than ever before to protect their assets from cyber-attacks. During the COVID-19 pandemic, cybersecurity was a major concern (Alawida *et al.*, 2022). According to Alawida *et al.* (2022) the study found that spam emails were the second most common cyber-attack strategy, after hacking attempts. As more and more businesses accept remote work, it is clear that COVID-19 has hastened the incorporation of technology into both personal life and business processes. Amankwah-Amoah *et al.* (2021; Battisti, Alfiero and Leonidou (2022) Organizations must priorities cybersecurity because cybercriminals' tactics are evolving in tandem with technology (Pollini *et al.*, 2022). Despite the importance of protocols and technology in preventing cyber-attacks, organizational culture is just as crucial. Michael (2008); Ismail (2017); Maalem Lahcen *et al.* (2020) Organisational culture's influence on cybersecurity is nothing new, but the growing number of threats has brought it into the spotlight in recent years (Ismail, 2017; Maalem Lahcen *et al.*, 2020). Now more than ever, businesses understand and accept that technology alone cannot protect them against cyberattacks. They are proactively implementing modern methods to efficiently prevent and mitigate cyber-attacks. Michael (2008); Ismail (2017); Maalem Lahcen *et al.* (2020);

Moustafa Bello and Maurushat (2021) The potential impact of cybersecurity risks on organisations is substantial, making it imperative to foster a security-first culture to effectively prevent and manage such risks. Perwej *et al.* (2021); Schoenmakers *et al.* (2023) Cybersecurity for present and future populations depends on a "self-renewing" belief system that shapes conduct, (Reid and Niekerk, 2014) A strong “information security culture” (ISC), according to the writers, is the key to meeting this demand.

1.6 Perceived Risks and Barriers to Cloud Computing Adoption

Businesses in wake of COVID-19 pandemic have been hit hard by the desire of workers, consumers, and suppliers to rethink what it means to be an employee and relationships that arise from their job. Dingel and Neiman (2020); Krishnamurthy (2020); PWC (2021); Meyer, Prescott and Sheng (2022) In this rethought environment, cloud-enabled technologies are taken into account; Sixty percent of large companies' environments will be on cloud by 2025, with an expected three trillion dollars in EBITDA value by 2030. McKinsey (2022) While large corporations are rethinking the nature of work, SMEs are encountering a surge in utilized of cloud-based services to accommodate employees and customers who wish to keep many of the same procedures and policies in place for their remote interactions as they had during the pandemic's peak. (Lutfi *et al.*, 2020). Considering cloud-enabled technologies is crucial for many SMEs in the present climate to achieve sustainable growth and remain relevant. Adian *et al.* (2020); George, Lakhani and Puranam (2020); Lu *et al.* (2020); Thorgren S (2020) Because of their adaptability, low cost, and ease of use, cloud technologies are enticing to SMEs. Liu *et al.* (2020); Akpan, Udoh and Adebisi (2022) This study uses "technological acceptance model" (TAM) and "theory of planned behaviour” (TPB) to address the topic of how decision-makers at small and medium-sized regional and local accounting firms see risks of using CC. A total of 116 senior accounting firm executives from various areas were surveyed online to get this evidence. To carry out the analysis, "partially least squares" (PLS) was utilized. Modisane and Jokonya (2021) The purpose of this research is to add to what is already known about the drivers and inhibitors of technology use by SMS accounting firms as they adapt to the modern workplace. The results reveal that the

management of SMS accounting businesses does not view potential increases in job performance and productivity as a reason to be wary of cloud adoption. Heidari and Jafari Navimipour (2022) The study results also showed that people are generally supportive of cloud computing because of how convenient and easy it is to use. Furthermore, our study's leadership believed they had the necessary expertise, insight, and backing to embrace cloud computing should the need arise. This study used technology acceptance model and theory of planned behaviours to look at how leadership's desire to use cloud technology, ideas about how easy it is to use, and how useful it is all factor into perceived risks of cloud adoption.

The use of CC, also known as distributive computing, is on the rise across a variety of industries around the world as a result of its reputation as a cutting-edge technology that offers integrated software and hardware services. A "cloud" is a server-hosted, virtualised database that includes several databases that work together. Because of the vast amounts of data made available by the cloud, many different types of businesses are interested in using it to access relevant data whenever and wherever they need it. There has been a dramatic shift in the IT business towards cloud computing, as there has been in other fields. Locating computing resources across the internet, often known as CC or distributive computing, allows for greater dynamism and flexibility. Many have hailed the rise of CC as a paradigm shift in industry over past few decades. Garg, Versteeg and Buyya (2013) A successful cloud infrastructure provides its users with the highest caliber of service. Alsmadi *et al.* (2022) CC adoption can be influenced by a variety of factors, such as cost, energy usage, performance, trust, and security. Djemame *et al.* (2013); Senarathna *et al.* (2018) Even though the majority of Western nations have been using CC, its uptake is still in its infancy, especially in developing nations. (AlBar and Hoque, 2019).

Technology's quick development has had a major influence on how businesses have developed since it has made it possible to conduct commercial operations in a diversity of ways. Businesses from a diversity of sectors and industries have adopted ICTs to improve operations and raise overall corporate value in the fiercely competitive

market climate of today. Skafi, Yunis and Zekri (2020b) The growth of smartphones, improvements in internet speed (4G/5G), shifting consumer habits, online payment systems, and liberalization of services sector have all contributed to an increase in volume of e-commerce transactions, particularly cross-border e-commerce. Chen and Kimura (2020) Globally, SMEs serve vital functions that are too numerous to ignore. According to academics, SMEs are the engine of economic growth Pathan *et al.* (2017) economic growth's silent hero Chemjor, Charles and Maru (2017), has been tremendously beneficial in fostering economic independence among individuals. It is now generally agreed upon that SMEs constitute the backbone of "Middle East and North Africa" (MENA) region's economy and are critical to long-term GDP of every country in the region. Otman (2021) As a result, SMEs account for 94.3% of all businesses in the country and generate 96.6%, 59.0%, and 25.0% of GDP in Sudan, Palestine, and Saudi Arabia, respectively. Nonetheless, SMEs have long sought ways to reduce operational expenses while maintaining sustainability. SMEs in the Middle East often face difficulties securing capital, which makes many financial institutions wary of lending to these businesses. Yoshino (2016) Therefore, SMEs can effectively reduce expenses and increase business sustainability by using cloud computing AL-Shboul (2019), SMEs may be interested in cloud computing due to how it can reduce costs, provide flexibility, and enable scalability of information technology resources. (Dixit *et al.*, 2021).

1.7 Cloud adoption risk considerations and compensating controls

Cloud computing's many advantages, such as allowing for remote collaboration, virtual data sharing, and access from any location, have made it a popular choice. According to the research, SMEs face significant challenges when trying to implement cloud computing due to the perceived dangers involved. These risks pose a threat to their business continuity and should be carefully considered and addressed. First, the reliability and connectivity of the network; second, control and security of stored data; third, cost of transition to cloud and storage; fourth, trustworthiness and ability of the service provider; fifth, the frequency, completeness, and deletion of data backups; and seventh, the technical knowledge and understanding of the internal staff. These are some of the most

commonly mentioned risks that businesses cite when considering cloud adoption (Alali and Yeh, 2012; Phaphoom *et al.*, 2015; Ali, Soar and Yong, 2016; Morrow and Faatz, 2018). There are additional systematic risks that need to be addressed after a shift to the cloud. System incompatibility, data loss or leakage during transfers, problems with infrastructure support, and network outages are all examples of such problems. (Kuo, 2011; Khan and Al-Yasiri, 2015; Gupta *et al.*, 2021). One of the most important things that users look for in cloud service providers is clear and open regulations about how data is protected and who can access it (Gao and Brink, 2019). Accounting professionals have recognised five types of trust services—security, availability, confidentiality, processing integrity, and privacy—that should be considered and handled in each contact while implementing an information system. AICPA (2022) Continuing with the AICPA's research on cloud computing, a major issue for customers is the lack of confidence in authorisation, authentication, and access management systems. Lee and Brink (2020) An individual's level of trust in a company or brand influences their willingness to try new technologies, level of risk they are willing to take, and ultimately, pace of adoption. Vos *et al.* (2014); Habib and Hamadneh (2021) One further way to build trust is by looking at service level agreements (SLAs) that the cloud provider offers. These guarantee certain things that customers need. Gupta, Saxena and Saini (2016) Companies of all sizes are starting to understand that risks associated with CC can sometimes slip through the cracks when it comes to governance measures like internal control assessments. This occurs when businesses place an excessive amount of trust in vendor controls and fail to include external service providers in their enterprise risk management and monitoring framework. The Treadway Commission's Committee of Sponsoring Organisations Grob, 2012; Meritalk (2021) By enhancing governance and implementing extended general controls audit procedures that cover all aspects of cloud services, not just physical ones, we can increase control coverage, which in turn reduces risks and increases trust in cloud computing among accountants. Church, Schmidt and Ajayi (2020) Protecting data and ensuring the survival of businesses is of utmost importance as SMEs move more and more data to the cloud. To be prepared for security measures, such as managing

passwords, implementing two-factor authentication, encrypting data, and thoroughly understanding the terms of service of service providers, is essential. ZA (2022) Companies of all sizes need to be on high alert for risks caused by their own and their cloud provider's employees, and they should have measures in place to detect and prevent any harmful activities taken by employees. Guillén, Morales-Rocha and Martínez (2020) Despite abundance of risks and hazards linked to cloud adoption, organizations are of belief that the mission-critical nature of the technology justifies its deployment with the right mitigation (Kajiyama, Jennex and Addo, 2017).

1.8 Perceived Usefulness and Benefits of Cloud Technologies

An emerging trend in IT, CC streamlines management of computing resources through the use of innovative approaches. Much anticipation has been generated about this new development in the IT sector, which is said to usher in an era of limitless possibilities, spark a revolution in IT applications, and profoundly impact how companies leverage IT to gain a competitive edge. When it comes to long-term strategy, most businesses see IT as an indispensable asset. The increasing quantity of investment, however, has management demanding measurable outcomes from IT investments before they will approve further funding. Despite the numerous claims made in research studies and white papers about potential benefits of cloud computing—including cost reduction and flexible deployment—many concerns remain unresolved about how to achieve these benefits and what elements in context could affect them. Four main branches of cloud computing scholarship address different aspects of the technology: technical, business, conceptual, and domain/application specific (Yang and Tate, 2012). For instance, research on privacy and security concerns was conducted by Srinivasan (2013) and Whitley, Willcocks and Venters (2013) Problems with cloud computing adoption and implementation were investigated by Furner (2013) and Werfs *et al.* (2013) The advantages of CC have only been briefly touched upon in few scholarly works. A shift in the model's design and the benefits of CC were introduced during the migration of an e-learning portal from an on-premise platform to cloud. Ganesan (2013); Sommer and Subramanian (2013) recognised advantages of CC for smaller pharmaceutical and biotech

firms. These examples demonstrate that the research zeroed in on a particular system in a particular kind of organisation. However, while many have claimed that cloud computing will be beneficial to businesses, few have provided evidence to back up their claims.

The ability to store, manage, and analyse data online without installing software on users' computers or networks is made possible by CC. Services related to the distribution of software, analytics, networking, databases, storage, and servers through Internet are also encompassed. As per an article published not long ago by Marston *et al.* (2011), Investments in information technology in India will reach 87.1 billion dollars in 2018, up 9.2 percent from 2017. On the very same line, Rao (2018) brought to light the fact that Indian spending on SaaS and IaaS on public clouds is approaching $1 billion apiece. Similarly, Aggarwal (2017) indicated that by 2022, more than 1.1 million new positions will be created as a result of the expansion and adoption of CC by Indian businesses. The adoption of CCT is rapidly increasing due to the enormous IT capability and cost-saving advantages it offers to all kinds of organizations. Liu *et al.* (2018) emphasized significance of cloud organization integration and flexibility in enhancing firm's agility. As far as Riera and Iijima (2019), Digital business value can be attained through the utilization of digital technology such as CC and is quantified by the extent to which the organization has succeeded in meeting its business goals throughout the years. Third-party service providers can host CCT and make use of its ability to store data on numerous remote virtual servers. One kind of cloud storage that anyone with an Internet connection can use is Dropbox. As previously stated by Thakurta, Urbach and Basu (2018), Many organizations have already made a switch to CC from on-premise systems due to the many benefits it offers, including greater performance, more functionality, lower running costs, and increased usability.

CC is a particular technical innovation that has been the subject of growing amounts of study into its acceptability (Takabi, Joshi and Ahn, 2010; Lin and Chen, 2012; Huang and Nicol, 2013). Instead of installing software on each user's computer, "cloud computing" makes a variety of programs and apps accessible over the Internet and shared among several users at the same time. Behrend *et al.* (2011) By drastically

reducing the high expenses of physically storing data and increasing the global computing model's capacity, productivity, and scale, it can completely transform an already ground-breaking technology. (Takabi, Joshi and Ahn, 2010; Gupta, Seetharaman and Raj, 2013). Cloud services were adopted by over 70% of responding organisations due to the potential to significantly reduce capital costs on computer hardware, software, information technology support, and data protection and storage. Brender and Markov (2013) The advantages that cloud computing offers businesses also extend to individual customers. Cloud computing is merely the newest storage/processing option for data consumers, which started with hard drives and moved through floppy discs, diskettes, CD-ROMs, and flash drives, much like mp3 files are the newest storage choice for music consumers. Cloud computing has the potential to become the contemporary technology Heidegger originally imagined, revealing the "standing-reserve" of everyone and everything that is waiting to be used (Hanks, 2009).

Companies in the life sciences, including those in the biotech and pharmaceutical industries, are excellent prospects for cloud computing. Whether they are new entrants to the market or long-standing competitors, these businesses are often defined by their dedication to R&D, which results in the continuous generation of enormous amounts of data. Phases such as pre-clinical trials, clinical trials, drug approval, manufacture, marketing, and post-sales all contribute to the data set. Data analysis, classification, and secure storage are required at each stage to meet legal requirements and company policies. Data processing and analysis might be laborious, but it's essential that these businesses get them done quickly because of the cutthroat worldwide competition. With ever-increasing development deadlines and ever-evolving worldwide laws, life-sciences enterprises must adhere to stringent time and cost limitations. Most new businesses in the bio sciences would be scared off by the expense and security measures alone (Sommer and Subramanian, 2013).

Innovations in cloud computing and cloud deployments provide small biotech and pharmaceutical organisations with the opportunity to access and process data more efficiently and at a lower cost, all while benefiting from multi-layered security and

controls. Examining the journeys of small to medium-sized life sciences organisations that have embraced cloud computing can shed light on challenges faced by these organisations and the opportunities presented by this technology.

1.9 Role of Trust in Cloud Service Providers

Cloud computing provides an easily manageable network of interconnected computer and device systems. Online platforms are typically utilised for this procedure. Businesses have a lot of options thanks to the many computing services it offers. The scalability, flexibility, and responsiveness of this technology are too good for businesses to pass up in today's cutthroat market. The problem is that chances like these don't materialise on their own. Additionally, they bring a deluge of difficulties with them. Establishing trust and what it means are both covered in this paper. In addition, the paper also addresses the difficulties associated with finding answers to these problems. Buyya *et al.* (2009) The advent of CC has opened up new possibilities and services for businesses in the realm of computing. Truly, the current climate is quite competitive. Enterprises are compelled to utilize this efficient technology when it provides multiple options, is dynamic, and is elastic. Problems are always there when chances present themselves, though. Zhang, Cheng and Boutaba (2010) As a result of its many trust scenarios, cloud computing has presented a new set of difficulties. CC reliability has become a major issue for numerous businesses. Trust in cloud service providers is high among enterprises. The CC are being questioned. Even said, technological solutions aren't the only answer to such problems. Customers lose faith in businesses when they encounter unclear security promises, data breaches, and a lack of transparency. Cloud computing has recently seen a meteoric rise in number of people utilizing it. People and businesses alike have given cloud computing serious thought and even put it into practice. Business IT executives have been urged to embrace CC due to its many advantageous aspects, including reduced entry cost, pricing, and easy access to a shared pool of data. Research in this area is not lacking. So, it's clear that building confidence in cloud computing is a top priority, as highlighted by numerous studies. Ahmed (2016) To bridge the gap between cloud computing and consumers, we must first comprehend the

trust issues. As a result, some customers are wary of putting their data in cloud. There are a lot of organizations that hold sensitive and critical information. They must so ensure the safety and integrity of this data.

One of most significant Internet-based services, cloud computing is quickly expanding. Amazon Elastic Compute Cloud (EC2) was the first to commercialise the term in 2006, making it relatively new to the IT industry (Abbadi and Martin, 2011). The use of cloud computing has been on the rise recently due to the many benefits it offers to various types of computing tasks, including those that assist businesses (Wang and Wei, 2015; Chang, Walters and Wills, 2016; Corrales, 2016). It gives users a way to pool resources and services from various sites and organisations that are spread out throughout the web. The delivery of computer infrastructure and services has been radically altered by this paradigm shift in computing (Sabi *et al.*, 2016). With cloud computing, the distributed computing environment is more powerful and flexible than ever before. This is a novel approach of providing the computational resources needed to operate online apps and websites (Chong *et al.*, 2014; Keshanchi, Souri and Navimipour, 2017). Many online services, including webmail, blogs, storage, and hosting, have begun to leverage cloud computing. Kim and Park (2013) and provides a range of services to suit consumer needs through infrastructure, platform, and software (Adjei, 2015; Mary Matthew and Quadir Md, 2017). The core components include preexisting technologies that have been successful in constructing and maintaining distributed computing systems, multiprocessors, virtualisation technology, distributed data storage over networks, and networking. By definition, cloud computing is an outsourcing model in which companies contract with third parties to handle various aspects of their IT infrastructure, applications, data, software, and platform needs. Corrales (2016); Du *et al.* (2017), also a popular way for on-demand data storing (L Tian, C Lin, 2010). Cloud computing is a spectacularly calculated method that facilitates service requests by making use of the Internet to build resources for customers. (Xie *et al.*, 2015). Furthermore, it's a method where users in a network environment can make use of both shared and private computer resources. (Mell and Grance, 2011; Chong *et al.*, 2014). Online resources that are

scalable, dynamic, shared, and flexible are made available to users utilising remote data centres. Furthermore, cloud computing expands upon earlier foundational IT practices, including grid computing, virtualisation, and distributed computing. Mehmi, Verma and Sangal (2017), oriented towards service, etc. "Software as a Service" (SaaS) (Espadas *et al.*, 2013; Gani *et al.*, 2014), "Platform as a Service" (PaaS) (Anselmi, Ardagna and Passacantando, 2014), “Infrastructure as a Service” (IaaS) (Manuel, 2015), and "Expert as a Service" (EaaS) are four service delivery models that cloud infrastructure supports (Navimipour and Zareie, 2015).

1.10 Problem Statement

Indian MSMEs find themselves in a challenging environment where selling the dream of using cloud computing for improving business outcomes is equally accompanied by the risk of cyber threats. As much as cloud solutions =enhance efficiency, cut costs, and provide a competitive edge, the escalation in risk of data compromise and leakage, extra access, regulation violation discourages companies. This refers to the ability of an organization in term of workforce, investment in security infrastructure and managing risk that defines how and to what extend cloud can be made a reality. Due to limited capital and unique requirements, it may be problematic for MSEs to develop adequate protection against such threats to avoid stagnation in advancing technology.

However, such perceived risks as inability to control the data, the fear to lose it, and the legal and jurisdictional issues associated with storing it compound the reluctance. Firstly, the trust that enterprises have in cloud service provider is paramount; the success of cloud adoption drive is directly proportional with the faith placed by these enterprises in the cloud service provider to uphold security best practices. This underscores the probable need for transparent practices, strong service level agreement (SLA) and compliance with international security standards. To address this, it is crucial to understand exactly how the Indian MSEs perform a risk-reward calculation on the information shared and stored in the cloud, and which trust-enhancing tools provide them

with the proper cybersecurity reassurances required to expand the utilisation of cloud services.

1.11 Research Objectives and Questions

Objectives

- To identify the various cybersecurity concerns influencing the adoption of cloud computing among Indian MSEs.
- To examine the major role of organisational factors in addressing cybersecurity concerns during cloud adoption.
- To analyse the perceived risks and barriers that hinder cloud computing adoption in MSEs.
- To evaluate the usefulness and benefits perceived by Indian MSEs in order to adopt cloud technologies despite cybersecurity concerns.
- To analyse the role of trust in cloud service providers in mitigating cybersecurity concerns and influencing cloud adoption decisions.

Research Questions:

- What are the various cybersecurity concerns influencing the adoption of cloud computing among Indian MSEs?
- What role do the organisational factors play in addressing cybersecurity concerns during cloud adoption?
- What are the perceived risks and barriers that hinder cloud computing adoption in MSEs?
- What are the usefulness and benefits perceived by Indian MSEs in order to adopt cloud technologies despite cybersecurity concerns?
- How does the trust in cloud service providers mitigate cybersecurity concerns and influence cloud adoption decisions?

CHAPTER II:
REVIEW OF LITERATURE

2.1 Importance of Cloud Computing for Medium-Sized Enterprises (MSEs) in India

Díaz-Arancibia *et al.* (2024) This study analyses developing-world SMEs' digital transformation and adoption of new technologies. In these settings, where particular socioeconomic and cultural elements typically operate as constraints, emphasis is on determining the processes that either help or hinder the incorporation of new technology. This study used a systematic literature review methodology to systematically examine previous research. Important steps in conducting this evaluation were formulating research goals, creating a thorough search strategy, and methodically choosing and evaluating studies from major databases. While more sophisticated technologies such as CC and AI are not as prevalent, the research shows that basic information systems are the most commonly adopted kind of technology by SMEs in developing countries. The entrepreneurial environment and societal factors, such as public and private sector programs, have significant impacts on these adoption trends. This research shows that business and public sector activities aren't as effective as community-driven ones when it comes to encouraging the use of new technologies. Research into specific models for technology adoption that take into account the specific difficulties faced by SMEs in developing nations is warranted in light of the results. Another way to make technology integration initiatives work better in these areas is to take a more inclusive approach that takes sociocultural aspects into account.

In India, Kumar and Nanda (2023) the MSME sector is incredibly varied in terms of size, product diversity, service regions, and technology kinds utilised. It helps lessen provincial prejudice, ensures better, more equitable distribution of national revenue and capital, and promotes industrial growth in rural and underdeveloped areas. From a policy and technological standpoint, this research delves into the many facets of MSMEs' growth in India. They have looked at how "micro, small, and medium-sized enterprises" (MSMEs) have grown in response to specific technology roles and domestic and foreign policy. Internet, e-commerce, mobile communication, online payment systems,

computer-aided design, social media, and internet are the most important technical aspects impacting the success of MSMEs. Various government schemes and initiatives have had an effect on the growth of certain types of MSMEs, and their provisions and effects have been detailed.

Nkwinika and Akinola (2023) this study is on the significance of financial management in SMEs, with an emphasis on the difficulties, successes, and potential developments in this area. A key component that impacts the development, longevity, and competitiveness of SMEs is their financial management. Financial management is crucial to performance of SMEs, which is defined at the outset of research. It stresses that to run a solid firm, SME owners must be well-versed in financial principles, make calculated judgements, and put financial planning first. Case studies provide valuable insight into the financial management strategies used by SMEs. Also discussed are government programs and initiatives that help SMEs manage their finances, particularly initiatives, tax incentives, and access to monetary advising services. SMEs rely heavily on these government interventions because they provide them with resources and guidance, they need to effectively manage their finances. Future developments, such as new technologies (AI, blockchain, IoT) and changes to regulations, are also considered in the analysis, along with their potential effects on the financial management of SMEs. It delves into the topic of financial forecasting, exploring both obstacles and opportunities, with a focus on how information analytics and predictive modelling may enhance accuracy. Reviewing the literature, we find that financial control is crucial for SMEs, and we stress the need for financial literacy, technology adoption, and regulatory compliance. The key to a successful long-term financial balance and success in today's fast-paced business world is for SMEs to adopt best practices and seek assistance from relevant authorities. As SMEs continue to adapt to digital technologies, strong economic control is crucial for their long-term growth and success.

Gupta (2023) looks into how micro-enterprises in Delhi, India, have changed their accounting processes after they started using technology. The main goals of this research were to determine what variables micro-enterprises encounter when trying to integrate

technology into their accounting processes, what factors impact software selection, and how technology adoption relates to perceived gains in financial efficiency. To accomplish these goals, a thorough study was carried out among a varied group of micro-firms in Delhi. The study checked organizations' confidence in data security, how satisfied they were with the software's operation, and the factors they used to purchase accounting software. It also looked at the problems with software adoption and found out what aspects micro-enterprises thought were important for software development. The study's main assumptions show that when choosing accounting software, micro-enterprises in Delhi care most about how much it costs and how useful it is. Adoption of technology increases pleasure and trust in data security, but it does not always result in the impression of more financial efficiency. Software adoption challenges are often business-specific, highlighting the need for individualized solutions. Better tax compliance capabilities, scalability, cloud access, and reporting tools are all things that software users would like to see improved. Policymakers, company owners, and accountants can all benefit from the study's findings, which go beyond Delhi's smaller firms. With these results in hand, lawmakers can craft programs to aid small companies' digital transformation. With this information, business owners can choose the best accounting software for their needs, and accountants may update their skills to keep up with ever-changing world of financial technology.

Wamuyu (2022) To support their business activities, MSEs need the correct OICTI. Large MSEs are anticipated to allocate substantial human and financial resources towards the acquisition, implementation, and upkeep of ICTs to achieve an appropriate OICTI. Instead of pouring a lot of money into private ICT infrastructure, OICTI uses CCS. The purpose of this research was to find out if and how CCS's information processing skills match up with the needs of Kenyan MSEs in terms of OICTI, and if that's the case, how that fitting influences the MSEs' decision to use CCS. The three theories that formed the basis of our model in this quantitative analysis were task-technology fit, organization information processing, and technology-organization-environment. The study's findings point to a close connection

between CCS and MSE operations, as well as between MSE data processing requirements and CCS's capacity to meet those demands. Affordability and the nature of the interaction between CCS suppliers and MSEs are two other recognized criteria that impact CCS procurement. Among the study's notable contributions to the literature on technology adoption in MSEs is the discovery of a multidimensional match between CCS and the OICTI needs of MSEs.

Dixit, Sharma and Sharma (2021) Rural parts of India provide the bulk of the country's workforce because that's where the majority of Indians run their small businesses and help support their communities. As time went on, these mom-and-pop shops became the engine that propelled industrialization. Besides contributing to India's gross domestic product, MSSs have been instrumental in lifting countless people out of poverty. Decisions and policies in India's economy, from the micro to the macro, have been impacted by the recent revolution in big data. By detailing the ins and outs of cloud storage for SMB and MSMB data, this research hopes to illuminate the advantages of big data and how "small and medium-sized businesses" (SMBs) may maximise their use of it. This will help to enhance data filtering and access efficiency. Big data and business analytics have the potential that MSMEs and other small and medium-sized businesses can tap into.

Reyes (2021) Although just 15% of our economically active population (EAP) has access to information and communication technologies (ICTs), 60% of our workforce is employed by micro and small-sized companies (MSEs). It follows that these businesses are hesitant to embrace and make use of ICTs since they are believed to lack understanding, value, and proper importance of these tools. We hope to learn more about the elements that influence this sort of company's adoption of IT through this non-experimental research. In order to achieve this goal, 179 businessmen from Lima Metropolitan Area participated in a survey. Eleven variables were determined to be positively correlated with IT adoption after data evaluation and analysis; three variables were eliminated due to a significance level higher than 0.05. This type of business needs

a fresh approach to information and communication technology adoption, and the 11 acknowledged variables provide it.

Dyubele, Cele and Mbangata (2020) The increase of contemporary technologies such as cloud-based services has attracted various institutions, especially in developing countries. Many businesses have started to show interest in migrating to cloud to increase their businesses, particularly in urban areas. However, it has become challenging for rural-based SMEs to integrate themselves with ICT innovations such as cloud services as they are facing various challenges like poor development of ICT infrastructure. At its heart, this study seeks to evaluate the obstacles that SMEs headquartered in rural areas encounter when attempting to deploy cloud services. A literature review from the previous studies was used to identify these challenges, which were later transformed into variables that ended up being tested in this study. The variables that make up this set include dependent variable—cloud services—and independent variables—security, compatibility, PU, and PEU. To determine if the aforementioned difficulties affect SMEs' adoption of cloud services, researchers used a Likert-scale questionnaire to poll small business owners and staff in the South African town of Elliotdale. Inferential statistics, including correlations between independent and dependent components, regression (predictor), and tests of the validity and reliability of the data-gathering tool (questionnaires) were used to analyses data. According to the findings, aforementioned difficulties—including Security, Compatibility, Perceived Usefulness, and Perceived Ease of Use—substantially hinder the adoption of cloud services by SMEs situated in rural areas.

Shetty, Choudhury and Panda (2020) increase cloud adoption among Indian SMEs by evaluating the performance of Digital-MSME implementation with the aid of the Digital India program and providing suggestions for its successful execution. The authors use a case research approach via theory elaboration technique to empirically corroborate updated general theoretical framework through eight in-depth interviews with industry peers, cloud service providers, and top government officials. In addition to offering insight into well-crafted policies, the study shows that Digital India program is

an excellent means of bridging gap between the creation and dissemination sides of initiatives. For the benefit of stakeholders, the results have introduced a new dimension of nodal points to improve cloud installation. As a consequence of the study, technical dispersion happens in both individuals and businesses. Value is added by the integration of the creating and dissemination sides of policies through participatory governance and participatory citizenry.

Mukherjee (2018) As the world becomes more interconnected, MSMSs in India are falling behind their competitors. When it comes to export competitiveness, the competing enterprises come from neighbouring countries. This is mainly caused by people not using modern technology, but there are other important factors as well. Because of this, immediate measures are required. They look at the Indian Coir Industry as an example of a traditional export-oriented sector that is struggling to compete with other synthetic product manufacturers. Looking at the export pattern over the past five years, it is clear that the value of exports has not seen a significant increase. Competitiveness can be boosted via technology. There have been several theoretical elaborations on technology transfer pathways, export competitiveness, and technological advancements. Inadequate technology will limit the potential of MSMEs, which in turn reduces product demand, sales, and profit margins. A lot of effort has to go into bringing in modern technology, which includes raising people's consciousness, embracing best practices, creating (indigenous technology), and collaborating with partners around the world to develop new technologies. From time to time, the Indian government has been introducing some MSME projects that are linked to technology. Nevertheless, further action is required. Increased investment in R&D and cutting-edge technology, greater use of digital and technology-enabled platforms, technology transfer, increased investment in human resources, improved access to financing, fewer infrastructure gaps, and loosened business regulations can all help MSMEs become more competitive.

Kumar, Samalia and Verma (2018) In developing economies like India's, MSMEs confront numerous obstacles, such as a lack of funding, talent, and ICT capacity. Such limitations prevent MSMEs from making use of many advantages that

contemporary information and communication technology solutions provide. For SMEs in this situation, CC can be a good way to improve internal operations, communicate better with clients and partners, and expand market reach with minimal investment and effort using current ICT solutions. CC is a novel approach to delivering necessary ICT to clients through the Internet on demand and a pay-per-usage basis. SMEs in northern India are the target of this research, which aims to determine whether CC is relevant to them. For this goal, a systematic literature review and a survey based on questionnaires were employed. According to the research, SMEs rank CC's perceived ease of use, cost advantage, simplicity, affordability, scalability, rapid installation, and increased business continuity as its top benefits. Concerns over security, privacy, dependability, and vendor lock-in, however, pose the greatest obstacles to MSMEs' use of CC. Researchers hope that by outlining pros and cons of CC, this study will provide MSMEs with a solid understanding of how CC might benefit their businesses.

Li (2017) This study suggests CC strategies for SMEs as a means to efficiently address resource dynamic demand and final cost, improve management, decrease costs, promote informatisation development, and achieve resource integration. Utilising research methods such as experiments, literature reviews, and experience summaries, this study examines the modern commercial society's competitive environment for SMEs, their CC value, and their CC strategy from three angles: "infrastructure as a service" (IaaS), "platform as a service" (PaaS), and "software as a service" (SaaS). The report goes on to detail the IT-to-cloud computing process for SMEs, their CC model, fundamentals of CC, and how to secure cloud computing for SMEs. The empirical results demonstrate that SMEs have successfully transitioned their IT to cloud. This move could help SMEs save expenses, improve management, and allocate resources more dynamically. Since cloud computing has far-reaching effects on businesses, SMEs need to adapt it to build and boost their competitiveness.

Carlos *et al.* (2017) This research provides an overview of CC, including its key features, components, and applications. Furthermore, it also executed alongside technological review. When it comes to organisational competitiveness in a world where

information systems have long played a crucial role, SMEs whose main focus is not technology need to figure out how cloud computing may become a formidable ally.

2.2 Concerns in Cloud Computing Adoption

Overview of Cybersecurity in Cloud Computing

Ahmad *et al.* (2022) CC's flexible design enables the distributed storage of data and resources, which in turn makes them available for a variety of industrial applications. There has been a shift in how businesses store, retrieve, and share applications due to CC. Due to its increased availability, decreased price, and enhanced performance, CC has recently attracted a large number of industries. There have been major developments in IoT thanks to cloud computing as well. But there were a lot of security worries brought up by the quick move to the cloud. When it comes to cloud-based systems, traditional security solutions aren't always the best option. Even though multifarious cyber weapons have proliferated and been used successively over the previous three years, the difficulties and security issues related to cloud platforms have been resolved. Cloud-based industrial security issues may be resolved with the many benefits that "deep learning's" (DL) rapid advances in AI have brought forth. The following findings are part of the proposed study: a comprehensive analysis of cloud-based IoT architecture, services, configurations, and security models; a thorough discussion of how cloud security concerns in IoT are divided into four main categories (data, network and service, applications, and people-related security issues); an analysis of recent developments in cloud-based IoT attacks; the presentation of limitations from the perspectives of deep learning, artificial intelligence, and general; identification of technological challenges in the literature; and, lastly, the identification of important research gaps in IoT-based cloud infrastructure to highlight.

Nafea and Amin Almaiah (2021) There has been a meteoric rise in the speed, amount, and variety of data in past few years. This has led to massive and complicated big data, which in turn has created difficulties with storing, managing, analysing, and protecting this data. CC has become increasingly popular among businesses, but many still fail to adequately address the security and privacy concerns associated with this

model, and as a result, fail to apply best practices and procedures when utilizing CC. As a result, additional study is needed to identify and address these security risks in the cloud system environment. Through the analysis of published research from 2019 to 2020 and a cloud risk assessment in a Saudi Arabian company, this study attempts to gather the most frequent mitigation strategies and cyber security threats in the cloud system environment.

Tissir, El Kafhali and Aboutabit (2021) The core idea behind the new paradigm of distributed computing is cloud computing. Utilisation of shared computing resources is central to its concept. Cybercriminals can exploit security holes in Cloud Computing just like they can with any other new technology. Recent research on the effects of security measures has focused on cyber-security, also known as cyberspace security, which encompasses the interplay between software, users, and services across the Internet. So far, no research has been able to pin down exactly what Cloud Computing cybersecurity management requires. Issues with CC security, ISO, cybersecurity variations, and NIST standards are the primary foci of this research. By analysing NIST's "Cybersecurity Framework" (CSF), ISO 27,032, ISO 27,001, and ISO 27,017, It intends to provide a comprehensive framework for controlling and averting cyber threats in cloud computing, as well as to clarify the tenets and protocols of these standards. Aside from that, their research zeroes in on criteria for gauging level of development of framework-using organizations. Their goal is to help businesses choose the best way to handle cybersecurity risks in the cloud or to enhance the procedures they currently have in place.

Ervural and Ervural (2018) The global development sector is undergoing a metamorphosis to satisfy the increasingly intricate and fiercely competitive needs of the modern business world. Industry 4.0 is a new phenomenon that has evolved in the current period due to the tremendous advancements in technology. Cybersecurity in particular is one of the emerging concerns brought about by the convergence of operational and information technologies. Cybersecurity, one of the most talked-about topics in recent years, has been studied in this section. The advent of the IoT is another important shift in the evolution of cyber threats. Within the framework of IoT, a global perspective including both the public and commercial sectors examines IoT security risks and

vulnerabilities, industrial challenges, main reasons for cyberattacks, necessity of cyber security, and various cyber security solutions and methodologies.

Aljumah and Ahanger (2020) CC has emerged as one of key new aspects of computer technology since invention of computers and their extensive use. CC's advantages, such as processing power and internet-connected computing resources, have improved users' personal and professional lives, but they have also brought about serious security and privacy risks that need CC systems to be adjusted. In light of this, the current study examines the several risks that cloud computing faces and outlines countermeasures. It was discovered that absence of management knowledge regarding utilization of CC services and their protection mechanisms poses a serious hazard in terms of data breaches. Additionally, cloud computing services may be abused, which could impact not only the organization's sensitive data but also the user's personal information and identity.

Shanbhag et al. (2020) intends to offer a thorough understanding of the cloud computing technologies being applied in the process control industry up to the chosen year, as a large portion of the literature currently available on the topic includes research conducted up until 2019. This study presents the main concepts of cloud computing, how the technologies were used in process control systems, and some possible benefits and drawbacks. It also emphasises the key areas of application, best practices, and concepts including the applicability of AI in the fields of manufacturing, public sector, education, healthcare, and retail. Furthermore, it discusses the cloud computing prospects in process control, presents examples, and investigates the latest trends. According to the study's findings, problems with security, delays, and anticipating regulatory requirements still exist even though cloud integration can have a significant positive influence on costs, flexibility, and data analysis. To help stakeholders deal with the expanding trend of cloud-enabled process control systems, the study's last part provides advice.

Duncan, Creese and Goldsmith (2015) Cloud computing can significantly lower costs while giving customers more flexibility. Nonetheless, security issues are still brought up as a possible deterrent to the use of public, private, and community clouds.

Trusted cloud models were identified as one of the European Network and Information Security Agency's top research goals in its report on goals for Research on Current and Emerging Network Technologies. In September 2012, computer emergency response team at Carnegie Mellon University published a study outlining insider risks to cloud computing as a potential area for future investigation. Additionally, a 2010 initiative at the University of Warwick examined cloud computing security, namely the possibility of cascading effects. The threat and vulnerability landscape, as well as the incentives and motivations that potential attackers might have, were meticulously modelled for this study. Insider threats may be biggest source of danger, according to one of the findings. This study outlines the advancements made in this field of study by examining the types of attacks that insiders can launch, as well as the consequences and harm they can cause.

P.S, S and M (2018) Cybersecurity refers to the methods described in published works that aim to protect an organization's or user's cyber environment. Security measures are overseen by it to ensure that networks, programs, and data remain intact and protected from unauthorized access. Information technology security is another name for the same set of procedures and technologies that fall under this umbrella. As more and more of our daily lives are conducted on computers, smartphones, TVs, and the myriads of little gadgets that make up the IoT, the field is becoming increasingly important.

Sun (2018) Modern network service practices are being reshaped by the meteoric rise of cloud computing. Many “X-as-a-Service” (XaaS) cloud-based service providers are facilitating on-demand, adaptable adoptions. Many advantages come with CC, but it also comes with some security risks. To properly implement cloud solutions, one must have a solid grasp of CC security risks. Computer, network, and information security are the three main facets of cloud security that this study examines in depth. It also covers a range of other CC security challenges. Reviewing the literature gives a bird's-eye perspective of cloud security and brings together the most current findings in the area. The key results of this study can give theoretical backing and evidence for future cloud security research.

Key Cybersecurity Concerns for MSEs

Ikuero and Zeng (2022) When MSEs take advantage of the internet's features, they boost industrial growth, raise their productivity, and ultimately contribute more to the nation's prosperity. Businesses should promptly notify the relevant incident response organization whenever they are targeted by cyberattacks so that they can recover quickly. In this study, we look at the reporting practices of MSEs in Nigeria about cyber events. A hundred MSEs were polled for this research. The majority of MSEs (72%) failed to disclose cyber incidents because they were ignorant of the reporting mechanism. By sensitizing the public, 90% of participants think "Sectoral Computer Security Incident Response Team" (CSIRT) might increase the number of cybersecurity incidents reported. Their list of recommendations for the Sectoral CSIRTs included creating an IRRP to handle cybersecurity events in MSEs.

MUNIR (2024) This study's overarching goal is to ascertain how MSE employees' normative beliefs, understanding, control perceptions, and attitudes towards information security change as a result of meeting ISO 27001 requirements. Participant selection includes a convenience sample; 21 MSE-related professionals filled out an online questionnaire as part of study's methodology. This study's survey sought to collect information on demographic aspects as well as participants' perceptions and attitudes about ISO 27001 and its effects on various psychological components. Compliance is often seen as a good thing and thought to help with the security of the organisation. However, the results showed that compliance doesn't help with improving employees' knowledge, attitude, or behaviour when it comes to IS. Compliance was found to have a moderately favourable association with perceived behavioural control and subjective norms, suggesting that it prepared employees to follow security standards and foster a security culture accordingly. On the other hand, recent tendencies towards poor correlations between compliance levels and knowledge, attitude, and behaviour highlight the necessity for thorough training and a culture that supports its employees. Achieving strong information security policies and effective compliance in MSEs requires real participation, ongoing assistance, and the use of social norms, according to the report. There are a few caveats to the study, such as a small sample size and a lack of depth in

the analysis. This points to the need for more research to see what other elements could play a role and how to apply a wider range of samples.

Muhati (2018) Cybercrime is a platform that has emerged as a new basis for competitive advantage: data. Computer systems have made this transition possible. Since the number of cyber threats has grown, cyber-security is no longer an optional extra for businesses of all sizes. Since they lack the capital to adequately combat new forms of cybercrime, SMEs are considerably more vulnerable to these attacks. Based on research showing that cyber-security duties and liabilities are severely impacted by leadership and laws, economics provides a better framework for understanding the problems surrounding cyber-security than purely technological approaches. In an attempt to address cyber-insecurity, this study set out to identify consistent elements impacting company strategies in several SME sectors. To achieve this objective, the study examined leadership and government policies as well as other economic elements that are significant in establishing a secure cyber-space business environment for SMEs. The study's author is crossing her fingers that the findings will shed light on cyber habits of SMEs and serve as a road map for fixing their cyberspace problems. Research in this descriptive study used questionnaires to determine which cyber-security factors contributed to the lessening of cyber-threat effects and which did not. For this analysis, we used SPSS, a statistical program. Research aimed for a sample with a 95% confidence interval. Also, to check for significant relationships in the data, we utilised a Cronbach Alpha test to evaluate reliability and a correlational analysis.

Hossain *et al.* (2019) This study carries out an extensive investigation into the integration of big data and ML into the electrical power grid, a feature brought about by the advent of "smart grid (SG), next-generation power system. The IoT provides the connectivity that is essential to this new grid infrastructure. Because of the system's interconnectedness and the need for continual communication, a huge amount of data has been generated, necessitating analysis and decision-making procedures that surpass those of the past. An inexpensive and effective method of data collecting and load forecasting is available with an IoT-integrated SG system. These advantages cannot be realized

without the use of big data analysis and ML tools. IoT, gadgets and data they contain have become prime targets for cybercriminals in the intricate network of SG. This paper also covers these security concerns and how to fix them. This comprehensive evaluation provides a synopsis of the subject and an outline of potential future academic and industry research areas in this sector. To give a concise summary, the relevant sections include tabulated key points from the literature review.

Efiong *et al.* (2024) A relevant dataset depicting or simulating "smart grid networks" (SGN) is necessary for development of cybersecurity models that can adequately protect mission-critical infrastructure. Researchers in the field face a significant obstacle when trying to get appropriate SGN real-life statistics. Additionally, current datasets do not include IEC61850 protocol, which is necessary for simulating substation automation operations to develop cybersecurity solutions. Research and experiments requiring large amounts of data near the real-world scenario can be supported by the datasets presented in this study, which are simulated from a fully virtual testbed. For this experiment, an intrusion detection model was trained on the dataset using the following parameters: precision, recall, accuracy, F1-score, detection rate, "false alarm rate" (FAR), "missed alarm rate" (MAR), "mean squared error" (MSE), "mean absolute error" (MAE), and loss. The model was based on a combination of "deep belief networks" (DBN) and "gated recurrent units" (GRU). According to the results, models for substation automation system security that use distributed network protocol version 3, IEC61850, and "Modbus-transmission control protocol" (Modbus TCP) are better suited to standalone "deep learning" (DL) algorithms than hybridised ones. These systems support "generic object-oriented substation events" (GOOSE) and "manufacturing message specification" (MMS).

Ullman *et al.* (2024) Research focusing on both behaviors and design is necessary to tackle the ever-increasing threat of cybersecurity. Amazon Web Services and other public cloud providers, as well as federal funding agencies like the National Science Foundation, have spent billions of dollars creating HPC resources that users may access through VM images that can be customized. This method gives users freedom to adapt

their environment to their specific computing requirements. Although there are many advantages, users frequently put thousands of vulnerabilities at risk when they install open-source software or misconfigure their file systems. Security staff face challenges when trying to prioritize the identification and remediation of vulnerable assets due to the extent of the vulnerabilities. This study developed a new "Multi-View Combinatorial-Attentive Autoencoder" (MV-CAAE) that uses unsupervised deep learning to automatically detect clusters of vulnerable compute instances and collect data on multiple dimensions; this will aid in creation of targeted remediation plans. Using three technical clustering experiments, they thoroughly tested the suggested MV-CAAE against cutting-edge approaches. The MV-CAAE outperforms benchmark approaches by 8–48% in terms of V-measure scores, which are metrics for cluster quality. Through a thorough case study, they clustered susceptible virtual machines and used semi-structured interviews to gather qualitative feedback from seasoned security experts, demonstrating the practical value. Based on the findings, it is possible to improve decision-making and prioritise repair efforts by clustering sensitive assets. Our theoretical understanding of cyber-defence is also enhanced by the current design research activity.

2.3 Role of Organisational Factors in Cloud Computing Adoption

Ali *et al.* (2020) Cloud services are becoming more important in the IT industry as a way to improve efficiency, save costs, and increase productivity. Since organisations like local governments may focus on their major business goals using cloud-based services, the stability and scalability of their systems can be improved. This study seeks to identify critical factors that might impact the adoption of cloud-based services within the context of the Australian state and regional governments. A more all-encompassing model for adoption of IT innovations for cloud technology was created by merging components from the desires model, the diffusion of innovation model, and TOE model. "Information technology" (IT) professionals from 47 different government agencies provided the data. Compatibility, security concerns, cost, anticipated benefits, complexity, and organisation size were determined to be most important factors influencing the

adoption of cloud-based services by local governments, according to the report. Any business looking to decide whether or not to invest in cloud-based services can probably benefit from findings of this study. The data is imperfect to LGAs in Queensland, Australia, which means the results may not be applicable outside of that state. In addition, majority of the participants were managers, therefore results may not be representative of factors influencing cloud implementation among IT workers on the front lines. Another drawback is that chosen theories might cause certain important aspects to be overlooked. Last but not least, hybrid models, as well as public, community, and private cloud usage, were not included in this study. Based on a literature assessment on cloud implementation from an IS viewpoint, the report presents a combined framework of cloud-based service adoption. It builds a more thorough innovation implementation framework for cloud technology by adopting an integrated approach.

Aharony (2015) This study aims to discover what makes information workers embrace new technologies like CC in their workplaces. The goals of this study are to determine how much cloud computing intentions are explained by "technology acceptance model" (TAM) and how much CC intentions are explained by personal characteristics like cognitive evaluation and openness to experience among information professionals. Two categories of information professionals—librarians and information specialists—were subjects of the study that took place in Israel in the autumn of 2013. Information about participants' identities, computer skills, attitudes towards CC, behavioral intentions, cognitive appraisal, receptivity to new experiences, and self-efficacy were gathered through seven surveys. Several of the TAM variables, as well as individual traits and level of computer proficiency, were identified as factors that influence behavioral intention to utilize CC in this research. The study applies the TAM to information professionals and CC, broadening the scope of previous research on the topic. It also emphasizes the significance of individual traits like computer competence, openness to experience, cognitive appraisal, and personal innovativeness in determining technology acceptance. In addition, the present research suggests that IT directors should be well-versed in TAM and the matter of individual differences if they believe that new

technology might enhance the operation of their organizations. They may be able to choose the best employees based on these criteria.

Hsu and Lin (2016) CC services provide numerous benefits to enterprise clients, including lower prices, easier maintenance, and the ability to re-provision resources with ease. These factors enable improved revenues. Unfortunately, there is a lack of data regarding how businesses use these types of services. The technology-organization-environment technique is utilised in this research to examine the elements that influence choice to employ CC services. Numbers derived from 102 legitimate Taiwanese businesses lend credence to idea. The findings Technological (i.e., relative advantage, observability, and security), organisational (i.e., financial costs and satisfaction with existing IS) and environmental (i.e., competition intensity) elements all have a positive effect on the intention to use CC services. These accounted for 52% of the variance. Considerations of potential consequences and constraints are addressed.

Raut *et al.* (2018) find out what factors influence private companies in India to use CCA services, and then to suggest a method called SEANIS, which is a hybrid of "Structural Equation Modelling" (SEM), "Artificial Neural Network" (ANN), and "Interpretive Structural Modelling" (ISM). This study's results suggest that risk analysis and the perception of IT security risk may be added as new factors to "Technology Organisation Environment" (TOE) model. Using SEM and ANN methodologies, the data collected from the experts in the area was analysed. The results of SEM investigation revealed that the variables "trust," "management style," "technology innovation," "risk analysis," and "perceived IT security risk" (PITR) had a substantial effect on CCA. The SEM data was utilised to train the ANN and ISM networks. Trust, management style, and perceived danger to IT security were the most important factors identified by ANN as driving CCA. On the other hand, the ISM tool identified five critical factors out of 43: a decrease in internal systems availability (F1) in the PITR cluster, the use of internal resources (F14) in the MS cluster, the assurance of data privacy increasing adoption rate (F16) in the T cluster, innovativeness (F21) in the PIT cluster, and prior experience (F22) in the TI cluster. To let decision-makers and policy-makers easily evaluate their

organization's goals and choose the best computing environment to improve their performance, the hybrid method is expected to provide useful results.

Alharbi, Atkins and Stanier (2016) CC is a new model in information technology that is changing numerous industries throughout world. Despite CC's prominence as a new technology, very little is known about its use in Saudi Arabia's healthcare system. This research looks at the healthcare organisations in Saudi Arabia and finds out what factors would affect their use of cloud computing. The study integrates "Technology-Organization-Environment" (TOE) framework, "Information System Strategic Triangle" (IS Triangle), and "Human-Organization-Technology" (HOT-fit) model to provide a thorough evaluation of the aspects impacting healthcare organisations' adoption of CC. This study ranked the five viewpoints—Business, Technology, Organisational, and Environmental—in descending order of importance. The Human perspective came in last. The study found that the five most important factors influencing the adoption of CC in this setting are relative advantage, hard financial analysis, attitude towards change, soft financial analysis, and pressure from business ecosystem partners. This study delves into the important elements that academics and practitioners in Saudi healthcare consider before deciding to utilize CC.

Weerd, Mangula and Brinkkemper (2016) studied the organizational aspects that led to the implementation of "software as a service" (SaaS) by businesses in Indonesia. They found three trends after analysing data from 18 different Indonesian businesses in a multiple-case study: Adoption of SaaS is facilitated by the backing of upper management; SMEs are more inclined to do so than large organizations; and organizational readiness is not a prerequisite for SaaS adoption. The latter two trends go counter to what is already known about how people embrace new forms of IT. They break it down by looking at what makes Indonesia a developing nation and what SaaS is as an innovation in IT.

Hashim, Hassan and Hashim (2015) One innovative technology that has arisen in current years is CC. Research in the fields of business and literary reviews has largely concentrated on this topic. Examining and cataloguing the elements that impact CC adoption is the goal of this study. Business organisations, educational institutions, end

users, and IT professionals' points of view were the four primary foci of the research. Our search yielded 25 papers published between 2010 and 2015 from a pool of 81 articles covering this topic. The factors that the researchers have utilized were analyzed using a frequency distribution. The outcomes showed that relative advantage, compatibility, complexity, usability, and utility were the most critical criteria, followed by security and privacy. In terms of CC adoption research, the top four theories were TAM, Diffusion of Innovation, TOE, and the Unified Theory of Acceptance and Use of Technology.

Alkhater, Walters and Wills (2018) The use of CC is in its infancy in many developing nations, including Saudi Arabia. The motivations behind private companies' decisions to use CC are focus of this study. To better understand the organization's decision to use cloud services, this study proposes an combined model that takes into account both the essential criteria identified in the literature analysis and other, as-yet-unexplored ones, such as physical location. Data was collected from 100 IT staff members in different private sector companies in Saudi Arabia to assess the cloud adoption model and study the aspects positively and negatively associated with cloud adoption. Trust and service quality were found to be the two most important elements impacting cloud adoption. However, many in this nation are still hesitant to use the cloud because of privacy and security worries. The influence of these factors varied across adopter and non-adopter firms, as well as across different organizational sizes, as demonstrated by this study. In sum, the results of this study throw light on important questions for cloud service providers, administrators, and policymakers in the Middle East, with a focus on Saudi Arabia, including how to best promote and facilitate the expansion of CC across the region.

Sharma *et al.* (2016) An innovative new approach to information technology, CC has emerged as a game-changer in the realm of network applications. This research aims to create a hybrid model that can foretell the factors that will encourage IT workers to use cloud computing services. By adding three extrinsic variables—computer self-efficacy, trust, and employment opportunity—to TAM, the study suggests a novel paradigm. This study makes a significant contribution by introducing a new construct called "Job

Opportunity" (JO) to a technology adoption study. This is a first. The data was analysed using "neural network" (NN) and "multiple linear regression" (MLR) after being obtained from 101 IT professionals. Results showing "reduced mean squared errors" (RMSEs) indicate that NN models perform better than MLR models. Perceived utility, trustworthiness, ease of use, and job opportunities were among the factors that MLR found to be significant. Job opportunities, trust, perceived utility, self-efficacy, and perceived ease of use were found to be top predictors of CCA, according to the NN models. When investigating a relatively new technology, such as cloud computing, this study's results show that the basic TAM needs to be expanded. Academics, researchers, government organisations, IT service providers, and professionals in the field will all benefit from the study's findings.

Senarathna *et al.* (2018) The term CC refers to a relatively new paradigm in computing that allows businesses to rent highly professional computer resources over the Internet. It enables SMEs to join the ranks of larger companies in terms of technological sophistication without incurring huge costs. In this research, they looked at what matters most for SMEs seeking to use cloud computing. Researchers drew on ideas from “Diffusion of Innovation Theory” (DIT) and TOE framework to create a model of CCA by SMEs. They then put this model to the test by surveying 149 SMEs online in Australia. After applying multiple regression methods to the data, we found that factors about SMEs' organisational capabilities (e.g., advantage, relative, quality of service, and awareness) had a greater impact than risk-related factors (e.g., privacy, security, and flexibility). Government agencies, cloud service providers, and owners of SMEs can all use the results to inform CC adoption strategies.

Al-rawahna, Hung and Chen (2018) determine the level of readiness of the Jordanian government to utilize CC. Empirically applying the TOE research paradigm, the study surveyed 132 participants across three groups, including IT managers and IT professionals from different Jordanian organizations. Because the sample size was so small, the data was analyzed using Partial Least Square. The results showed that government organizations are prepared to implement CC based on top-down support,

organizational capabilities, and government policy. The results of the multigroup analysis showed that, despite differences in company size, the factors driving CC adoption are consistent across all of the groups. While familiarity with the cloud has no bearing on adoption intent, IT-related experience does. The study emphasised the need for decision-makers to be aware of organization's preparedness before making the adoption choice to avoid falling into the CC trap. Some practical evidence was found in the study. For example, government organizations need to be ready to adopt CC so they can reap its benefits. Strong IT skills and infrastructure are also crucial for government organisations to be ready. Top management support has a positive effect on organizational readiness, which shows that top managers are responsible for the success of new technology adoption. Government policies that are supportive of organizations' readiness can help convince agency managers to approve the transition to CC and allocate necessary resources.

Gangwar, Date and Ramaswamy (2015) This research aims to help organisations adopt CC by integrating TAM model and TOE framework. It was proposed that environmental factors directly affect adoption of CC, and a conceptual framework was developed using organisational and technological variables from the TOE framework as external variables of the TAM model. Data was gathered from 280 organizations in India's IT, industrial, and financial sectors using a questionnaire. Utilizing both exploratory and confirmatory factor analyses, the data were examined. Aside from that, the suggested model was tested using structural equation modelling. According to the study, some important factors, such as relative benefit, compatibility, complexity, organisational preparation, top management commitment, and training and education, affect the adoption of CC. It was determined that "perceived usefulness" (PU) and "perceived ease of use" (PEOU) were mediating factors. There was a direct correlation between the desire to use CC and factors such as competitive pressure and the support of trading partners. About 62% of CC adoption may be accounted for by the model. When businesses want their CC adoption to be successful, they can utilise this model as a roadmap. To create an atmosphere that is favourable for the use of CC, it also offers

pertinent recommendations. To make a more accurate prediction, this study combines two models of IT adoption.

AlBar and Hoque (2019) A sea change has occurred in the field of information technology with advent of cloud-based "enterprise resource planning" (ERP) platforms. Any kind of business can benefit from its configurable data, scalability, adaptability, cost-efficiency, and flexibility. All around the globe, this system has been booming. Little is known about the state of cloud ERP adoption in growing Middle Eastern nations like Saudi Arabia, where the trend is only beginning. This study examined the factors influencing the adoption of cloud ERP in Saudi Arabia by combining DOI theory with TOE framework. The study found that the adoption of cloud ERP was unaffected by compatibility, organizational culture, and trialability. The impact of parameters such complexity, relative advantage, ICT expertise, regulatory environment, observability, and support from senior management was significant ($p < 0.05$). In addition to helping Saudi Arabia, other developing nations in a similar position can use the study's findings to plan for and implement cloud ERP services.

Liu *et al.* (2018) revolutionized the way information technology is paid for and improved a company's agility with its pay-as-you-go model. However, there hasn't been much research on this topic, and what little there is about how CC affects organizational agility is murky. Based on survey responses from Chinese Alibaba cloud users, this study seeks to understand how CC relates to organizational agility. Structural equation modelling with Smart PLS 2.0 based on "partial least squares" (PLS) is used to conduct the empirical analysis. They argue that for businesses to become more agile, two features connected to CC—CI flexibility and CI integration—are essential. They examine how IT spending on CC acts as a moderator based on the IT—agility contradiction. The theoretical and practical aspects of CC can be better understood with the help of this study.

El-Gazzar, Hustad and Olsen (2016) provide the findings of a Delphi study that aimed to determine the most important factors that companies consider when determining if they should use CC. They brought together 34 specialists in the field to form a Delphi

panel. Experts in information technology and cloud computing from a variety of backgrounds (customers, providers, and academics) made up the panel, which was split into three sections. Brainstorming, refining, and ranking were the three steps that made up the Delphi technique. Security, legal, strategy, and culture, awareness, migration, availability, ethical, business, IT governance, and influence were the 10 groups into which the 55 issues that the panellists identified in the first stage were analysed and classified. There was a moderate level of agreement throughout the subpanels after ranking the top 18 issues. To have a better grasp of the concerns and the relative importance of each, 16 follow-up interviews were carried out with the specialists. According to the results, the top three concerns are strategy, legal and ethical considerations, and security. As a consequence of the group's deliberation, a framework outlining the factors that encourage and discourage CC adoption was developed. The study concludes with important recommendations to help decision-makers with CC adoption, with a focus on competence, maturity, and change management.

2.4 Environmental Factors Influencing Cloud Adoption

Gutierrez, Boukrami and Lumsden (2015) utilized TOE paradigm to identify basics that influence UK managers' decisions to use CC. A total of 257 business and IT professionals from various end-user businesses in UK, ranging from mid to senior-level decision makers, filled out a self-designed questionnaire survey. Principal component analysis and logistic regression were among the data analysis methods used to assess the resulting hypotheses. The decision to use cloud computing services in UK is influenced by four of the eight criteria that were examined. Among the most crucial factors are the following: complexity, technical preparedness, trading partners, and competitive pressure. The most important factor influencing an organization's choice to embrace cloud services was the level of pressure from trade partners due to concerns about legal restrictions, co-creation and customization, service linkage, and vendor locking, which makes choosing the right vendor more difficult. According to the results, managers are significantly influenced by their business partners, namely cloud service providers, when deciding to use cloud services. However, given increasing number of vendors in the

market, additional research is necessary to thoroughly comprehend all the factors at play. Not enough replies were collected from each industrial sector or organisation size to do further analysis, even though over 250 valid responses were received and evaluated. The results show how important it is for cloud service providers to assist end users in making better CC assessments. Businesses are starting to use CC services, which provide cheaper and more flexible IT resources, to assist their growth, even without the approval of upper management.

Asadi et al. (2017) The rise of CC has altered the Internet's function for numerous companies and groups. To meet their diverse needs and establish a banking environment that can swiftly react to new business requirements, banks are currently embracing cloud technologies at an increasing rate. Nevertheless, prior research has mostly ignored the consumers' point of view in favour of examining CC adoption challenges from an organisational standpoint. Therefore, this study's goal is to develop an adoption model for CC and investigate, from the perspective of the clients, the variables influencing its acceptability in banking sector. It is based on "TAM-diffusion theory model" (TAM-DTM) and adds three additional constructs: trust, cost, and security and privacy. Questionnaires were randomly sent to 162 Malaysian bank customers. SmartPLS was used to test hypotheses and validate the suggested structure, and PLS method was used to evaluate survey data. Based on the findings, it appears that the TAM-TDM may effectively incorporate trust, cost, security, and privacy. Perceived usability, perceived utility, and trust were all positively impacted by the privacy and security constructs. Researchers discovered that consumers' behavioural intention to use CC was significantly influenced by their perceptions of user utility, perceived cost, perceived ease of use, trust, and cloud attitudes. The results of this study will help financial institutions better understand their customers' views on cloud-based apps and how they feel about using them.

Senyo, Effah and Addae (2016) examined the factors that influence CCA in developing nations using TOE paradigm. According to a quantitative research technique, the study was carried out by surveying 305 businesses in Ghana across several industries.

Based on a conceptual model put out utilizing the TOE framework, ten hypotheses were examined using logistic regression analysis and confirmatory factors. The findings indicate that relative advantage, security concern, top management support, technological readiness, competitive pressure, and trade partner pressure are among the TOE characteristics that were shown to be important in CCA in a developing country setting. Interoperability, corporate scale, scope, regulatory support, and similar criteria were shown to be non-factors. CCA in a developing nation context is explored in this work, which adds originality and value. Specifically focusing on Ghana, the study may be the first of its kind to do empirical research into CCA in a developing nation setting. Given cloud computing's relative youth in the developing world, this study's results lay the groundwork for future research and offer useful insights on the technology's future.

Priyadarshinee, Raut, Jha and Gardas (2017) After telephone, gas, electricity and water, CC is regarded as the fifth utility. Similar to other utility services, social computing services are accessible whenever needed. The objective of the project is to develop a hybrid two-stage SEM-"artificial neural network" (ANN) model that can pinpoint the factors impacting Indian private organizations' adoption of cloud computing services. For the first time in technology adoption research, this study introduces a new paradigm by expanding TOE with external components, notably perceived IT security risk and risk analysis. The addition of additional factors, such as perceived IT security risk and risk analysis, is one of study's primary contributions. SEM and ANN modelling were used to collect and assess data from 660 professional experts. According to the SEM results, the adoption of CC is significantly impacted by PITR, RA, TI, MS, and T. The adoption of CC was statistically unaffected by technology (UT) and industry (IU), the only exceptions. Additionally, an ANN model was trained using SEM data, and findings showed that the three most significant predictors of CC adoption were "trust," "perceived IT security risk," and "management style."

Singh, Jeong and Park (2016) Through the Internet, CC can deliver customers more adaptable, cost-effective on-demand services. A major barrier to the new vision of computing capabilities that is emerging is security, which is preventing us from moving

towards on-demand services, resource pooling, and a distributive environment. This poll covers all the bases when it comes to the security issues plaguing CC. Embedded systems, applications, storage systems, clustering challenges, and a host of other important topics will also be thoroughly covered. Authorities in both public and private clouds, along with associated security issues, are the primary subjects of this research. A three-tier security architecture is also provided, along with requirements for effective security management. New security concepts and suggestions are covered, along with open issues.

Jianwen and Wakil (2019). Organisations nowadays can't help but notice the meteoric ascent of IT strategies like CC. The advantages of the cloud environment, such as more innovation, flexibility, and cost reductions, cannot be ignored. Therefore, assessing the factors impacting CCA is the major subject. This study aims to provide light on factors that impact CCA and its advantages for businesses. A research framework including four assumptions was developed in light of previous study results. The structural equation modelling method was used to examine the data. The findings provide credence to suggested model. In addition, the results show that four factors impact CCA: humans (with indicators of knowledge and innovativeness), organisations (with indicators of size, adequate resources, and support from upper management), technologies (with indicators of compatibility and security), and environment (with indicators of regulatory pressure, competitive pressure, and trading partners). The results will aid researchers, administrators, and ICT providers in creating more effective strategies for CCA, which is a major consequence of the study. Providers of services can benefit from the suggested method by learning why certain industries embrace the cloud's perks while others, with comparable market conditions, refuse to. In addition, to dispel any uncertainty about this technology and provide a well-organised environment for CCA, the aforementioned providers should strengthen their ties to the service sectors that have enhanced the CC experience. In addition, only respondents from Iran are included in the sample. Research studies on the use of CC have revealed its effects on organisations today. In addition, the various effects of CC on other situations and organisations are under consideration.

Organisations may benefit significantly from carefully assessing and controlling CCA logics. Earlier research has focused on CC's technological and operational difficulties. Some surveys have described the adoption of CC by organisations in terms of human qualities or contextual factors. As a result, a model and outline should be developed to measure the impact of the aforementioned elements on CCA.

Scholtz, Govender and Gomez (2016) CC may assist nations and enterprises in many ways. However, there are environmental and technological limitations that might make it difficult for underdeveloped countries to adopt these technologies. The purpose of this study is to find out how common these components are in the public sector in developing countries such as South Africa. A comprehensive review of literature revealed some characteristics that affect the adoption of CC, which a survey approach was used to evaluate empirically. Fifty-one respondents from forty South African public sector entities completed the survey. According to the results, majority of respondents expressed concerns over data privacy and access. The most crucial environmental factors for CC installations, according to respondents, are adoption strategies, followed by use rules and organisational regulatory requirements.

Isa *et al.* (2020) Research on factors that influence CCA in higher education institutions is limited. The institution, however, does not fully grasp the nature of the CCA challenges. Researching what influences CCA in a university setting is the main objective of this study. One case study at a public university in Malaysia and qualitative interviews with key stakeholders made up the research methodology. Analyses were carried out utilizing Atlatl. The eighteen parts can be divided into three groups: technical, organizational, and environmental. In sum, these are only a few of the factors that could influence whether or not a public institution chooses cloud computing. First, there is the technological category, which includes nine factors: (i) relative advantage, (ii) cost reduction, (iii) ease of use, (iv) compatibility, (v) operational needs, (vi) security, (vii) sustainability, (viii) trialability, and (ix) complexity. Section two, "organizational," consists of the following four elements: (i) prepared infrastructure, (ii) senior leadership, (iii) expertise in information technology, and (iv) funding. Five components make up the

environmental category: (i) the cloud service provider, (ii) location, (iii) data privacy, (iv) policies and guidelines, and (v) service level agreement. Research in this area has the potential to inform CCA practices in the mobile learning and computing sectors. It is planned to conduct comparable investigations in other case studies in the future, encompassing both public and private institutions in Malaysia.

Sandu and Gide (2018) Cloud-based services are widely employed by organisations, particularly SMEs, due to their numerous benefits. SMEs are regarded to play a vital part in any country's economic growth. They are in charge of reducing poverty, developing rural areas, creating job opportunities, fostering entrepreneurship, and growing national exports. SMEs lack the resources to implement new technology to improve their business performance. However, various characteristics encourage these businesses to use CBS. These studies concentrated on TOE aspects that influence the implementation of CBS in various businesses. Given the relevance of Cloud-based technology to SMEs, the study seeks to classify factors influencing the adoption of CBS in Indian SMEs.

Narwane *et al.* (2019) apply exploratory and confirmatory factor analysis to determine key parameters impacting adoption of "Cloud of Things" (CoT) by SMS organisations in India. Approach, methodology, and design To find important factors impacting the application of CoT, a thorough literature review was carried out. The essential factors that were found include things like cost savings, relative advantage, sharing and collaboration, reliability, security and privacy, technological challenges, and adoption purpose. To connect these things, a conceptual framework and certain hypotheses were proposed. This study used an online survey to collect data from 270 SMEs in India. A SEM was used to test the suggested solution. Conclusions - Factors including "sharing and collaboration," "cost savings," and "relative advantage" were found to positively impact the installation of CoT. The results of the study further supported the theory that "security and privacy" were the primary motivators for the adoption of CoT. Potential pitfalls and consequences of the study: When gathering qualitative data, it can be helpful to have a representative sample from a variety of

geographic areas. Considering that SEM methodology is limited to checking linear connections, a hybrid strategy that incorporates artificial neural networks and multiple linear regression can be used to overcome this.

Gide and Sandu (2015) delve into the elements that impact the adoption of cloud-based services by Indian SMEs. Through an exhaustive literature review, this study investigates the current situation, advantages, and disadvantages of CBS adoption by SMEs in India. Based on secondary data, it confirms and defines the key factors (such as relative advantage, security, regulatory support, firm size, support from upper management, and technological readiness) that impact the adoption of cloud-based services by SMEs in India. SMEs in India that utilise or are thinking about using cloud-based services are the focus of this research. Principles of both DOI and TOE theory form the basis of this investigation. The two theories of technology adoption offer a solid theoretical foundation for this research. The usage of cloud-based services by SMEs in India is examined in this study to determine the extent to which innovation characteristics, technological context, organisational context, and environmental context impact this decision.

2.5 Impact of Geographical Location on Cloud Computing Accessibility

Yang *et al.* (2017) With the advent of Big Data, new opportunities have arisen in the fields of R&D, innovation, and industry. Its "four Vs"—volume, velocity, veracity, and variety—set it apart, and Big Data processing might give it tremendous value. A major issue with processing capacity arises when Big Data's four Vs are expanded to include a fifth (value). To address different processing needs, cloud computing has emerged as a new paradigm for delivering computing as a utility service. It does this through a) on-demand services, b) pooled resources, c) flexibility, d) broadband access, and e) quantifiable services. One possible way to add a fifth V to Big Data is through the practical use of computational capabilities. This research delves at the potential of CC to address Big Data issues and pave the way for this kind of transformation. They present and go over four examples of geospatial science: dust storm modelling, land cover simulation, climate studies, and geographic knowledge mining. To help you use CC for

Big Data solutions, we've laid out the process in a tabular manner. The four cases show how the method of the framework helps with all stages of Big Data processing, from management and access to mining analytics, modelling, and forecasting. Potential answers to other significant spatial data challenges and projects, such smart cities, can also be mapped out using this tabular structure.

In the realm computers, Kumar, Raj and Jelciana (2018) CC is among the most rapidly developing technology. CC has limited security risks and many benefits. CC in a multi-tenant context presents unique data security challenges, which this paper investigates and offers solutions to. Research in this area also details several models used in CC, including those for deployment and service delivery. The loss of trust in a company or CC service as a result of data leaks or corruption can be fatal to the enterprise. Countless companies rely on CC in some way, shape, or form; any data breach affecting CC would have repercussions for both cloud and the company's operations. This is why data security is becoming an increasingly important focus for cloud computing organisations.

Sabi *et al.* (2016) CC has revolutionized the way computer infrastructure and services are delivered. CC studies conducted recently have focused on questions raised by SMEs regarding the technology, applications, cost, benefits, and security of CC. There has been a dearth of scholarly discussion on the role of context in implementation and usage of cloud computing in schools. Universities in poor countries are unable to invest in expensive information systems that are essential for global competitiveness due to challenging social, economic, and political constraints. The model presented here takes into consideration cultural, economic, and technological aspects in the perception and adoption of CC at sub-Saharan African colleges. This model borrows heavily on theory of innovation diffusion and technology acceptance paradigm. The instrument's reliability and validity were demonstrated in pilot research that surveyed university lecturers and IS experts; the results lend credence to its use in a larger-scale investigation. The discussion centres on the implications, possible contributions to the field, and recommendations for further research.

Subramanian and Jeyaraj (2018) The term CC refers to a generalised model for on-demand, or pay-as-you-go, access to a shared pool of computational resources. CC offers operational and financial advantages to both individuals and organisations. Despite these benefits, CC is nevertheless constrained by some issues. They constantly keep security in mind as a top priority. In the absence of this crucial component, the computing archetype has a negative effect, leading to harm on a personal, ethical, and economic level. The difficulties that cloud entities have in terms of security are the primary topic and investigation of this paper. Everyone from the cloud provider to the data owner to the end user is part of this ecosystem. Paying special attention to the crypto-cloud, which includes various CCAs (Communication, Computation, and Service Level Agreements). It will deliver the required improvements after studying causes and effects of different cyber assaults.

Hassan *et al.* (2020) The widespread influence of CC on human productivity is immense. Computing, storage, intelligent decision-making, and prediction are just a few of its modern applications. The use of Machine Learning for Intelligent Decision-Making has increased the demand for faster, more reliable, and more accurate Cloud Services. Cloud security is still a big deal, but there are a lot of other problems with cloud adoption that need fixing, like poorly managed service level agreements (SLAs), frequent disconnections, insufficient resources, privacy concerns, and unreliability. The security issues that are emerging from the broad use of Containers for cloud deployment still require a tremendous lot of investigation. They go on to talk about cloud computing's impact and cloud standards. The study paints a detailed picture of cloud computing, covering all the bases from its fundamental ideas and architectural principles to its essential services and the difficulties inherent in developing, deploying, and implementing it. In this age of data science and ML, it also pinpoints crucial areas for further study.

Amoore (2018) CC’s architecture is getting more and more entangled with geopolitics, from intelligence immigration determinations, data sharing to border controls and drone strikes. The study delves into the geography of CC by drawing a comparison to

cloud chamber of early twentieth-century particle physics. The study compares two different models that deal with the spatial aspect of CC. The first, "Cloud I," also known as a geography of cloud formations, focuses on pinpointing the exact geographic locations of data centres that are believed to house the cloud. In this context, the cloud is made sense of inside specific annals of observation, annals that allow the seemingly nebulous and evasive universe to be seen and made sense of. For the second iteration, "Cloud II" or "geography of a cloud analytic," the cloud is a collection of experimental algorithmic methods that operate at the very edge of perception. The goal of modern CC, similar to that of the cloud chamber in the 1800s, is to make visible and actionable things that would be impossible to discover otherwise. Condensing traces, detecting patterns, and archiving future are the three components of correlative cloud reasoning that study suggests, all of which have geopolitical modern relevance.

Opara-Martins, Sahandi and Tian (2016) Due to the absence of standards, vendor lock-in poses a significant threat to extensive use of CC. The majority of the current approaches and solutions to the vendor lock-in problem focus on technology. There is a dearth of research that attempts to dissect cloud vendor lock-in problem and shed light on its complexity. Consequently, when it comes to companies' proprietary standards, the majority of customers have no idea how they limit application portability and interoperability. From a business point of view, this research examines the vendor lock-in issue and offers a critical critique. The primary risk factors that lead to lock-in situations were discovered by a survey that utilised both qualitative and quantitative methodologies. Our poll of 114 people reveals that the trend towards moving computer resources to the cloud is making vendor lock-in a bigger issue. The results also show how crucial CC standards, interoperability, and portability are. To prevent or lessen the impact of lock-in issues associated with moving to the cloud, several approaches have been suggested. Contracts, suppliers that provide standardized data structures and APIs, and raising awareness of cloud-based solutions' commonalities and dependencies are all part of the plans. Their conviction in these measures' ability to lessen vendor lock-in risks is unwavering.

Varghese and Buyya (2018) A lot has changed in the world of cloud computing in the last ten years. Aside from an increase in the number of service providers and services available, the cloud is also evolving away from a model where data centres are owned by a single provider. Part one of this study covers the changing cloud infrastructure, covering topics such as the benefits of decentralising computing away from data centres and how users make use of infrastructure from different providers. A variety of much-needed novel computer designs will be made available by future cloud infrastructure as a result of these tendencies. Many industries stand to benefit from these innovations, including data-intensive computing, self-learning systems, the service industry, and the connectivity of people and objects. Final step: they lay out the problems that need fixing before next-gen cloud systems can reach their full potential.

2.6 Perceived Risks and Barriers to Cloud Adoption

Khayer *et al.* (2020) looks into what factors influence the decision to use CC and then evaluates effects of CC on effectiveness and productivity of SMSs. By integrating SEM with neural networks, they have implemented a two-stage analytical procedure to evaluate the predicted model. The decision to use CC depends on some factors, including comparative advantage, service quality, perceived risks, backing from higher-ups, enabling conditions, cloud providers' influence, server placement, computer self-efficacy, resistance to change, and so on. The positive influence of CC on company performance is further supported by the study's results. Managers should prioritise actions that increase top-level buy-in, perceived risk, and relative benefit, according to "importance-performance map analysis" (IPMA). Aside from that, according to neural network analysis, the following factors are the most important in determining whether a company will use the cloud: server location, relative advantage, service quality, support from upper management, computer self-efficacy, perceived risks, interference from cloud providers, and resistance to change. They conclude by discussing research's implications, which might be useful for cloud providers, lawmakers, owners/managers, and researchers in understanding what factors SMEs consider when deciding to utilise CC.

El-Haddadeh (2020) Organisations can now generate possibilities to bolster their competitive advantage thanks to digital innovations. Therefore, it is crucial to the success of these technologies to understand the dynamics that impact their adoption. The invention, deployment, and acceptance of technology by employees have received a lot of attention, but how digital innovation impacts technology uptake in businesses has received less attention. This study takes a look at how innovation dynamics implementation in cloud affects SMEs, using the Technology Organisation and Environment paradigm. The results from the survey of IT and senior managers show that when it comes to SMEs and their chances of using CC, factors such as perceived innovation risk, organisational innovativeness, and perceived innovation barriers play a larger role than IT innovation-driven competitiveness. Therefore, this shows how providing the necessary assistance for SMEs to maintain success can be achieved by understating the details of innovation dynamics.

Sallehudin *et al.* (2020) Cloud computing offers businesses the chance to make use of scalable, agile, and reasonably priced technology. Nevertheless, despite cloud computing's proven benefits, businesses have been slow to embrace these technologies. This study offers an empirical investigation aimed at improving comprehension of cloud service adoption, based on a multi-theoretical research approach. An online survey was performed to address the criteria identified from the literature for three specific common cloud application types (cloud storage, cloud mail, and cloud office). The study model was analyzed using variance-based structural equation modelling. According to the findings, compatibility, relative advantage, security and confidence, and a lower level of complexity all contribute to a more positive attitude towards cloud adoption. Relative advantage is impacted both directly and indirectly by complexity, compatibility, image, security, and trust. These elements also account for a significant portion of the attitudes on cloud adoption, but not its use.

Kim, Jang and Yang (2017) Instead of creating their information systems, CC is a cutting-edge IT that uses external suppliers to supply computer resources and services. One CC paradigm, SaaS, is useful for improving business operations and supporting

small businesses' IT skills because it is based on an innate best business practice. The factors that affect Korean small enterprises' intentions to use SaaS were examined in the study. The results showed that (1) they were more concerned about security risks than economic or performance risks, (2) they were trying to improve business processes instead of quality or cost, (3) they thought that management support was more important than IT capacity or resources for adoption of SaaS, and (4) they also thought that vendor support was more important than government support. The study's findings will offer useful tactics to small businesses thinking about implementing SaaS, SaaS vendors, and the government when establishing regulations.

Palos-Sanchez, Arenas-Marquez and Aguayo-Camacho (2017) conducts an empirical analysis of elements that influence CC, SaaS model adoption in businesses where this approach is deemed strategic for carrying out their operations. The factors that influence the intention to use CC have been evaluated using a research model that combines the variables from TAM with extra external variables such as communication, training, top management support, organisation size, and technological complexity. 150 Andalusian (Spanish) firms' worth of data is used to test the theories. The study's results show the crucial factors to consider and how they are interrelated. They also illustrate organisational requirements that businesses hoping to adopt a true management model for the digital economy—particularly those about cloud computing—must take into account.

Lynn *et al.* (2018) The complex realm of "high-performance computing" (HPC) still largely lacks knowledge about the factors driving technology adoption decisions. This study extends the DOI and "Human-Organisation-Technology fit" (HOT-fit) theories into an integrated model to examine the impact of ten factors on CCA decisions in the HPC scenario. The findings show that adopters and non-adopters have differing perspectives on cloud computing's compatibility for HPC, resource sufficiency, top management support, and indirect benefits. Furthermore, perceptions of the indirect advantages and HPC competencies can be used to forecast the choice to adopt CC for HPC. This is one of the first studies in the IS literature to look at the factors influencing the decision to employ CC in the important setting of HPC. It integrates two significant

theories of technology adoption and advances understanding of key factors influencing companies' choices to employ CC in this context.

Priyadarshinee, Raut, Jha and Kamble (2017) analyze the criteria' reliability, structure, and validity in the context of SME industry to determine which elements and crucial success criteria influence the implementation of CC. This study employs a ranking model that considers nine different categories of criteria/factors with fifty-one sub-criteria to assist decision-makers in assessing the effectiveness of CCA in the past. A questionnaire-based survey study was used to gather information from 110 businesses in India's SMEs sector. In this study, the collected data was analysed using an integrated manner. The Analytic Hierarchy Process was employed to identify the key elements of each criterion as quantifiable markers of CCA. Second, the criteria' validity, reliability, and structure were investigated using Exploratory and Confirmatory Factor Analysis. Before being imported into “Statistical Package for Social Sciences”, (SPSS version 20), data was tabulated in a Microsoft Excel sheet. Results showed that factors including "Confidentiality," "Sharing and Collaboration," "Organizational Risk," and "Integrity" significantly impact cloud computing adoption. There may be limitations to the findings' generalizability due to the research's focus on the SMEs industry in India. Customers and CC service providers can both gain from the findings and recommendations by developing a more sophisticated understanding of the elements impacting CCA in current context. By applying some criteria, the study contributed to the adoption of CC as a new technology in India's SME sector. Businesses can also utilize the findings to better assess "return on investment" (ROI) of their IT investments in CC.

Jones *et al.* (2019) To take advantage of CC many benefits and decrease their overall investments in IT infrastructures and resources, government agencies have been moving to cloud-based services. There are, however, worries about hazards of adopting CBT, as there are with any other technological investment. Government authorities and others need to conduct exploratory research to address these problems and fill the gap in academic literature on cloud computing from a governmental perspective. This would help reduce costly blunders. Consequently, this research looks at three UK LGAs' cloud

computing implementations from a practical and organisational user standpoint. The researchers map perceived reward and risk indicators using qualitative case study queries against the literature to find emergent features. Variable results from three cloud installations included key advantages like better information management and more flexible work habits, as well as risks like loss of control and lack of data ownership. These results from aggregated organisational user views can be useful for studying cloud computing and its strategic application in the public sector.

2.7 Perceived Usefulness and Benefits of Cloud Technologies

Arpaci (2017) Achieving excellent academic achievement, efficacy, and efficiency requires efficient knowledge management. By implementing cloud computing in the classroom, knowledge management could be improved. The purpose of this study is to investigate the reasons for and consequences of the use of CC in education for knowledge management. Thus, this study provided participants with teaching and training while implementing CC in a real-world learning environment to improve knowledge organization techniques. At the beginning and end of the 14-week intervention, pre-and post-tests were given. This study looked at how expectations for knowledge management procedures relate to how beneficial cloud computing services are thought to be. The study additionally investigated the causal links among PEU, training and education, and innovativeness. The study model was verified by analysing survey data from 221 undergraduate students using structural equation modelling. The findings indicate that perceived utility and expectations for information generation, discovery, storage, and sharing are strongly connected. Among other things, the perceived utility is more strongly correlated with expectations for knowledge sharing and preservation. Additionally, evaluations of ease of use are strongly correlated with innovativeness training and education. According to findings, educational institutions should encourage the use of CC in the classroom by raising awareness of knowledge organization techniques.

Shiau and Chau (2016) Although CC has been integral to the rise of cloud computing classrooms, the precise nature of students' intentions about their behaviours

towards this novel information technology is still up for debate. Few hypotheses have been examined, integrated, or compared by most researchers in their examination of user behavioural intention. This study used six well-known theories—service quality, self-efficacy, motivational model, technology acceptance model, theory of reasoned action or theory of planned behaviours, and innovation diffusion theory—in context of CC, classrooms to test, contrast, and finally integrate their findings. Respondents to this empirical investigation filled out surveys that were accessible online. Analyzed utilizing structural equation modelling were data acquired from the samples (n=478). They broke out each idea and came up with a unified model after doing this. Three useful points emerged from the investigation. My first point is that the combined model, along with other five theoretical frameworks, provided sufficient explanations. In addition, the findings of Chi-square statistics, variance explanation, effect size, and predictive relevance showed how important theoretical models were. Thirdly, the integrated model clarified all the elements that have a major impact on how college students plan to act in a cloud computing course. Researchers and practitioners alike must pay close attention to the study's debates and consequences.

Wang *et al.* (2019) Especially in field of higher education, traditional e-learning methods are no longer adequate to satisfy the expectations of modernized learning processes in this quickly changing digital era. One way to make e-learning more adaptable, shareable, content-reusable, and scalable is to use cloud computing. There are a lot of Cloud e-learning frameworks out there, but not many studies look at what characteristics relate to usability and predict whether or not people will keep using these apps. “Computer Self-Efficacy” (CSE), “Enjoyment” (E), PEU, PU, and UP are the five usability criteria that were examined in this study. The presumption was that Continuance Intention (CI), the dependent measure, was positively correlated with each of the five independent variables. A poll was administered to one hundred seventy information technology majors at a private university in Malaysia. The Cloud e-learning program was made available to the students for one trimester so they could test it out. Using a questionnaire with thirty questions, we were able to assess the usability characteristics

that contribute to the intention to continue using the program. Data analysis was performed using SMARTPLS 3.0. While perceived utility, simplicity of use, and user perception were found to be negligible predictors of continuing intention, this study found that computer self-efficacy and satisfaction as intrinsic motives were strongly related. This finding suggests that students' ability to use and enjoy using cloud e-learning applications has a substantial impact on their desire to do so. Anyone interested in or involved with educational technology in higher education would do well to read this study and consider its comments and consequences.

Bello *et al.* (2021) Several sectors have been impacted by the revolutionary power of cloud computing technology for quite a while now. Despite the fact that these technologies have a lot of potential to benefit the construction industry, their adoption by the sector is happening at a snail's pace. As a result, this study highlights the current contributions and applications of CC in construction. Thus, 92 peer-reviewed publications from 2009 to 2019 served as the basis for their systematic review. One of the findings that stands out is the notion that CC makes it easier to introduce new technologies in the construction industry, including big data analytics, VR/AR, the IoT, and BIM. CC has many present and future uses in the construction sector, and this paper highlights some of those uses. The research also delves into the challenges that the construction sector faces when trying to implement CC and offers suggestions for how to overcome them.

Arpaci (2016) Because mobile devices have constraints in terms of processing power, storage capacity, and bandwidth, manufacturers and service providers have developed valuable and creative mobile services. As a solution to these limitations, mobile CC has developed into a service that offers platforms, software, and infrastructure on demand. This study's main objective is to build a better research framework based on TAM by determining what factors affect students' opinions on and intentions to adopt mobile cloud storage services. A structural equation model utilising data from 262 students was used to assess the proposed model. The results show that perceived utility, subjective norm, and trust all positively impact attitude, which is a powerful predictor of

behavioural intentions. The study model predicts 82% of the variation in attitudes towards mobile cloud storage services. Academics, administrators, and educational institutions can all benefit from the results, both in theory and practice.

Ooi *et al.* (2018) explores how manufacturing companies might use CC technology to improve their business performance and innovativeness. It looks at influence of "absorptive capacity" (AC), firm size (FS), "top management support" (MS)," performance expectancy" (PE), and "effort expectancy" (EE). They analysed data from 188 management roles using "partial least squares" (PLS), SEM and “Artificial Neural Networks” (ANN). According to the findings, they are aware that PE, FS, and AC have a positive and significant impact on IN, which in turn has a positive effect on FP. In keeping with Industry 4.0, next industrial revolution, this study offers helpful insights into how cloud computing may improve IN and FP.

Ramachandra, Iftikhar and Khan (2017) Spending on cloud-based security is predicted to rise by 42%, per a 2015 Forbes article. Another study found that by 2015, IT security spending had risen to 79.1%, indicating an annual increase of over 10%. According to a 2011 study by the "International Data Corporation" (IDC), 74.6% of business clients said that security was a significant concern. This paper compiles several peer-reviewed studies on CC security risks and mitigation strategies. Their goal is to comprehend the threats, security concerns, and components of the cloud as well as new developments that could lessen its vulnerabilities. Although it has been widely acknowledged since 2008 that the cloud is a feasible hosting platform, there is a belief that substantial security enhancements are need to achieve greater rates of enterprise-scale adaptation. Many of the problems with CC need to be fixed immediately, according to another study. Though the industry has made great strides in thwarting cloud computing threats, more work needs to be done to bring the technology up to the level of traditional/on-premise serving.

Al-Sharafi *et al.* (2019) Over the past decade, "Cloud-Based Business Services" (CBBS) has grown in popularity as a tool for companies to gain an edge in the market through better use of ICT services. Previous research has shown that

organisational performance can be negatively impacted by service inconsistency, which in turn reduces the effectiveness of ICT projects. Thus, this study intends to analyse the effects on both monetary and non-monetary benefits to regulate the connection between perceived benefits of cloud-based business services and their ongoing use. So, to test the measurement model and its associated theories, PLS-SEM was used. Four hundred fifteen SMEs across a range of industries in Malaysia make up the study's population sample. According to the study's findings, SMEs in Malaysia can't improve their organisational performance without consistently implementing CBBS.

Botta *et al.* (2016) Although they are extremely distinct technologies, cloud computing and the IoT are both present in their daily lives. As their usage and adoption continue to grow, they will play a important role in the Internet of Future. Many different kinds of applications could be made possible by a new paradigm that combines CC with IoT. The researchers here zeroed in on a concept they coined "Cloud IoT"—the merging of CC with the IoT. Separate literature reviews of Cloud and IoT have focused on its key features, attributes, underlying technology, and unanswered questions. The new Cloud IoT paradigm brings entirely new applications, difficulties, and research concerns; yet, these works do not, as far as they are aware, provide a comprehensive examination of these aspects. To fill this void, this study surveys the literature on Cloud and IoT integration. As a starting point, they examine the fundamentals of both IoT and cloud computing. Then, they talk about how the two are complementary and explain the factors that are forcing their integration. Many new applications are taking off as a result of widespread utilized of the Cloud IoT paradigm; this article summarizes the recent state of the literature on Cloud IoT applications and highlights the unique research obstacles faced by each. To reveal the present direction of the primary body of research, these obstacles are subsequently examined in depth. In addition, they go over the current state of affairs regarding open source and proprietary platforms, as well as initiatives that have adopted the Cloud IoT paradigm.

2.8 Role of Trust in Cloud Service Providers

Tang *et al.* (2017) Utilizing a variety of cloud services to construct dependable cloud apps has grown in popularity since the introduction of cloud computing. An important and pressing research subject is how to ensure the reliability of cloud services, as this is a major obstacle to the growth of cloud applications. While much research has looked at whether services are trustworthy by either QoS monitoring systems or user feedback ratings, very few have attempted to improve service trust evaluation by combining the two. The TRUSS framework is suggested as a reliable method for choosing cloud services in this research. Their goal is to provide TRUSS-compatible trust evaluation middleware, and they suggest an approach that combines subjective and objective trust assessments into one. Both the subjective and objective trust assessments rely on user feedback ratings and quality of service monitoring, respectively. Compared to the previous trust and reputation methods, our suggested solution performs far better in experiments run on a synthetic dataset.

Khan (2016) CC has become a popular paradigm due to the high quality, low cost, and better performance of the computing services it provides. CC has been popular because of its adaptable architecture, focus on the internet, and user-friendliness. However, the cloud computing paradigm is still failing to resolve security concerns, which is reducing its widespread utilisation and could worsen service quality and consumer data privacy. This study provides an overview of security challenges by outlining potential threats and solutions to those issues. The purpose of this contribution is to review the existing literature on security challenges and their potential solutions, and to classify the processes by which these problems operate. They assess the risks that cloud platforms are currently facing using a parametric comparison. In addition, they evaluate and contrast different frameworks for intrusion detection and prevention that are currently in use to deal with security concerns. Additionally, we examine trusted CC and methods for controlling cloud service providers' security compliance. Given the ever-changing nature of security systems, they also reveal where cloud security issues are headed and how to prevent them.

Alouffi *et al.* (2021) The study of CC has grown into a lucrative field for both academics and businesses. Users and "cloud service providers" (CSPs) alike reap the rewards of CC. There has been a lot of research on security issues with CC. Reviewing previous research on cloud computing security, dangers, and difficulties is goal of this "systematic literature review" (SLR). The studies published in popular digital libraries between 2010 and 2020 were the focus of this SLR. After carefully reviewing all published publications that could address the research questions, they settled on 80 studies. This SLR's findings revealed seven serious security threats to cloud services. According to the findings, data leakage and manipulation were two of the most talked-about issues in the selected literature. Additional security concerns related to data intrusion and storage in cloud were also discovered. Consumer data outsourcing is still an issue for cloud service providers and cloud users, according to this SLR's findings. According to their poll, blockchain technology can work in tandem with other solutions to address safety issues. To ensure privacy, authenticity, and accessibility of data, the SLR results provide several recommendations for future research.

Hajare *et al.* (2021) One of the most pervasive problems with IT is data security. Given that data stored in the cloud resides in various locations around the globe, becomes very important in this context. Users are concerned about data security and privacy when it comes to CC. CC has been the subject of extensive methodological scrutiny in both academia and business. As cloud computing technologies advance in business, government, and industry, data security and privacy protection will become more and more crucial. CC’s hardware and software components are all subject to privacy and security concerns. Examining different security tactics and issues from software and hardware components that contribute to cloud data security is the main focus of this study, which aims to improve data security and privacy protection for a reliable cloud environment. With this document, they are getting ready to behaviour a pertinent literature review on CC data security and privacy protection methods.

Tang *et al.* (2017) With the advent of CC, remote computing has become a commodity, and online collaboration has never been easier. However, they do demand

absolute faith from customers in the reliability, honesty, and accessibility of the service provider. This research presents VICOS, a protocol for verifying the consistency and integrity of cloud object storage, to minimise the goal of minimizing this reliance. VICOS allows a network of trusted clients to identify instances of data consistency and integrity breaches in a cloud object storage service. Service scenarios where numerous customers share data held remotely on a service that might be acting up are its targets. In comparison to earlier protocols, VICOS minimizes computation and transmission overhead, enables wait-free client semantics for most operations, and enforces the consistency idea of fork-linearizability. VICOS relies on a standard format for authenticated data. It also supports a real-world interface in addition to a simple abstraction, and its processes span the hierarchical namespace of a cloud object store. An evaluation shows that the VICOS prototype outperforms the current systems, and it is compatible with key-value store interface of commodity cloud storage services.

2.9 Conclusion and Recommendations for Future Research

Kamarudin *et al.* (2022) Managing human resources, payroll, finances, and accounting are all essential business functions for SMEs. Consequently, technology like cloud computing is anticipated to be advantageous for SMEs. It is still difficult for entrepreneurs running SMEs to switch to CC from their current methods of doing business. As a result, this research provides a concise overview of CC, including its principles, features, and the many models for deploying and providing cloud services. The report sheds light on the pros and cons of CC for entrepreneurs running SMSs. In addition, the research delves into current CC services that SMEs have access to. With this research, they hope to fill in some gaps in our understanding of how SMEs might benefit from cloud computing for operational management.

Hentschel, Leyh and Baumhauer (2019) A major factor propelling businesses towards digital transformation, CC is a rapidly expanding field of technology. Business management and IT departments must take a significant interest in and actively participate in the process of implementing and adopting an appropriate cloud service because it is complex, knowledge-intensive, and demanding. "Critical success

factors" (CSFs) for cloud application projects have received little attention from researchers, even though they are crucial for SMEs and other types of organisations looking to avoid project failures. Because of this, our work adds to existing body of knowledge by identifying 26 CSFs via a comprehensive literature analysis and an interview study with German SMEs. So, they divide up CSFs among all the people who would be working on cloud implementation projects using a thorough model they established.

Isma' *et al.* (2016) There are a lot of advantages that businesses may expect to reap from CC, including cost savings, improved business processes and services, and a jump in the competition. Despite the fast-paced evolution of technology, SME's adoption of CC is still on the sluggish side. The socio-technical factors impacting the decision of SMEs to embrace cloud computing are examined in this study, decision-support model based on the PAPRIKA multi-criteria decision-making approach is shown. Evaluating different cloud services and deployment models has become a big challenge because of the complex nature of CCA. This research provides a methodical framework for assessing various CC services and associated deployment strategies. As part of the decision-making process, they have collaborated with five decision-makers from SMEs to carry out conjoint analysis activities grounded in preset criteria. You can use the suggested model to evaluate and choose among various cloud services and deployment procedures.

Ruaro and Rabelo (2016) A well-known approach for helping SMEs take advantage of new sustainable models is "virtual enterprise" (VE). Enterprises form a VE when they work together online to accomplish shared objectives while dividing up resources and the associated risks and rewards. Having said that, ICT assets and infrastructures are not shared amongst VE members. A solution that can accomplish that is CC. Researchers have built prototypes and created cloud-based environments to address specific problems in specific VE scenarios. On the other hand, business owners and operators of SMEs should have a more nuanced understanding of how well commercial cloud computing solutions can satisfy routine VE requirements. The main

goal of this study is to accomplish that. They examined two commercial SaaS, PaaS, and IaaS technologies, and they defined the requirements of VEs and performance metrics to assess cloud solutions.

Haselmann and Vossen (2013) The cloud is sometimes portrayed as the panacea for all of SMEs' IT problems. Although cloud sourcing and cloud services have many promising benefits, many SMEs are not using them because of the high upfront costs of learning the required enterprise knowledge, investigating and screening possible cloud service providers, and comprehending the intricate legal issues surrounding the outsourcing of sensitive data. To solve many of the current problems, this research introduces the idea of hybrid cloud intermediaries. For background, they provide actual results from cross-national research of cloud implementation in SMEs. They explain the concept in depth and present possible variations, comprising an entire consolidated model of value-creation by cloud intermediaries from multiple perspectives. The authors then go on to discuss how SMEs might benefit from a hybrid cloud intermediary and propose cooperative paradigm-based governance structures to assist with cloud adoption. For SMEs interested in cloud sourcing, this article presents a detailed discussion of the resultant entity, or, more simply put, co-op cloud, a cooperative hybrid cloud intermediary, outlining both possible scenarios and constraints.

Kaur and Sharma (2017) CC has grown astronomically in the last few years. CC refers to on-demand or pay-per-use provision of resources such as storage, servers, and networks, all of which are necessary and are made available via the Internet. Although the IT sector is being placated by cloud computing, the field's development and research are still in their infancy. My contribution to this document is a thorough analysis that focuses on concept of CC and the most pressing issue. This study provides a better understanding of CC and identifies the main areas of research in this rapidly expanding field of computer science. The introduction is given in Section 1. An overview of CC is given in Section 2. The cloud manifesto's complications are discussed in Section 3. The load equalising techniques are the subject of Sections 4 and 5. utilised current load

approaches in sections 6 and 7, and section 8 compares them. Comprised of a comparison graph However, the conclusion and gap in the literature in sections 9 and 10 persuaded.

Laurindo, Kissimoto and Escorcia (2022) explores whether using SaaS in SMSs might improve organisational performance from the standpoint of knowledge management. The technique includes a literature assessment of ideas related to cloud computing and knowledge management practices, along with an examination of how they complement one another. According to the findings, SMEs can embrace new software SaaS for organisational performance in a sustainable way by adopting knowledge management techniques.

Zhao, Zhang and Zhao (2022) In the context of China's expanding market economy, SMEs have seized the chance to expand quickly. These days, SMEs play a significant role in market economy. The key to enhancing the management style of SMEs is increasing the amount of accounting information. Accounting systems are an advanced type of management. CC is used in this study about enterprise accounting management systems. The findings demonstrate how SME accounting information management can successfully enhance financial settlements. It is impossible to overlook the increase in accounting management efficiency brought about by the growth of CC. Businesses can mitigate risks associated with accounting informatisation by implementing stringent, appropriate rules and regulations and building a secure network protection wall.

Nguyen and Liaw (2022) Cloud computing is growing in popularity and offers businesses some advantages. Nonetheless, a wide range of factors impact the uptake of CC. The goal of the current study is to identify the elements that influence SMEs' decisions to approve CC by using TOE paradigm. Analyses of pertinent studies have been conducted using quantitative methodologies. According to the study's findings, 28 factors may affect SMEs' decisions to use CC. Relative advantage, technology readiness, security concerns, and top management backing also have a greater influence on SMEs' implementation of CC. The study's conclusions contribute to the body of current CC knowledge and aid practitioners in understanding factors that influence CC

implementation. As a result, they can create a clear plan for increasing the use of CC in their businesses.

Zhang (2024) Financial work has benefited greatly from the introduction of financial CC, which has also given businesses more flexible and effective solutions. In addition to recognising the potential of the Internet and financial work, financial CC has also helped organisations achieve centralised administration and information gathering. The growth of Internet technology has put a lot of strain on traditional accounting employment. One way to describe the characteristics of the financial cloud in the Internet age is "more stable, faster, and better," which implies that industry insiders and the general public's understanding of intelligent finance is always evolving. In this study, the advantages of financial cloud on financial work are assessed by a comparison and analysis of ZTE's new cloud financial cloud system and Kingdee's financial cloud system. This will speed up the financial sharing process for Chinese SMSs and help them become unbeatable in the highly competitive market. Along with increasing business and financial management efficiency and generating more company value, financial cloud computing can assist organisations in achieving a smooth integration between finance and business.

Vandita, Jaiswal and Srivastava (2023) The MSME sector in India stands to gain greatly from digital technologies. There has been a significant shift in the business-oriented digital landscape in recent years. Several new components have surfaced that may aid in defining the boundaries of a robust digital ecosystem. There are difficulties in dealing with the complex and varied MSME sector, which is made up of small businesses with varying degrees of digital readiness. Companies would be more inclined to completely adopt digital technology if an ecosystem with end-to-end solutions for operations, management, payments, skilling, and even basic information sources was made available. Businesses, notably MSMEs, have been compelled to modernise their operational processes digitally as a result of the global COVID-19 pandemic. According to this study, they ought to take into account elements that present opportunities to enhance our comprehension of MSMEs' endeavours to digitise their business processes.

The operations of MSMEs are severely harmed by the government's policy of physical segregation and pervasive social restrictions. MSMEs may find it easier to become digital if business centres are developed using the digital transformation paradigm.

CHAPTER III:
METHODOLOGY

3.1 Overview of the Research Problem

Indian MSMEs make a dynamic and competitive business sector where cloud computing solution implementation is slowly being considered the path to achieving organisational effectiveness, lower cost and competitive advantage. However, it is difficult to harness this potential, considering that major cybersecurity threats have mostly turned out to be a significant impediment to cloud computing. Indian MSMEs do not have financial capital and invest little in security measures, and the workforce is not ready to handle these issues, leaving them with risks including data theft, unauthorised access, non-compliance with regulations, and cross-jurisdiction location of data.

The reason behind this reluctance is normally due to the perceived absence of control of data by MSMEs, sensitive information loss, legal requirements which are complex to comprehend and adhere to. The two factors inherent to the concept of cloud computing complicate these challenges: the upside and downside of cloud deployment. The confidence that the enterprises place in their CSP has been found to be strongly correlated with the extent of adoption of cloud solutions. These are very readily obtained by way of clear business transparency, unswerving SLAs and even adherence to international security standards.

This research paper points out the significance of understanding the rationale of the Indian MSMEs on risk-reward ratios within cloud adoption. This involves the offering of an evaluation of their concern, evaluation of trust-building solutions and other factors that could soothe their concern as far as cybersecurity is concerned. Concentrating on the factors affecting cybersecurity risk, organisational preparedness and the endeavours made by CSP to promote trust among clients in the MSME segment in India, the paper aims at finding ways in which Indian MSME organisations can improve their cloud adoption without jeopardising their security and compliance. Such trends will ultimately assist in developing the utilization of technology in the long run and enable MSME to be at a stand to be sustainable in the expanding technological world.

3.2 Operationalisation of Theoretical Constructs

This paper examines the level of cloud computing adoption among Indian MSMEs based on five theoretical constructs as defined below. Despite the growing trend of cloud adoption in MSMEs, cybersecurity, which includes data privacy, confidentiality, integrity, availability, and perceived risk associated with data leaks, showcases the fears MSMEs has for maintaining data security (Sarkar *et al.*, 2022). There are technological factors such as the technological adoption level and technological infrastructure, that support cloud computing integration as internal enablers of adoption at the organisational level (Eskrootchi *et al.*, 2020). Competitive pressure, reliability of Internet connection and geographical location are examples of external factors that define or hinder the cloud adoption strategies.

Vendor lock-in, reliability of services or availability and security and control over data are major perceived threats and barriers to/cloud adoption and hence, discourage enterprises from migration to cloud-based solutions (Hassan, 2017). On the other hand, perceived usefulness or benefits embraces aspects that explain why decision makers should adopt such a system, include reduced cost, flexibility, scalability and ease to use. Last but not least, reliability in cloud service providers can be assessed in terms of reputation, compliancy with security requirements and openness about data handling thus significantly influencing the mitigation of certain issues and therefore enhancing the adoption likelihood (Oliveira, Thomas and Espadanal, 2014). These, in turn, outlined factors affecting cloud adoption by Indian MSMEs, within this framework.

3.3 Research Purpose and Questions

Research Questions:

- What are the various cybersecurity concerns influencing the adoption of cloud computing among Indian MSEs?
- What role do the organisational factors play in addressing cybersecurity concerns during cloud adoption?

- What are the perceived risks and barriers that hinder cloud computing adoption in MSEs?
- What are the usefulness and benefits perceived by Indian MSEs in order to adopt cloud technologies despite cybersecurity concerns?
- How does the trust in cloud service providers mitigate cybersecurity concerns and influence cloud adoption decisions?

3.4 Research Design

The research method employed in this context of the study comprises of planning and implementing a systematic approach for collecting, analysing and interpreting data to examine the impact of cybersecurity threats on the adoption of cloud computing among Indian SMEs. An exploratory approach is used in the study, and data collection involved the collection of both qualitative and quantitative data, as this was deemed appropriate for the phenomenon under study. Primary information is gathered through questionnaires or surveys, which are design following the objectives of the study to reflect the experiences of SMEs on the threat of cybersecurity and its influence on cloud services. It makes it possible to directly gather data and, especially in quantitative research, variables can be measured on different levels of analysis, providing richness with depth, as well as precision (Creswell and Creswell, 2018).

3.5 Population and Sample

The target population in this study will be Micro, Small and Medium Enterprises (MSMEs) based in India who already or are intending to use cloud computing services. This population was selected because MSMEs are an importance segment in the context of the Indian economy, contributing about 30% to the country's Gross Domestic Product, and more than 45% to the overall exports (Ministry of Ports, 2022). These enterprises face unique challenges in adopting cloud solutions, particularly due to limited financial resources, workforce readiness, and heightened cybersecurity concerns.

Convenience sampling is used by the researcher to select participants for the study, thus the sample for the study is convenient and willing to respond to questions. Its

implementation guarantees time and resource optimality while embracing multiple perceptions from MSME stakeholders within varied industries and regions. In this work, the sample size is defined in order to ensure that the data collected are sufficient to enable the quantitative and qualitative examination of factors motivating the use of cloud computing. In this study, a sample size of 100 respondents were considered for the data collection.

To increase confidence in the study findings, the target population comprises of decision makers within the MSME's such as IT managers, business owners and operations managers since they are instrumental in implementing IT decisions of the business. The purposeful survey design to distribute both online and offline encourages the gathering of key specifics on cybersecurity issues and clouds.

3.6 Participant Selection

Criteria	Description
Target Population	MSMEs in India using or considering cloud computing solutions
Sample Size	100–150 MSMEs (estimated for diverse representation)
Sampling Technique	Convenience Sampling (to ensure accessibility and resource efficiency)
Selection Criteria	
- Industry Type	MSMEs from various industries (e.g., manufacturing, IT, retail, and services)
- Size of Enterprise	Micro, Small, and Medium-sized enterprises as per MSME classification in India
- Cloud Adoption Stage	MSMEs currently using, evaluating, or yet to adopt cloud services
- Geographical Location	MSMEs across urban, semi-urban, and rural areas for diverse perspectives
- Decision-Making Role	Owners, IT managers, or decision-makers responsible for technology adoption
Exclusion Criteria	
- Non-MSME entities	Large enterprises or individual entrepreneurs
- No interest in cloud usage	MSMEs not considering cloud adoption

3.7 Instrumentation

Independent Variables	Sub Variables	Dependent Variable

Cybersecurity Concerns	Data privacy Confidentiality Integrity Availability of data Perceived risk of data breaches	Adoption of Cloud Computing
Organizational Factors	Technological readiness Financial resources Top management support Awareness of cloud computing benefits	
Environmental Factors	Competitive pressure Internet reliability and speed Geographical location	
Perceived Risks and Barriers	Vendor lock-in Service reliability (downtime/outages) Lack of control over data	
Perceived Usefulness and Benefits	Cost reduction Flexibility and scalability Ease of use	
Trust in Cloud Service Providers	Reputation and compliance with security standards Transparency in data handling	

3.8 Data Collection Procedures

The research gathered information from two primary sources, which are primary and secondary, in order to shed light on the influence of concerns regarding cybersecurity on the adoption of cloud computing in medium-sized enterprises in India. Primary data was collected through structured questionnaires that were created to obtain information on the risks associated with cybersecurity, the level of concern among businesses, their confidence in cloud service providers, and the factors that influence their decision to deploy cloud computing. The questionnaire contained multiple-choice and Likert scale questions that facilitated quantitative data analysis. It was distributed through both online and offline channels to ensure that various medium-sized businesses from different regions of the country were covered in the survey (Joshi *et al.*, 2015). At the same time, secondary data was gathered from academic papers, industry reports, government databases, and other publications. This helped in building a theoretical background, understanding the industry trends, and putting the findings from the primary research into

context. Using both types of data together gave a thorough and balanced view of the issue being studied (Bookstaver, 2021).

3.9 Data Analysis Procedures

The findings of the survey data analyzed were concerned with how the perceived cybersecurity threats affect the uptake of cloud computing by Indian MSMEs. In an effort to determine correlation, as well as the magnitude of impact of these factors, correlation and regression analysis were used. SPSS software is used because of its efficiency in managing survey data as well as analysing it.

Pearson correlation coefficients were applied to compare and estimate the strength and direction of consumer's cybersecurity concerns (data privacy, confidentiality, integrity, availability and perceived risk of data breaches), organizational enabler (technology readiness, financial capability, management support) and trust in CSPs with the level of cloud computing adoption as the dependent variable. Such an analysis offered an understanding of how tight or lose those factors were connected and whether they could be mutually dependent (Field, 2013).

An ordinal regression test was performed in order to establish the overall degree of accuracy of the studied independent variables in the process of cloud computing adoption. Some proposed adopting strategies were stressed, and the key factors emphasised included cybersecurity and organisational preparedness. For instance, variables like trust in the suppliers of cloud services and perceived benefits, including the use of this technology to reduce costs and expand the scale of communities, affected adoption positively (Ali and Younas, 2021).

The regression model gave an insight into the way all these factors interacted and to what extent they were important as far as cloud adoption is concerned. The research offered numerical evidence to reach conclusions and outline recommendations on ways to address cybersecurity issues affecting Indian MSMEs and enhance trustworthy cloud services.

3.10 Research Design Limitations

Despite having gained a useful understanding of the suitability of the research design for exploring the impacts of cybersecurity considerations on the degree of cloud computing adoption among Indian MSMEs, it is important to point out some of the limitations. First, convenience sampling, while effective and inexpensive, may have an issue of sampling bias. This would not capture all the MSMEs' species in India, especially those located in the rural and hard-to-reach areas (Etikan, 2016).

Second, all the information gathered from the survey respondents could have been contaminated by socially desirable responding or misunderstanding of the questions proposed. People being interviewed may have exaggerated their capacity within organisations or attached less importance to cybersecurity challenges, and this could have influenced the results obtained.

The last one was the use of primary data only from structured questionnaires, while excluding other types of primary data collection, such as interviews or case studies, which would enrich the context. There are also limitations to cross-sectional data because of limitation of analysing dynamic changes which characterise the MSMEs behaviour.

Finally, the study was only able to employ correlation and regression methods that are effective in establishing a relationship between the variables but not causality. To overcome such limitations and provide a better insight into Cloud adoption, future studies should involve designs like longitudinal or employ more elaborate modelling strategies.

3.11 Conclusion

The research observed the impact of cybersecurity threats on the use of cloud computing in the Indian MSMEs and also the variables that efficiently influence such decisions. In this case, the research problem identified the two-sidedness of MSMEs based on the benefits that cloud computing offers to grow productivity and reduce costs and raise competitiveness position versus the threats which the technology imposes on organisations, such as the higher rates of data theft, the fact that the technology can lock them to a specific supplier and lose control over essential data. This was achieved to curb this by developing working sub-variables off theoretical concepts such as cybersecurity issues, organisational preparedness, perceived risks, perceived benefits, and trust in

CSPs. These variables were used to pose research questions that attempted to describe the relationship between these variables and cloud adoption in response to this, a structured survey was used as the data collecting tool.

A structured research method using convenient sampling allowed the study to gather data from a cross-section of players in the MSMEs in India, focusing on major decision-makers. Quantitative data was analysed using the SPSS statistical tool; correlation and regression analysis were used to determine the predictors of cloud adoption. Accordingly, the results indicated that perceptions of trust in CSPs, organisational preparedness, and perceptions of benefits are the antecedents, while perceptions of threats and benefits are the barriers to cloud implementation. However, there were also the study's limitations- firstly, there was a heavy probability of sampling bias in both samples; secondly, the use of self-report data is always problematic since this may not represent real occurrence Thirdly, since this was a cross-sectional study, causality cannot be inferred.

In sum, the paper establishes that work needs to be done regarding cybersecurity threats and establishing trust to improve the take-up of cloud services among MSMEs. If cloud service providers employ relatively transparent behaviours, clearly defined and stringent Service Level Agreements, and comply with international security standards, the perceived risks of cloud sources can be reduced, thus increasing its uptake. Future research could use longitudinal designs and also use qualitative designs to capture the dynamic trends and gain more depth. Overall, this work offers policy makers, cloud providers, as well as the MSE & MSMEs the ability to appreciate and jointly begin to solve for the opportunity laid in front of them by realising the future potential of cloud computing.

CHAPTER IV:
RESULTS

4.1 Reliability Analysis

For each of the fifty items that made up the survey, researchers calculated Cronbach's Alpha to see how well the research instrument held together. Table 4.1 displays the outcomes.

Table 4.1

Reliability Statistics

Cronbach's Alpha	N of Items
.929	50

As per the data reliability statistics presented in Table 4.1, the 50-item instrument generated a Cronbach's Alpha value of 0.929, which is significantly greater than the minimum required level of 0.7. Thus, it is a clear sign of excellent internal consistency, meaning that the items are measuring the same construct very reliably and with little error. To sum up, the instrument is deemed to be both stable and accurate for subsequent analyses.

4.2 Findings of Demographic Details

Demographic details of the participants in the study are shown in Table 4.2. The information gives a picture of the respondents with respect to their age, sex, job status, sector, qualification, AI/ML knowledge, AI/ML methods used, and programming language skills.

Table 4.2

Demographic details of respondents

Category	Sub-category	Frequency	Percent
Age	18-25 Years	36	36
	26-35 Years	33	33
	36-45 Years	21	21
	46-60 Years	7	7
	Above 60 Years	3	3
Gender	Male	55	55
	Female	45	45

Employment Status	Employed full-time	33	33
	Employed part-time	23	23
	Self-employed	24	24
	Unemployed	5	5
	Student	8	8
	Retired	7	7
Industry	Technology	25	25
	Healthcare	25	25
	Finance/Banking	21	21
	Education	15	15
	Retail/Consumer Goods	4	4
	Manufacturing	5	5
	Others	5	5
Education	High secondary school	10	10
	Bachelor's degree	37	37
	Master's degree	38	38
	Doctorate (PhD)	13	13
	Other	2	2
Experience in AI/ML	Less than 1 year	19	19
	1-3 years	43	43
	4-6 years	24	24
	7-10 years	8	8
	More than 10 years	6	6
AI/ML Techniques Used	Neural Networks (CNN, RNN, LSTM, etc.)	10	10
	Decision Trees (Random Forest, XGBoost, etc.)	16	16
	Natural Language Processing (NLP)	29	29
	Deep Learning (Transformers, GANs, etc.)	25	25
	Reinforcement Learning	9	9
	Others	11	11
Programming Languages	Python	33	33
	R	13	13
	Java	25	25
	Julia	10	10
	MATLAB	11	11
	Others	8	8

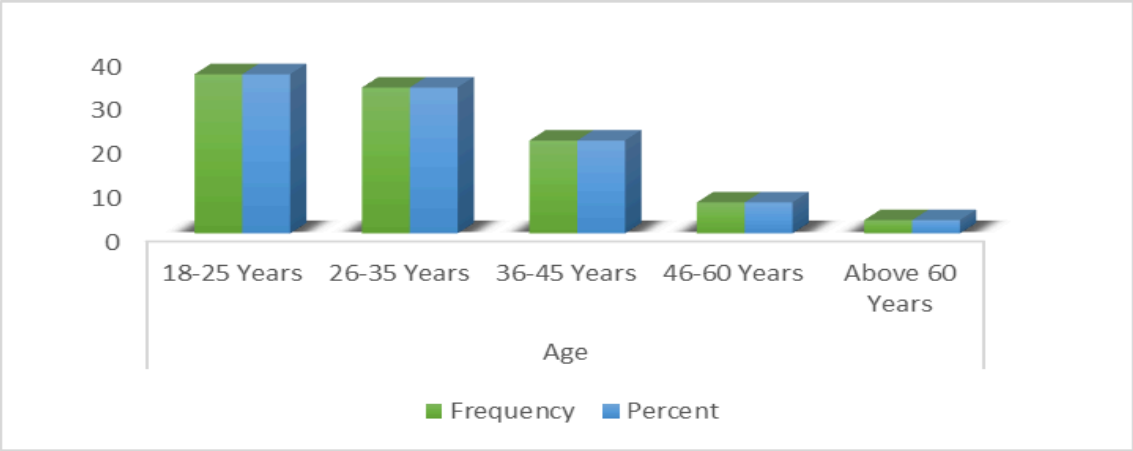

Figure 4.1

Age

The distribution of ages of respondents can be seen in the above figure. The data reveals that a considerable number of young people took part in the survey. In fact, 36% of the respondents were from the 18-25 years age group and 33% were from the 26-35 years age group, which together accounted for almost 70% of the overall sample. On the other hand, 21% of the respondents were in the age group of 36-45 years, while 7% were in the age group of 46-60 years, and only 3% were over 60 years old. This shows that the study is mainly influenced by the opinions of the younger professionals, with a little input from the older age groups.

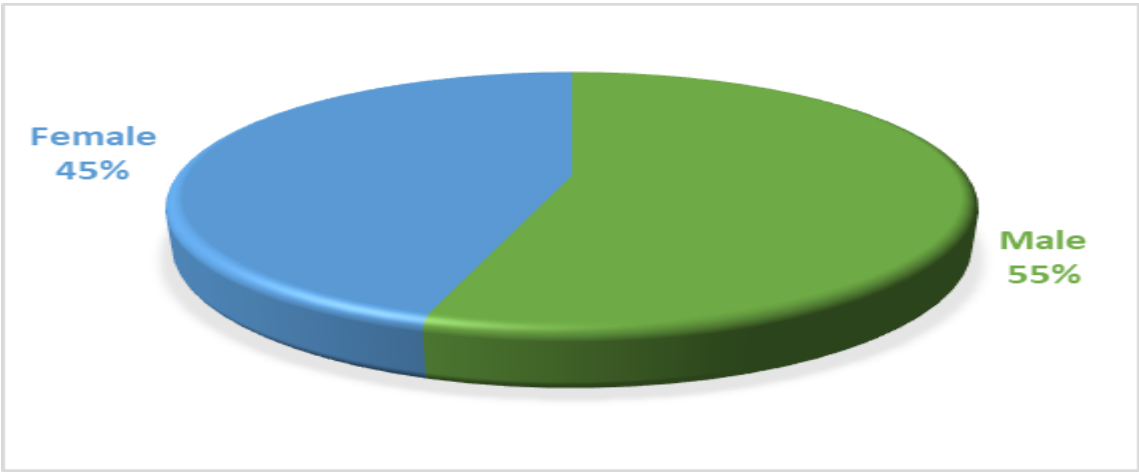

Figure 4.2

Gender

The gender composition of the participants is shown in the figure above. The sample is quite evenly distributed, comprising 55% males and 45% females. The presence of men as the majority is small, while the participation of both sexes grants the analysis a diversity of perspectives that is too little to be ignored.

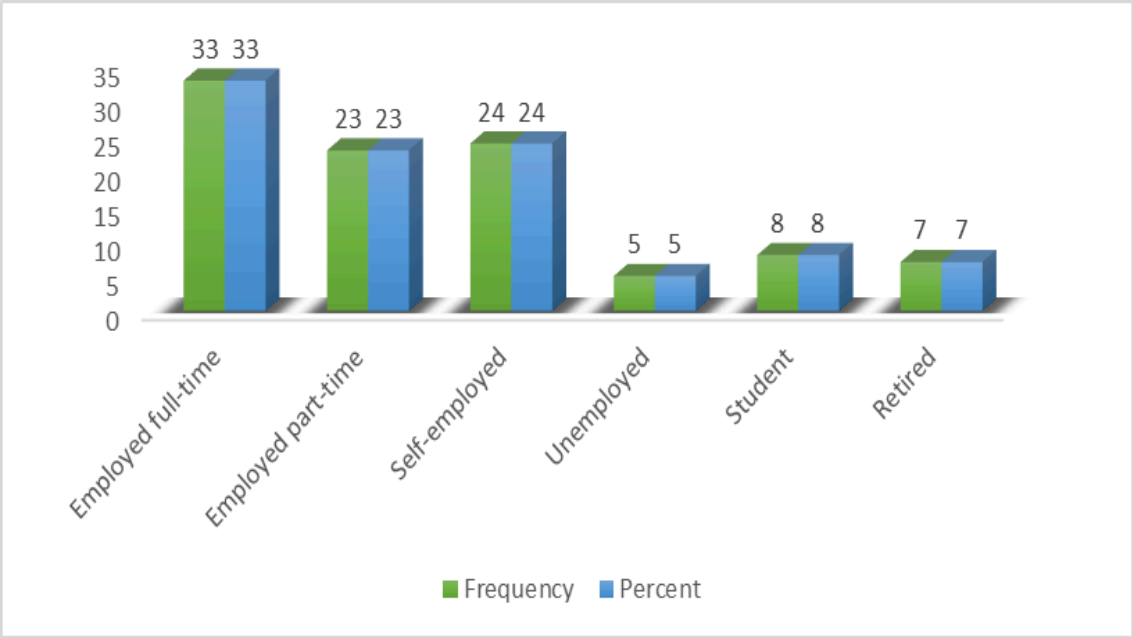

Figure 4.3

Employment Status

The diverse range of occupations of the respondents is evident in the present analysis. Full-time workers constitute the largest group (33%), while self-employed individuals (24%) and part-time workers (23%) follow closely behind. The remaining categories of respondents are students (8%), retirees (7%), and job seekers (5%), who form the smallest groups. This broad distribution implies that the research encompasses viewpoints from both the active professionals and the non-working population.

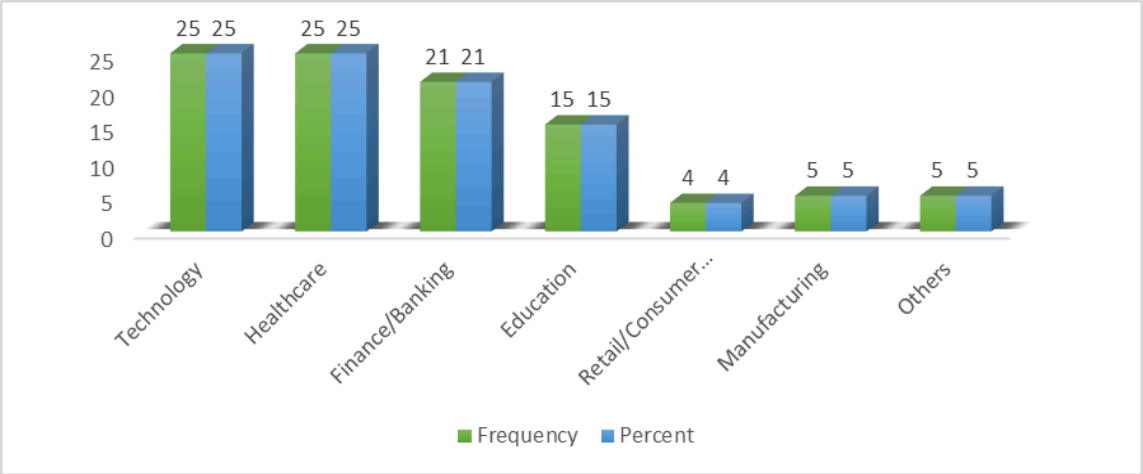

Figure 4.4

Education

This indicates that the respondents are very well-educated. The group with the largest number consists of people holding a Bachelor's degree (37%) and a Master's degree (38%), which when added together make up three-quarters of the sample. Moreover, 13% have PhDs, 10% have finished high school and only 2% have told about their education being in other forms. All this considered, the respondents usually have excellent academic qualifications.

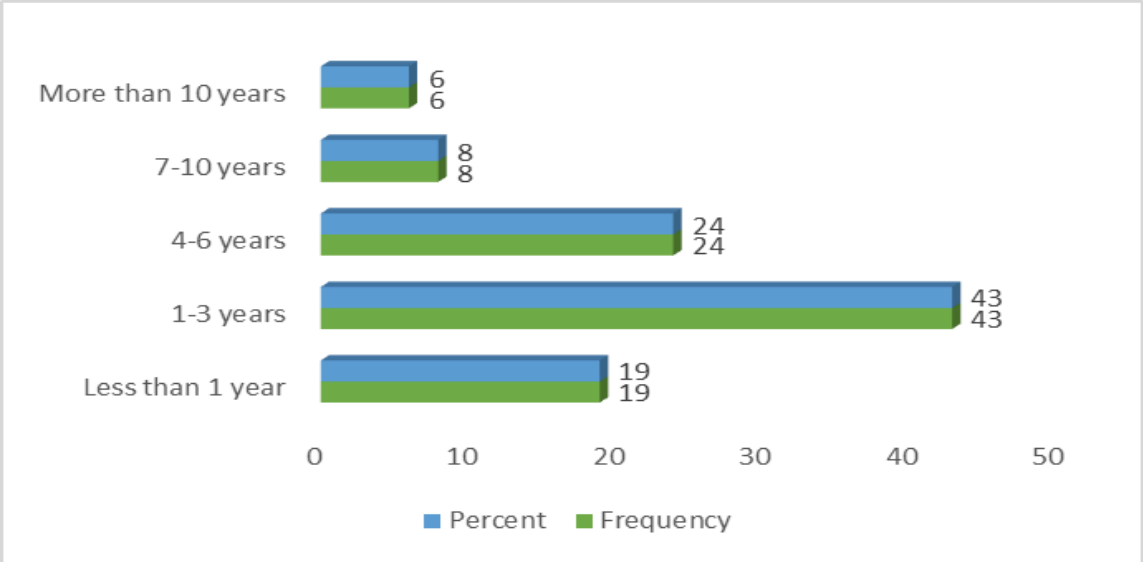

Figure 4.5

Experience in AI/ML

The data above show the participants' experience in AI/ML. 43% is the majority, which is the share of respondents who claimed 1-3 years of experience, then 24% with 4-6 years come next. Another 19% are the least experienced, having less than a year of experience, whereas 8% have 7-10 years and 6% more than 10 years of experience. This distribution indicates that the majority of the respondents are still at the beginning or mid-level of their AI/ML careers.

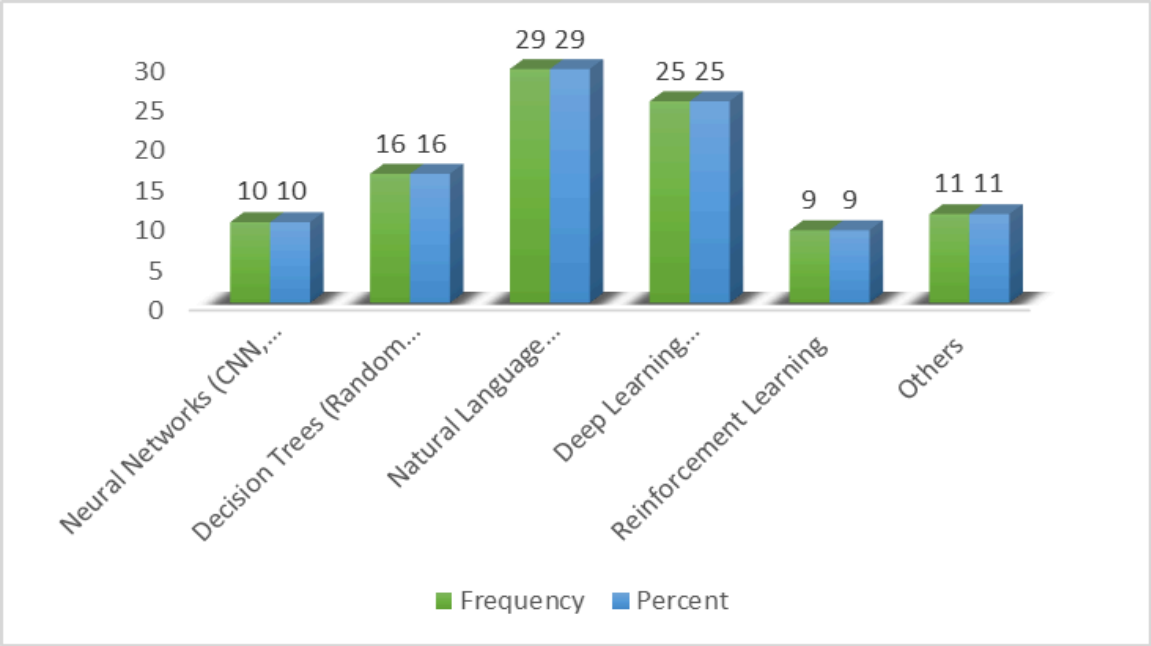

Figure 4.6

AI/ML Techniques Used

This gives a sketch of the AI/ML procedures that the respondents utilized. Natural Language Processing (29%) is the first on the list of methods used, then come Deep Learning techniques (25%) second. Among the remaining methods, Decision Trees (16%) and Neural Networks (10%) are the least used, while Reinforcement Learning (9%) and other methods (11%) indicate further application areas. This suggests an increased dependency on high-end and new AI techniques.

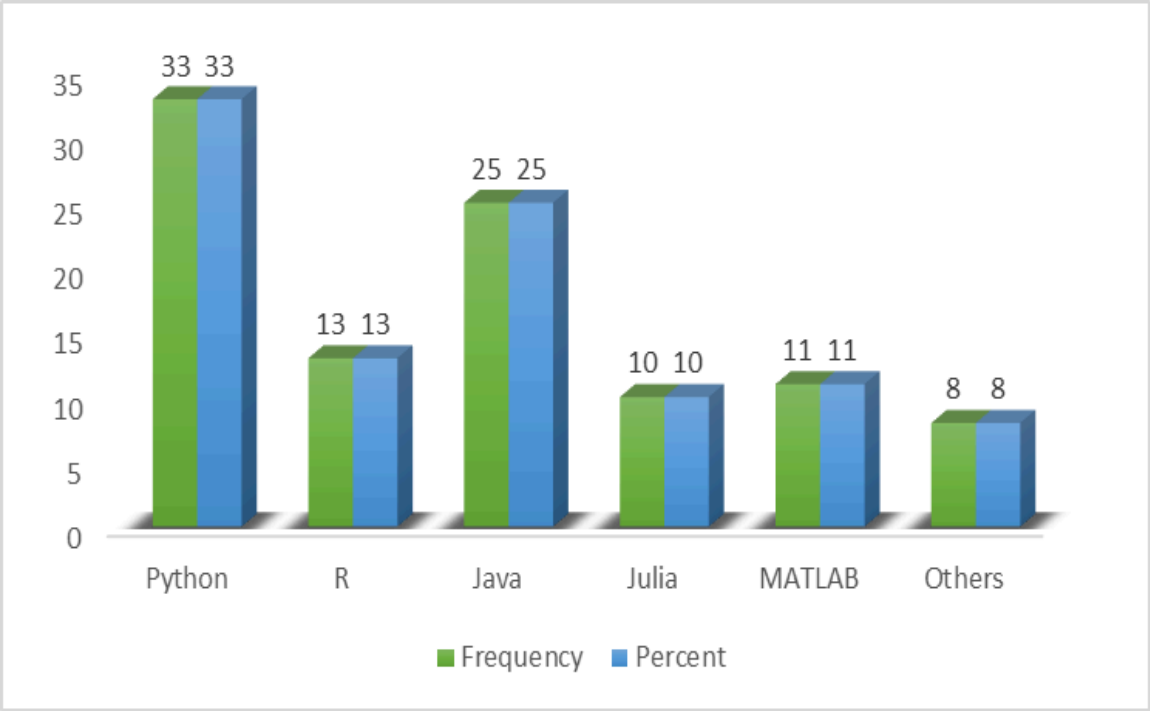

Figure 4.7

Programming Languages

This shows the results of programming languages favoured by the people surveyed. Python came first with a wide margin of 33% which confirms its position as the main tool for AI/ML applications. A very close second is Java with 25% that, too, has a significant position. R is used by 13%, MATLAB by 11%, and Julia is chosen by 10% of the respondents, which means that they are all moderately used. A minority of 8% sticks to other languages. The results suggest not only the superiority of Python but also the variety of programming capabilities among the respondents.

4.3 Findings Related to Cybersecurity Concerns

The inquiry looked into the opinions of the respondent's concerning cybersecurity in cloud computing, concentrating on data privacy, integrity, and availability. The frequency and percentage of responses for ten main statements are shown in Table 4.3.

Table 4.3

Cybersecurity Concerns

		SD	D	N	A	SA
I am concerned about the privacy of sensitive data stored on cloud platforms.	Frequency	13	9	28	30	20
	Percent	13	9	28	30	20
Cloud service providers adequately address data privacy issues.	Frequency	1	23	21	34	21
	Percent	1	23	21	34	21
I worry about unauthorized access to confidential data in the cloud.	Frequency	1	9	23	38	29
	Percent	1	9	23	38	29
Cloud systems ensure sufficient measures to protect data confidentiality.	Frequency	2	7	16	43	32
	Percent	2	7	16	43	32
Ensuring the integrity of data stored in the cloud is a major concern.	Frequency	7	12	18	27	36
	Percent	7	12	18	27	36
Cloud providers effectively maintain data integrity.	Frequency	4	10	22	43	21
	Percent	4	10	22	43	21
I am concerned about the availability of my data when needed.	Frequency	3	11	29	30	27
	Percent	3	11	29	30	27
Cloud providers have robust mechanisms to ensure continuous access to data.	Frequency	3	19	24	35	19
	Percent	3	19	24	35	19
I perceive a high risk of data breaches when using cloud services.	Frequency	7	9	18	43	23
	Percent	7	9	18	43	23
Cloud providers take adequate measures to mitigate the risk of data breaches.	Frequency	2	20	11	34	33
	Percent	2	20	11	34	33

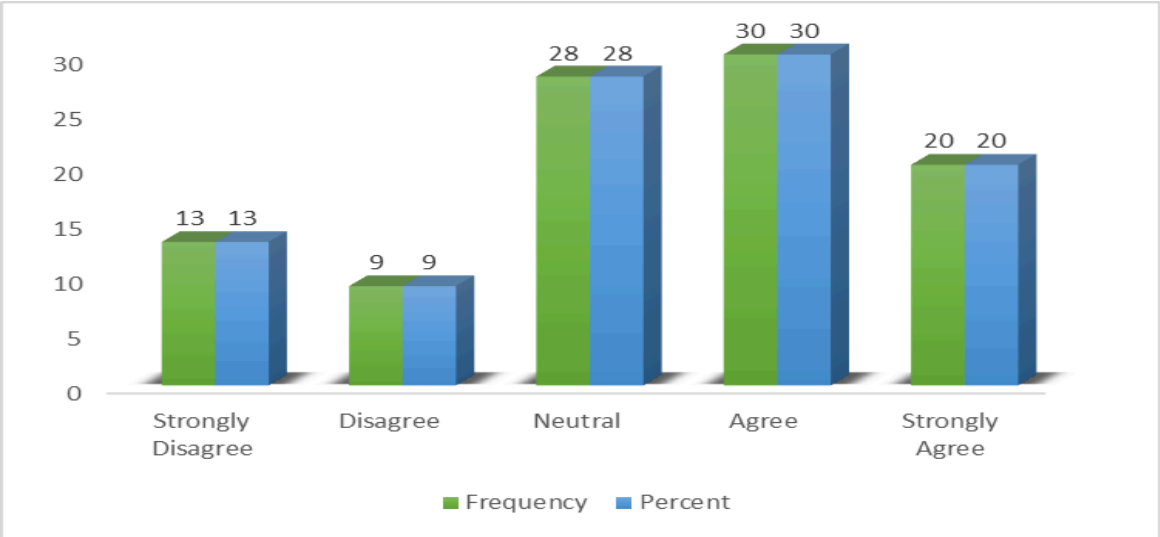

Figure 4.8

I am concerned about the privacy of sensitive data stored on cloud platforms.

As illustrated in Figure 4.8, a large part of the people who took part in the survey (30% agreed and 20% strongly agreed) showed concern regarding the privacy of sensitive data kept in cloud storage. On the other hand, 28% stayed neutral and only 22% disagreed to different degrees. This points to the fact that there is neutrality, but at the same time a considerable number of people sharing the worry about privacy matters in clouds.

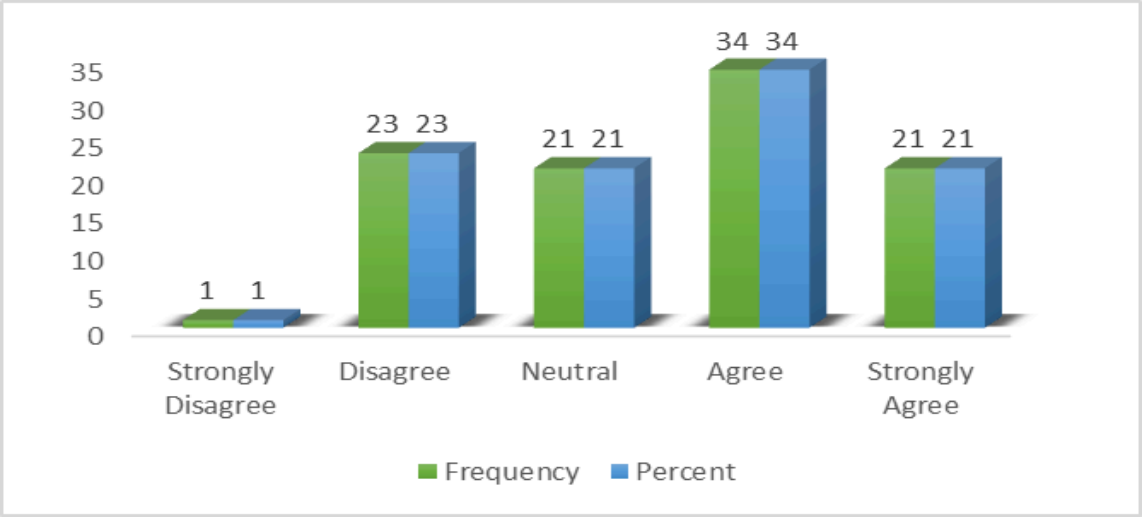

Figure 4.9

Cloud service providers adequately address data privacy issues.

The data from Figure 4.9 indicates that the opinions of the respondents concerning the cloud service providers' data privacy protection were split. Approximately 55% A (34% agree, 21% strongly agree), whereas 24% D. Furthermore, 21% remained N, revealing a diversity of opinions. The results point out the absence of a dominant agreement, suggesting that while a significant number of users have faith in the providers, the issue of sufficiency remains open.

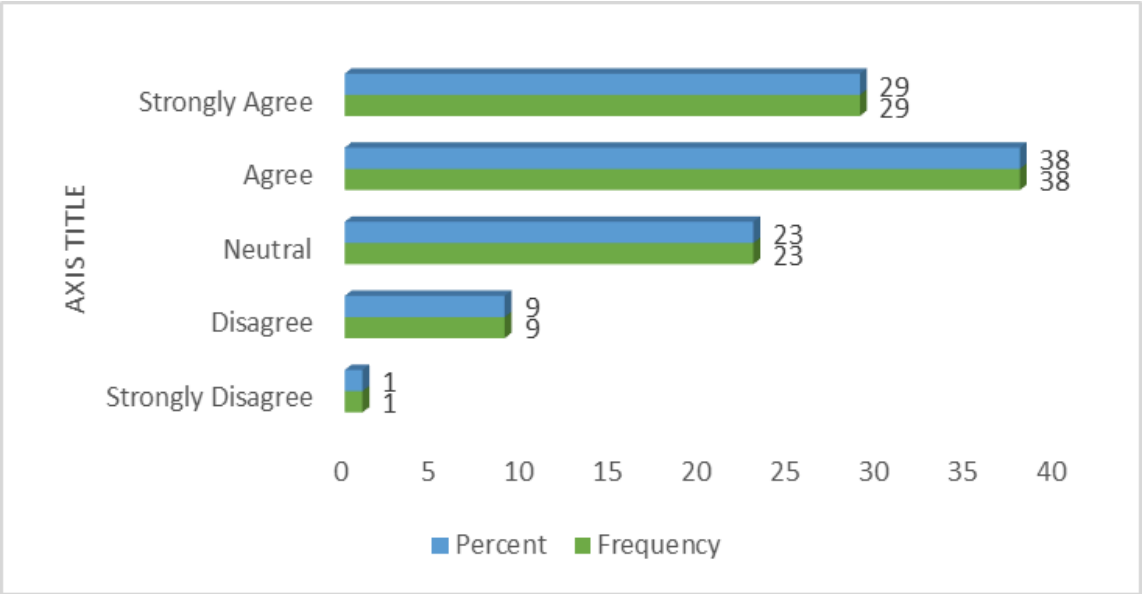

Figure 4.10

I worry about unauthorised access to confidential data in the cloud.

Figure 4.10 shows that there are large fears surrounding the unauthorized access of confidential information that was stored in the cloud. Almost 70% (67%) completely agree with the statement or agree to a large extent, but just a small percentage (10%) disagrees. About 23% of the participants were neutral. These findings unmistakably indicate that the respondents' fears about unauthorized access have increased, and they have even given data security the status of the biggest concern in the cloud adoption issue.

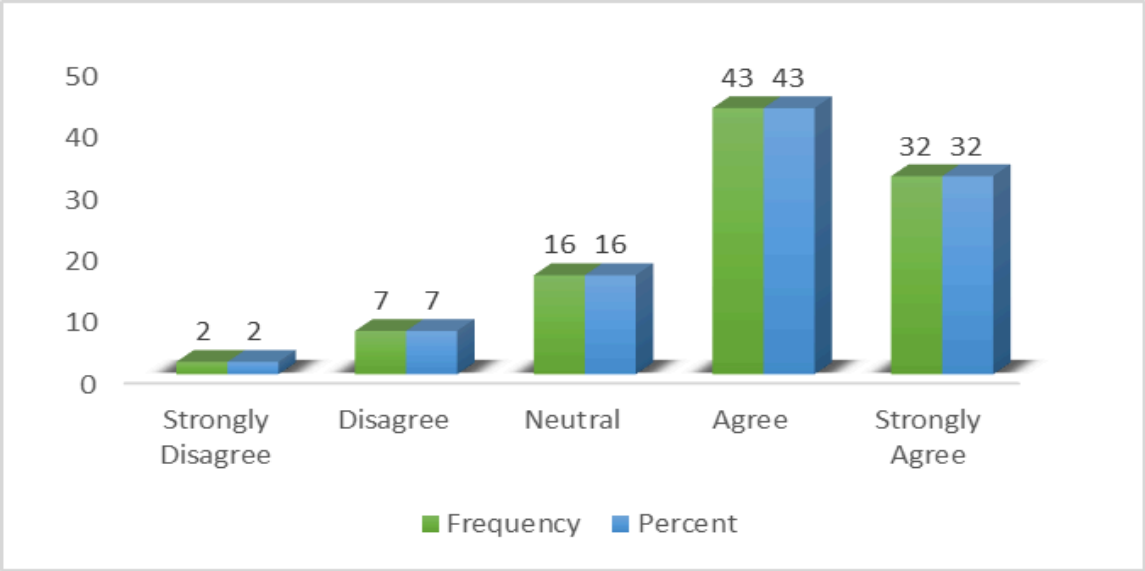

Figure 4.11

Cloud systems ensure sufficient measures to protect data confidentiality.

The perception of cloud systems around the issue of confidentiality is generally very positive among the respondents as depicted in Figure 4.11, where 75% expressed agreement (43% agree, 32% strongly agree). A mere 9% D, and 16% were N. This indicates that there is a trend towards more trust in the confidentiality measures of cloud providers, but still a small fraction as people who doubt the strength of such measures.

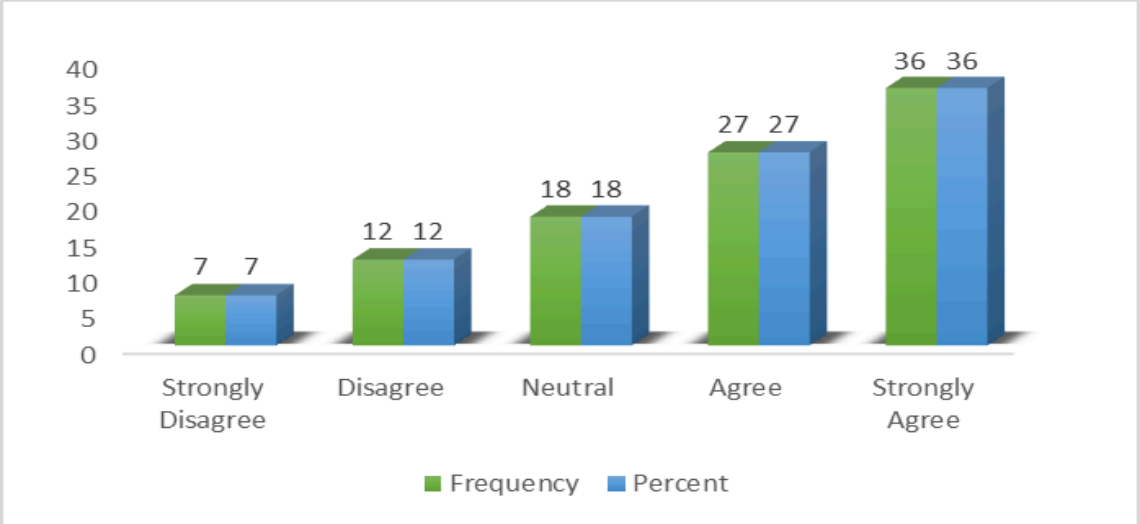

Figure 4.12

I perceive a high risk of data breaches when using cloud services.

As indicated by Figure 4.12, the integrity of the data stored in the cloud is a serious concern, as 63% of respondents rated it with either A or SA. Only 19%, on the other hand, rated it with D, while 18% remained neutral. The emphasis placed by the users on data integrity is thus revealed, which shows that it is still a major problem notwithstanding the technological safeguards in place.

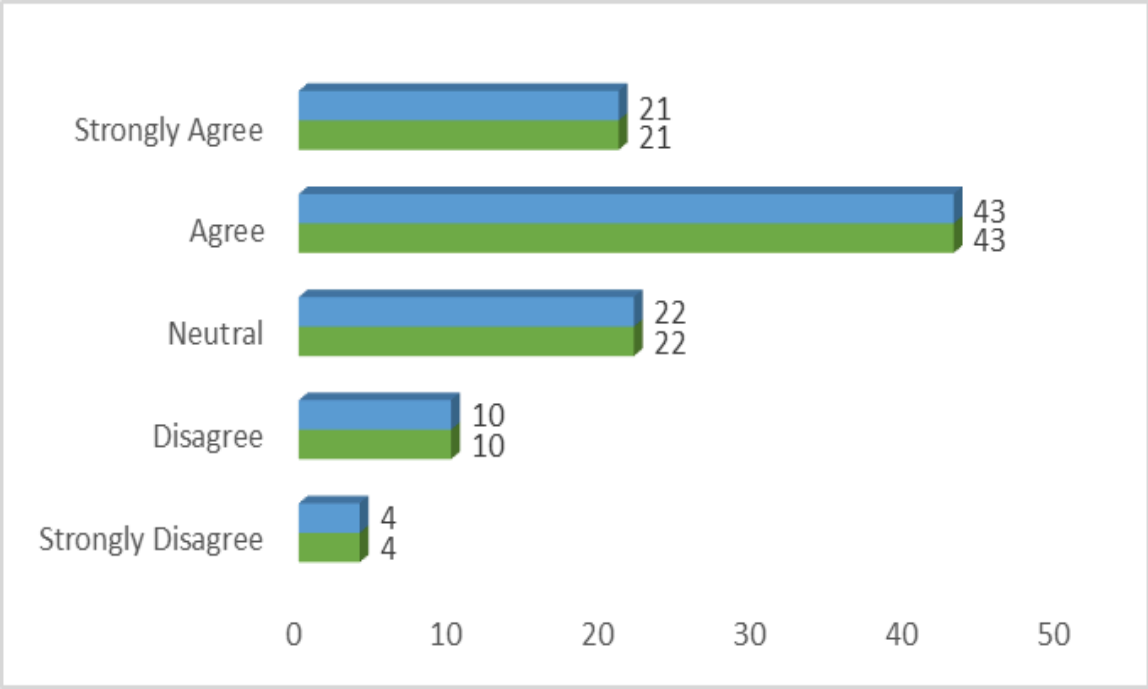

Figure 4.13

Cloud providers effectively maintain data integrity.

The respondents' relatively positive perception concerning the role of cloud providers in data integrity preservation is illustrated in Figure 4.13. Approximately 64% chose either A or SA, 14% chose D, and 22% were neutral. This implies that on one hand, a majority of the participants confidently rely on the providers to keep the integrity, while on the other hand, a significant minority does not completely trust them, thus indicating the need for developing more robust assurance mechanisms.

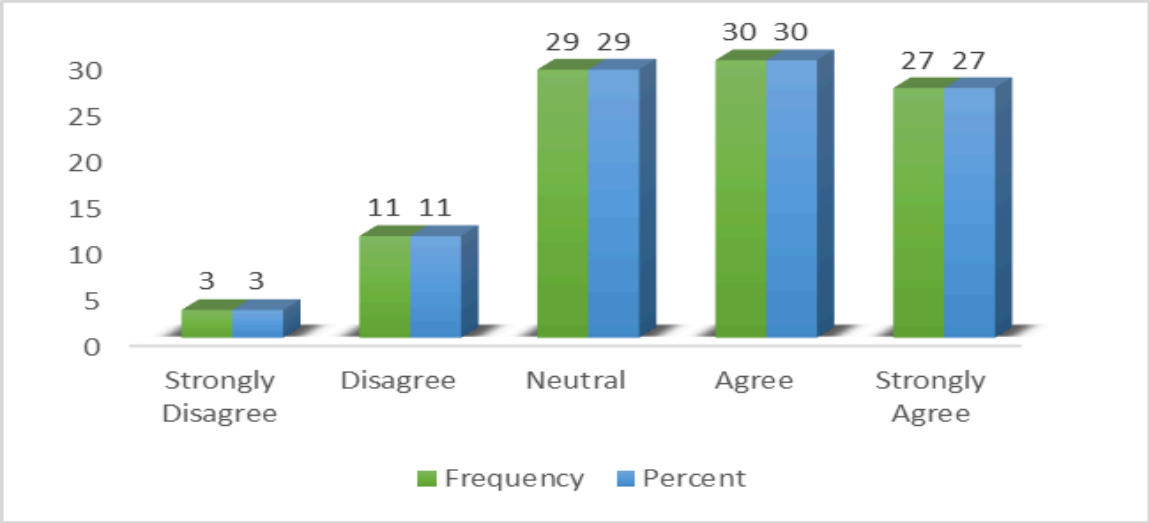

Figure 4.14

I am concerned about the availability of my data when needed.

Figure 4.14, 57% of the respondents rated data availability as a problem, with A or SA. At the same time D was 14%, and N was 29%. That means the majority of the people, though trusting the availability of the service, are still worried about it, thus making it very crucial for the systems operating in the cloud to have continuous and reliable access.

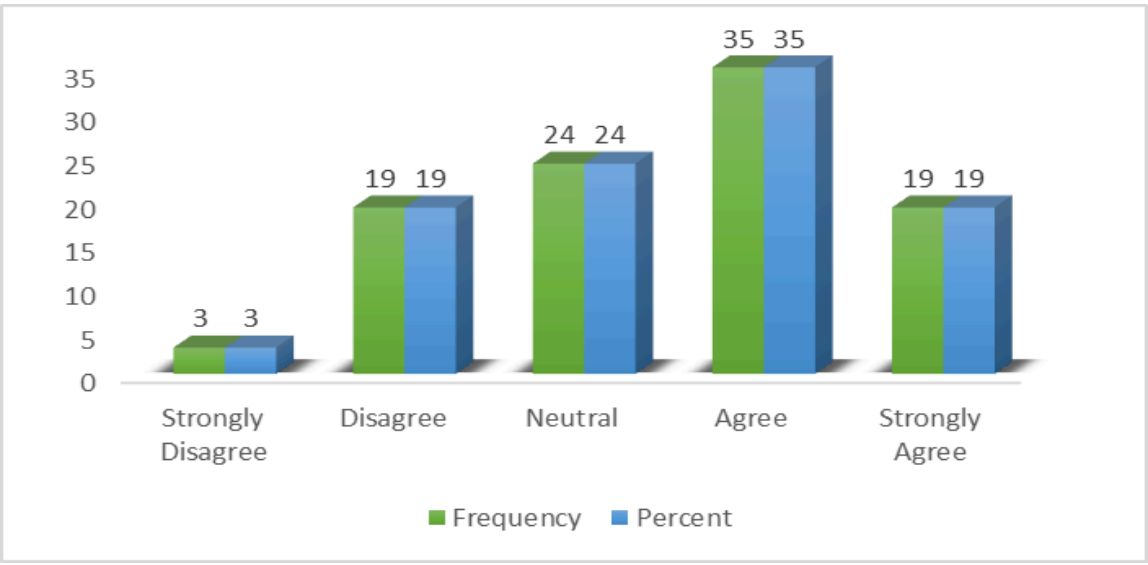

Figure 4.15

Cloud providers have robust mechanisms to ensure continuous access to data.

The data shown in Figure 4.15 indicates the opinions of the providers' mechanisms for data availability and at the same time shows the level of confidence in them. To be precise, over half of the respondents (54%) expressed their agreement to a certain extent (A or SA), 22% of them were in total disagreement (D), and 24% took a neutral position (N). It can be stated that most customers are sure about the providers' continuity measures; however, the quite high rates of disagreement and neutrality indicate that more transparency and reliability assurances could be a way to win over users' trust.

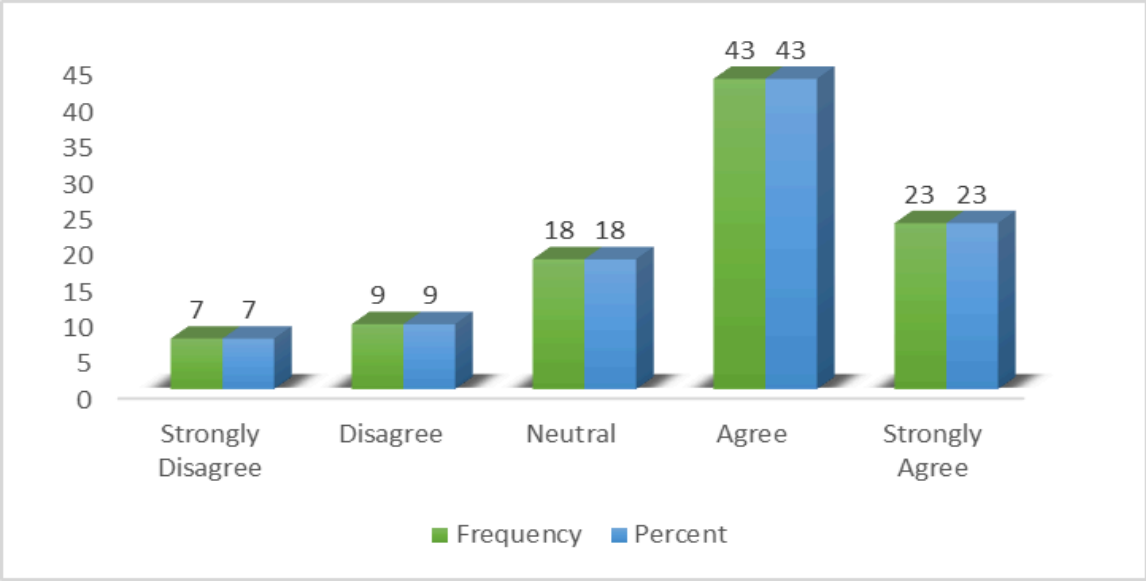

Figure 4.16

I perceive a high risk of data breaches when using cloud services.

The illustration in Figure 4.16 depicts a very clear opinion that data breaches in cloud services imply a very high risk. Around 66% expressed agreement or strong agreement (A or SA), 16% disagreed (D), and 18% were neutral (N). This indicates that data breach apprehension continues to be a major issue, which strengthens the argument that many users still view the cloud as being open to attacks even though there have been improvements.

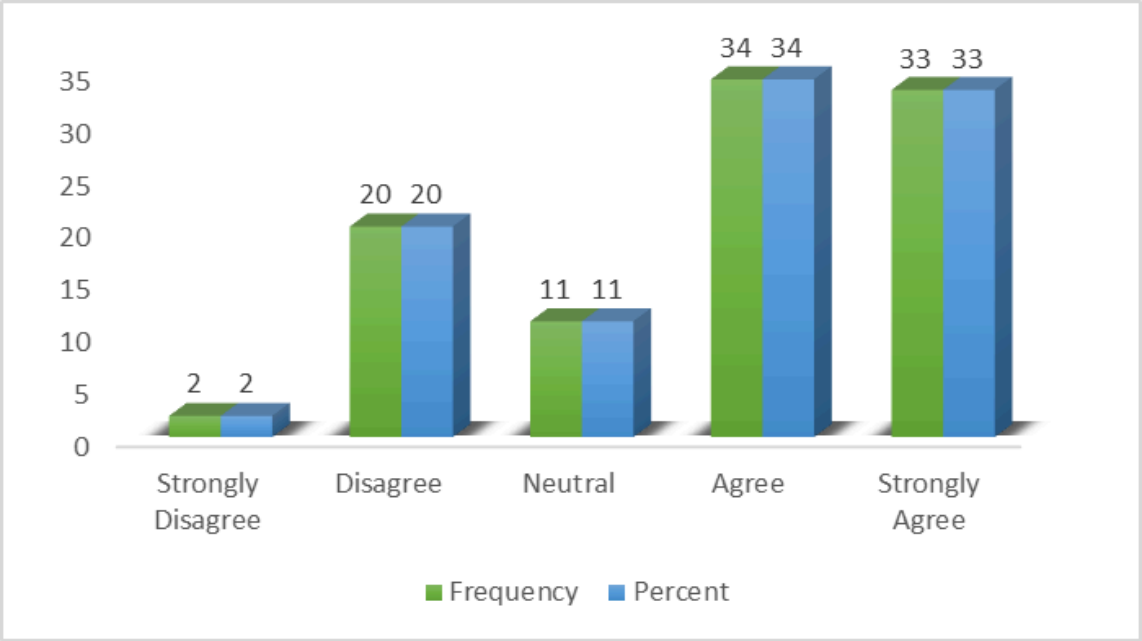

Figure 4.17

Cloud providers take adequate measures to mitigate the risk of data breaches.

In Figure 4.17 one can see the opinions of the respondents concerning the ability of the providers to reduce breach risks. The majority, i.e., approximately 67% agree to this statement, 22% disagree and the remaining 11% are neutral. Although the majority have confidence in the security measures of the providers, the substantial opposition implies ongoing doubt, thereby indicating that users still need more proof of satisfactory risk mitigation.

4.4 Findings on Organisational Factors

The research scrutinised various organisational factors that determine the adoption of cloud computing, like technological acceptance, infrastructure, financial resources, support of management and awareness of employees. The opinions of the respondents on eight vital statements are illustrated in Table 4.4.

Table 4.4

Organisational Factors

Statement		SD	D	N	A	SA
Our organisation is technologically prepared for cloud computing adoption.	Frequency	6	7	27	31	29
	Percent	6	7	27	31	29
We have the necessary IT infrastructure to support cloud adoption.	Frequency	1	11	22	41	25
	Percent	1	11	22	41	25
The organisation has sufficient financial resources to invest in cloud solutions.	Frequency	4	16	17	30	33
	Percent	4	16	17	30	33
Budgetary constraints hinder our ability to adopt cloud computing.	Frequency	5	12	18	37	28
	Percent	5	12	18	37	28
Top management is actively involved in cloud adoption decisions.	Frequency	2	10	29	33	26
	Percent	2	10	29	33	26
Senior leadership supports the allocation of resources for cloud initiatives.	Frequency	2	12	27	32	27
	Percent	2	12	27	32	27
The organisation is aware of the potential benefits of cloud computing.	Frequency	6	14	27	34	19
	Percent	6	14	27	34	19
Employees understand how cloud computing can enhance business processes.	Frequency	2	18	24	32	24
	Percent	2	18	24	32	24

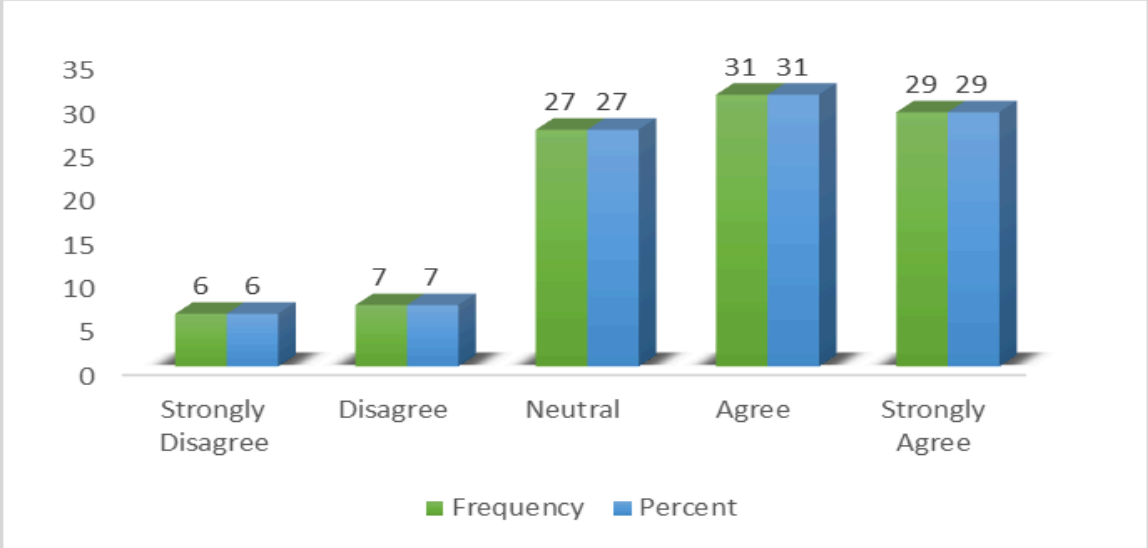

Figure 4.18

Our organisation is technologically prepared for cloud computing adoption.

From this, it can be inferred that the vast majority of the respondents' organizations were ready on the technology front for cloud adoption. 60% A or SA, 27% N, and merely 13% D were the figures representing the majority. It indicates that readiness is there in most organizations, but a small fraction still doubts their overall readiness for cloud computing.

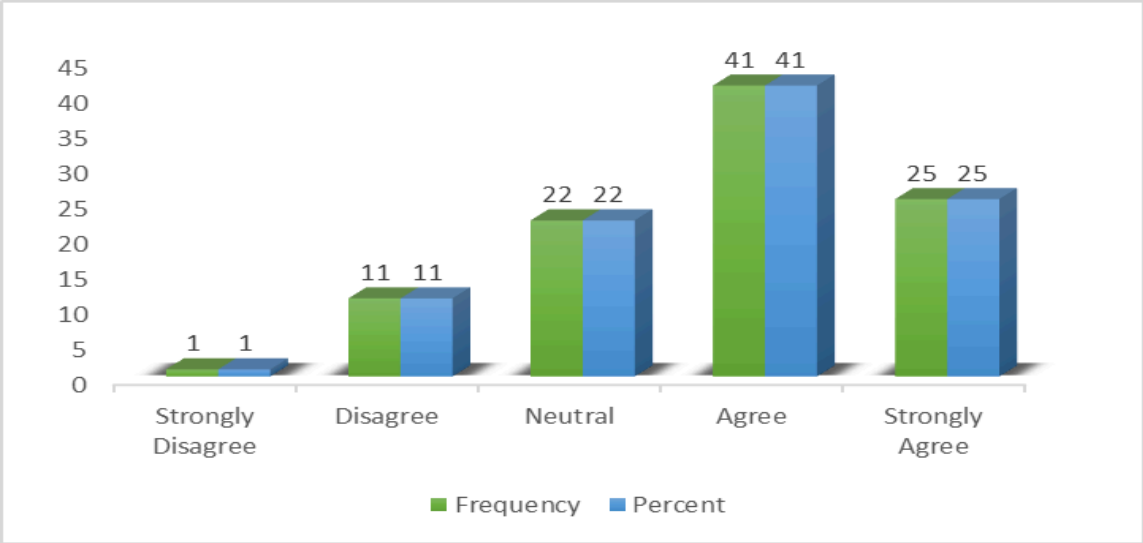

Figure 4,19

We have the necessary IT infrastructure to support cloud adoption.

This indicates a high level of assurance regarding the preparedness of IT infrastructure. Nearly two-thirds (66%) rated it as A or SA, 22% rated it as N, while a mere 12% expressed disagreement. This means that most of the participants consider their IT infrastructure to be sufficient for the support of cloud adoption, which in turn implies that the infrastructure is not viewed as a significant obstacle to adoption.

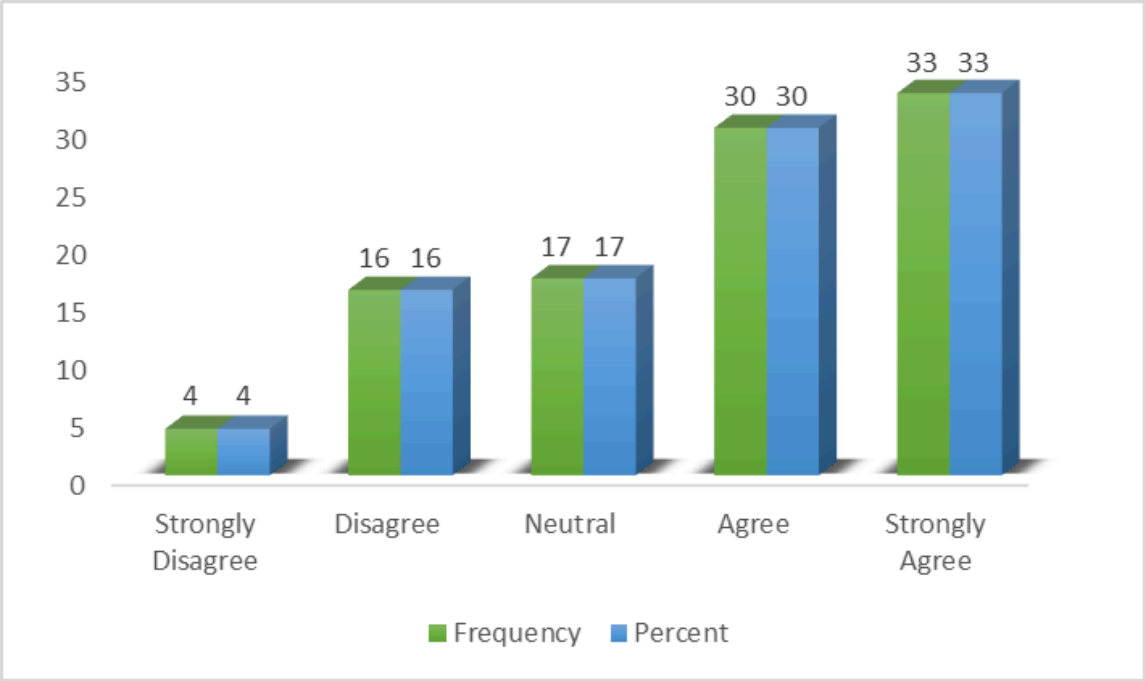

Figure 4.20

The organisations has sufficient financial resources to invest in cloud solutions.

Thus, it can be said that financial resources have been regarded as adequate for the investment in cloud technology. The distribution of the response showed that nearly 63% were in favour (A or SA), 17% remained neutral (N), and 20% were opposed (D). This means that financial capability is not the main factor against going for the cloud, but still some companies think their budgets would limit the progress of cloud projects and thus they are not fully ready to invest in the cloud at the moment.

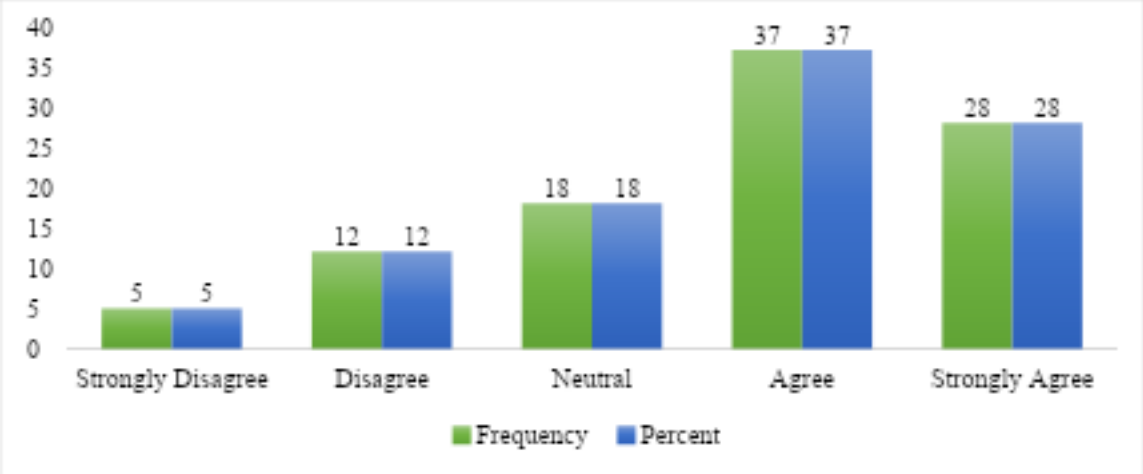

Figure 4.21

Budgetary constraints hinder our ability to adopt cloud computing.

This emphasizes the fact that limitations in budget are still an issue. Out of the total, 65% expressed opinions of either A or SA that one of the reasons for slow cloud adoption is financial difficulties, while only 23% D and 18% were N. This indicates that although resources are acknowledged, still costs-related obstacles are influencing the making of the decision, which in turn shows the mixed challenge of affordability and priority setting.

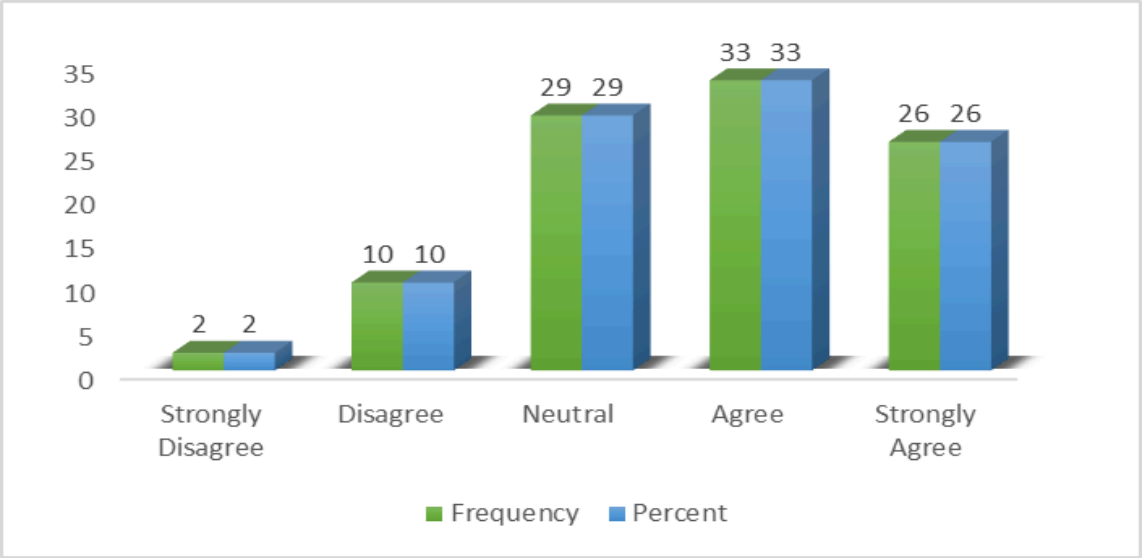

Figure 4.22

Top management is actively involved in cloud adoption decisions.

This reflects the participation of the top management in cloud adoption. Around 59% A or SA, 29% were N, and 12% D. The findings indicate that the leadership is a major factor in influencing the cloud initiatives; however, the N responses indicate that sometimes the management involvement may not be completely observable.

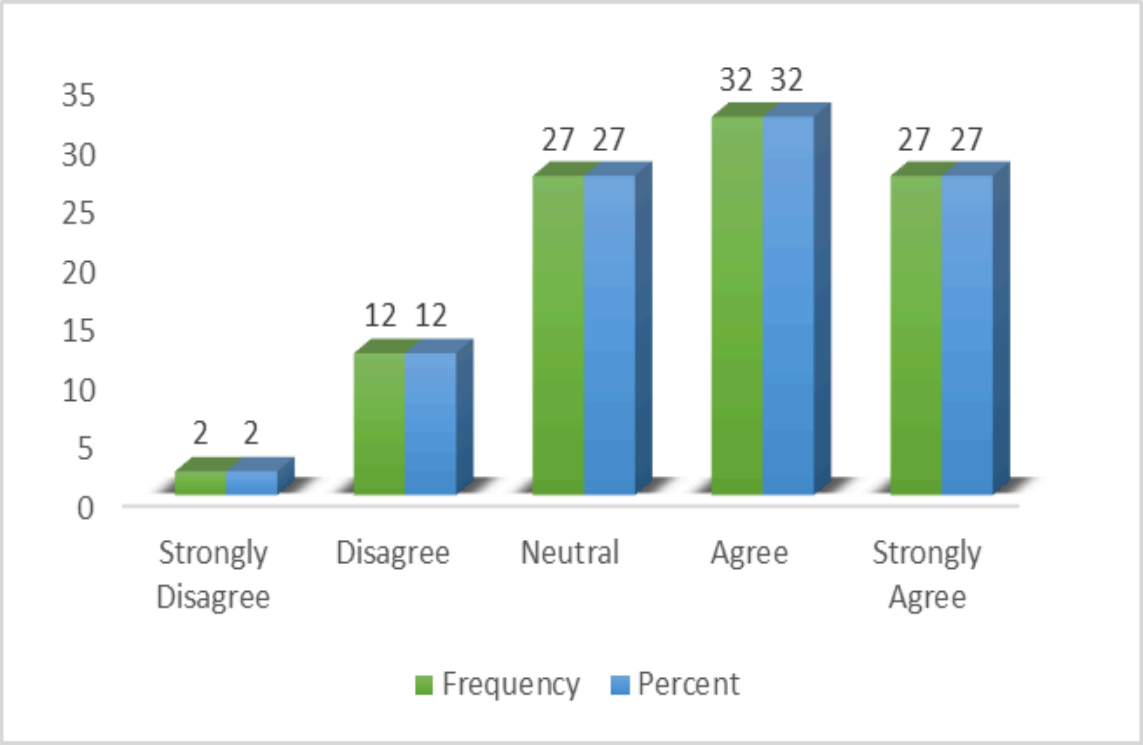

Figure 4.23

Senior leadership supports the allocation of resources for cloud initiatives.

This shows that the top management is backing the resource allocation for cloud projects. About 59% A or SA, 27% were N, and 14% D. The findings indicate that in most cases, the leadership support is there, however, the neutrality and disagreement indicate that in some companies, the support for resource allocation is still inconsistent or limited.

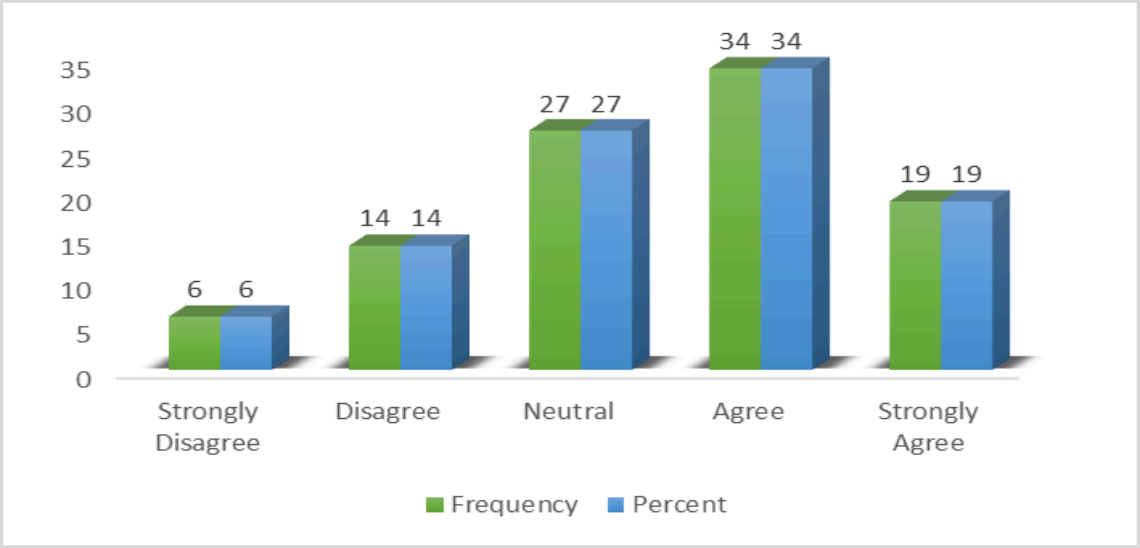

Figure 4.24

The organisation is aware of the potential benefits of cloud computing.

It can be inferred that the awareness of cloud benefits in the organisation is quite high as 53% of the respondents gave A or SA. But 20% gave D and 27% remained N. So, it can be concluded that the major part of the organisations is aware of the cloud computing advantages, but still the diffusion of knowledge is needed as the level of awareness and understanding is not the same in all organisations.

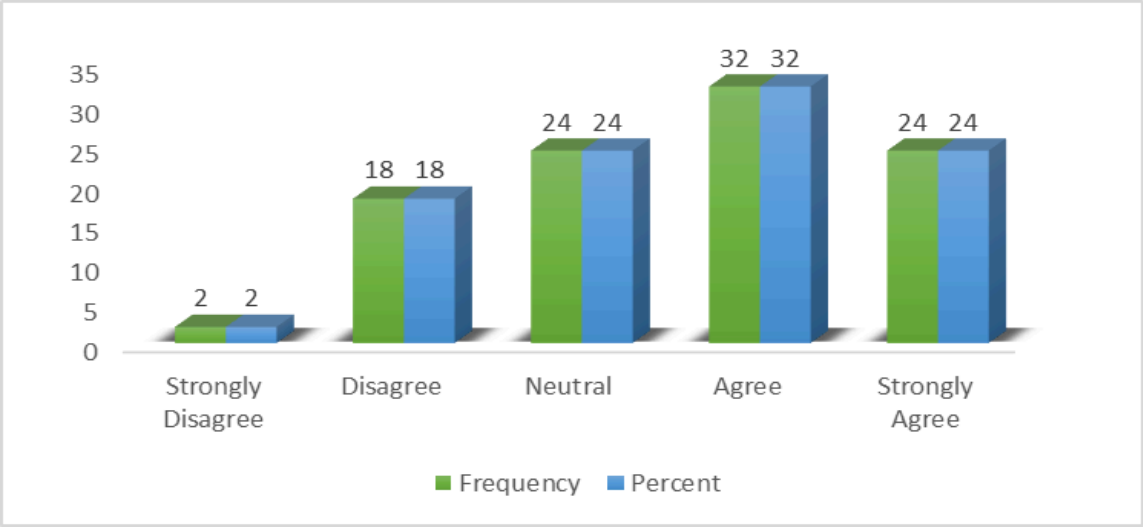

Figure 4.25

Employees understand how cloud computing can enhance business processes.

This is an example of a good understanding of cloud computing benefits by the employees. The majority of 56% A or SA, while the minority of 24% were N and 20% D. This shows that the awareness of employees is moderately strong but not complete, revealing the necessity of more training and communication to grasp the cloud-enabled business process improvements comprehensively in the entire organisation.

4.5 Findings on Environmental Factors

The research went into the matter of environmental influences that might push firms to use or not use cloud computing, and these were competitive pressure, internet connectivity, and challenges inherent to certain locations. Table 4.5 shows the perception of the respondents on six main statements.

Table 4.5

Environmental Factors

Statement		SD	D	N	A	SA
Competitive pressure drives our organisation to adopt cloud computing.	Frequency	4	15	15	38	28
	Percent	4	15	15	38	28
Competitors using cloud computing gain a significant competitive advantage.	Frequency	0	14	18	41	27
	Percent	0	14	18	41	27
Reliable internet connectivity is critical for adopting cloud computing.	Frequency	3	15	27	29	26
	Percent	3	15	27	29	26
Internet speed in our area is sufficient to support cloud computing adoption.	Frequency	2	5	24	42	27
	Percent	2	5	24	42	27
Our geographical location affects the availability of cloud service providers.	Frequency	0	15	23	35	27
	Percent	0	15	23	35	27
Location-specific challenges hinder our ability to adopt cloud technologies.	Frequency	2	16	17	38	27
	Percent	2	16	17	38	27

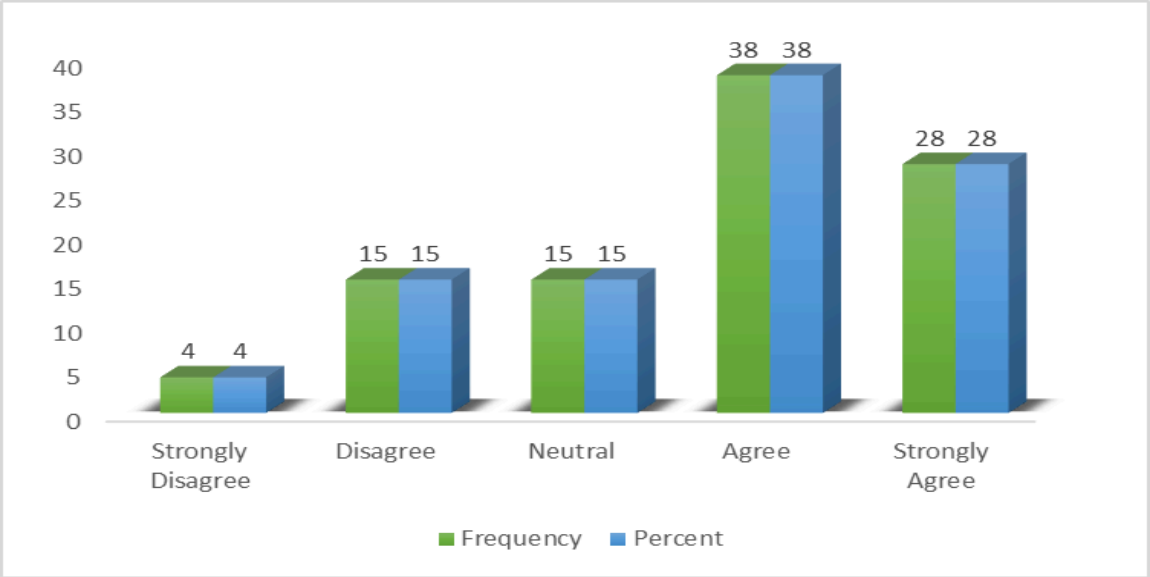

Figure 4.26

Competitive pressure drives our organisations to adopt cloud computing.

The notice reveals the fact that the pressure of competition has a major impact on the decision to adopt cloud services. The total of 66% rated it A or SA, 15% N, and 19% D. Thus, it can be concluded that the majority of companies consider the competition as a factor, which means that the external market forces have a strategic role in the adoption decision-making process.

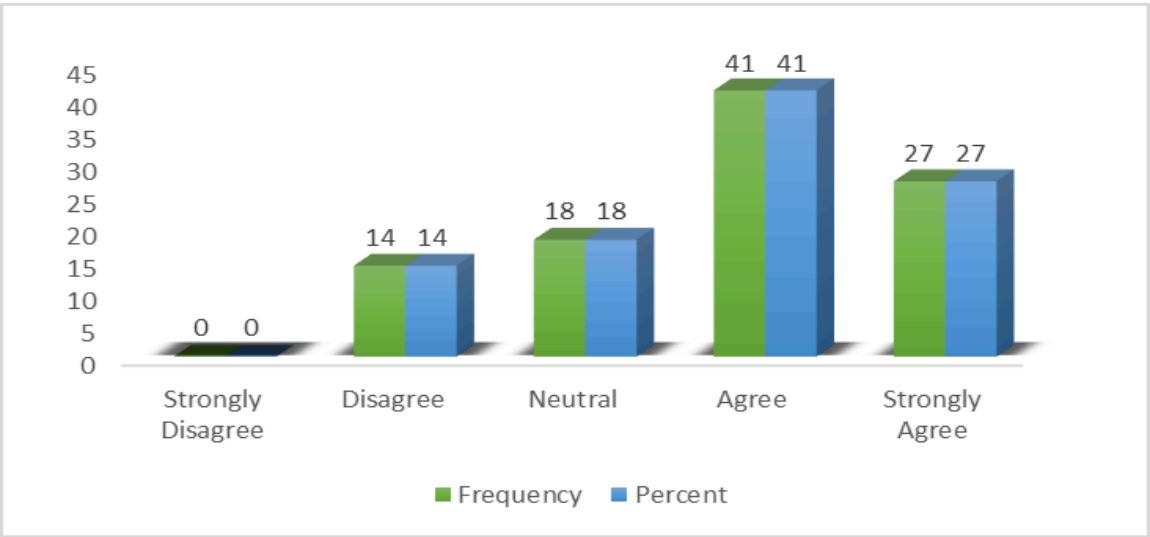

Figure 4.27

Competitors using cloud computing gain a significant competitive advantage.

The indicated situation suggests that the people who took part in the survey view the competitors who utilize cloud computing as a winner in the race for the market. The percentage of those who agreed or strongly agreed (68%) is significantly large; 18% were neutral, and only 14% disagreed. This indicates that the respondents strongly believe in the potential of cloud technologies to be the main factor of competition rather than being just supportive technologies.

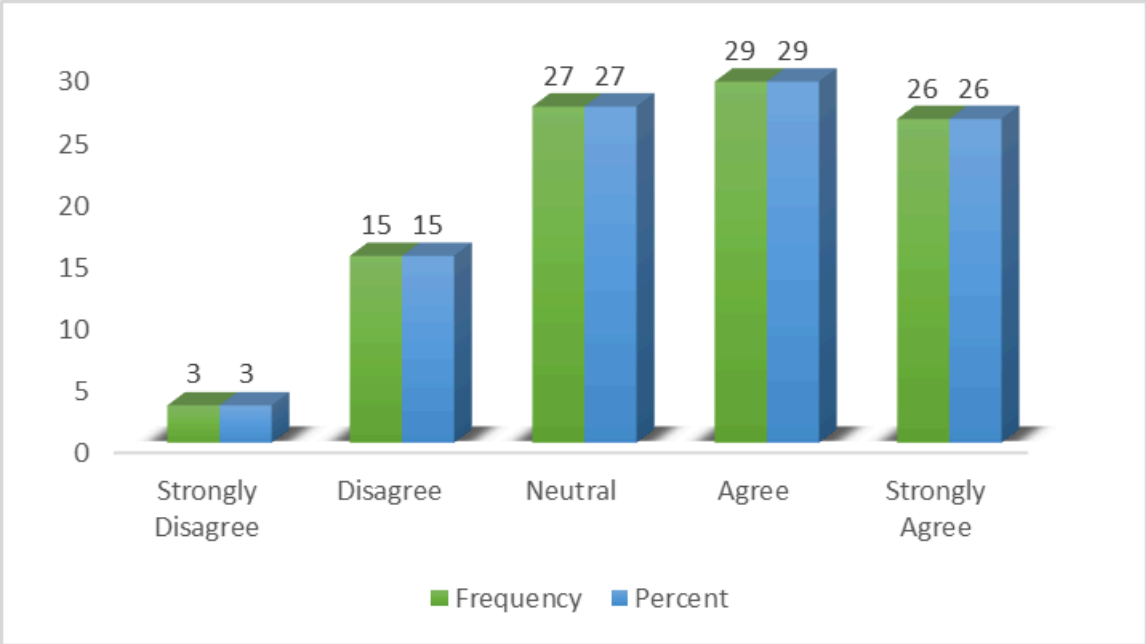

Figure 4.28

Reliable internet connectivity is critical for adopting cloud computing.

This illustrates the fundamental role that dependable internet connection plays in the process of moving to the cloud. Approximately 55% A or SA, 27% were N, and 18% D. The results highlight that internet reliability is regarded as a must-have, yet the moderate neutrality and disagreement imply that in certain companies, the issues of connectivity may not be of a critical nature to all.

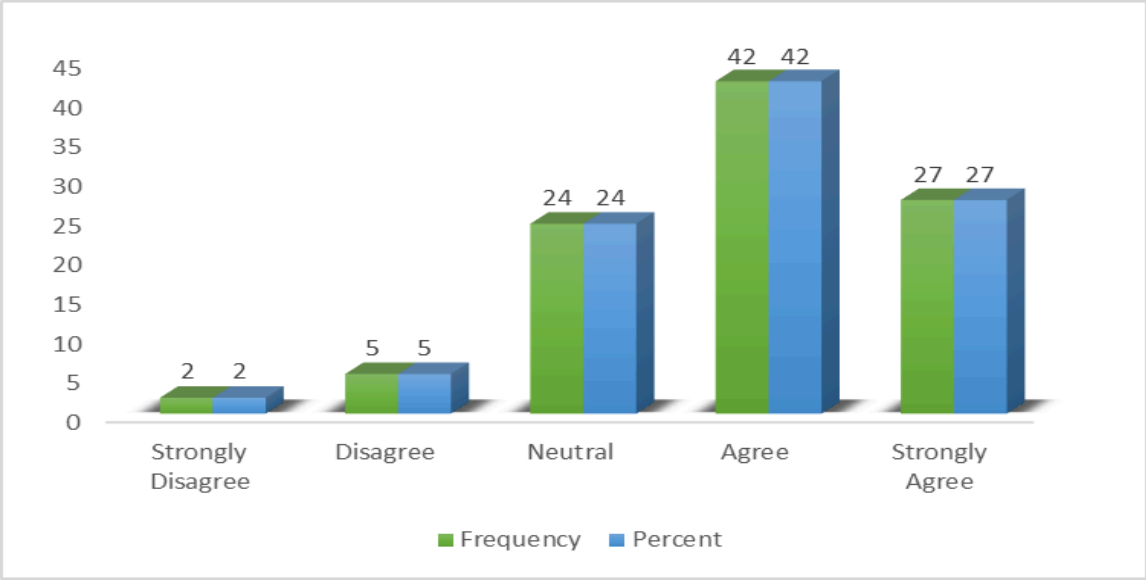

Figure 4.29

Internet speed in our area is sufficient to support cloud computing adoption.

This shows that there is a strong belief in the sufficiency of the internet speed. Approximately 69% A or SA, 24% were N and only 7% D. Thus, it can be interpreted that the majority of the local respondents consider internet speeds to be suitable for cloud adoption and they will not face any technological barriers that might hinder them to migrate to the cloud technology smoothly.

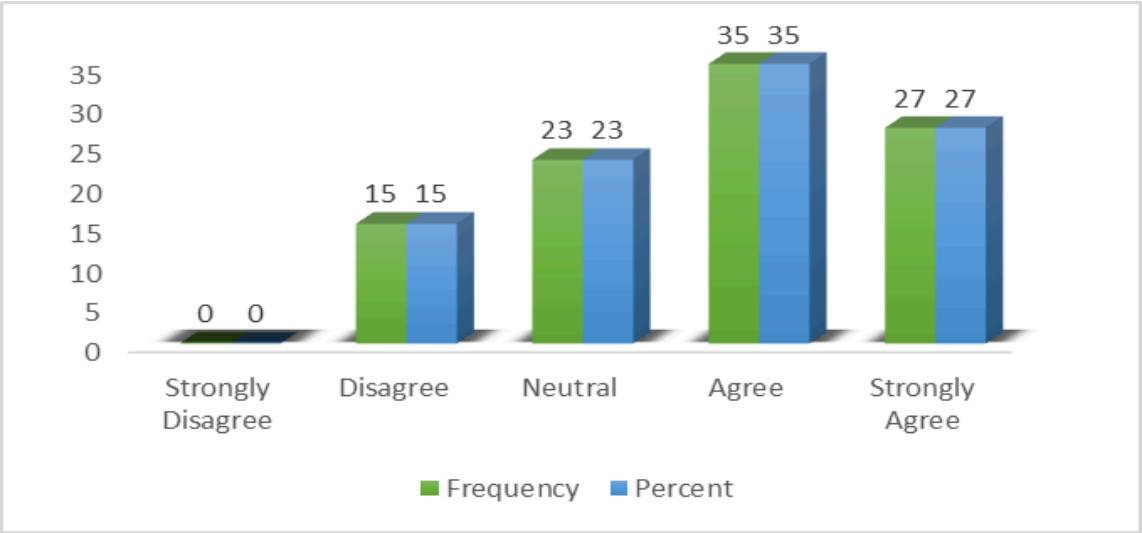

Figure 4.30

Our geographical location affects the availability of cloud service providers.

The outcome of this study is that the place where a company is located greatly determines the presence of cloud services it can access. Approximately 62% of the respondents rated it A or SA, 23% were Neutral, and 15% rated it D. Thus, the regional factors are still determining the access to the providers, which may result in an uneven playing field for the different organisations depending upon their locations.

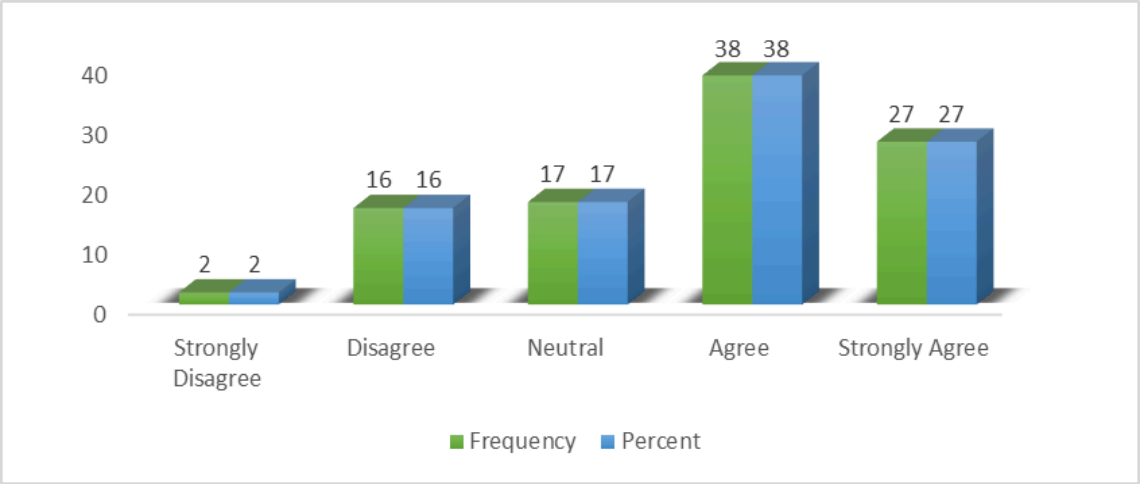

Figure 4.31

Location-specific challenges hinder our ability to adopt cloud technologies.

This demonstrates that the specific difficulties related to the location are the main reason for the cloud not being used at all in the case of many respondents. Approximately 65% A or SA, 17% were N, and 18% D. This implies that although geographical factors may not completely prevent the adoption of the cloud, they do create obstacles that organisations will have to consider and get around in their planning of cloud strategies.

4.6 Findings on Perceived Risks and Barriers

The research explored the participants' views about the risks and troubles in the adoption of cloud computing, emphasising vendor lock-in, service reliability, and data control. The frequencies and percentages of answers to six main statements are shown in Table 4.6.

Table 4.6

Perceived Risks and Barriers

Statement		SD	D	N	A	SA
I am concerned about being locked into a specific cloud vendor's ecosystem.	Frequency	8	13	23	30	26
	Percent	8	13	23	30	26
Vendor lock-in limits our ability to switch providers without significant cost or effort.	Frequency	1	16	19	32	32
	Percent	1	16	19	32	32
Frequent downtime or outages are a major concern with cloud services.	Frequency	5	11	16	37	31
	Percent	5	11	16	37	31
The reliability of cloud services affects our willingness to adopt them.	Frequency	6	17	19	35	23
	Percent	6	17	19	35	23
I am concerned about losing control over data stored in the cloud.	Frequency	5	16	19	35	25
	Percent	5	16	19	35	25
Using cloud services compromises our ability to manage and secure our data effectively.	Frequency	1	15	21	34	29
	Percent	1	15	21	34	29

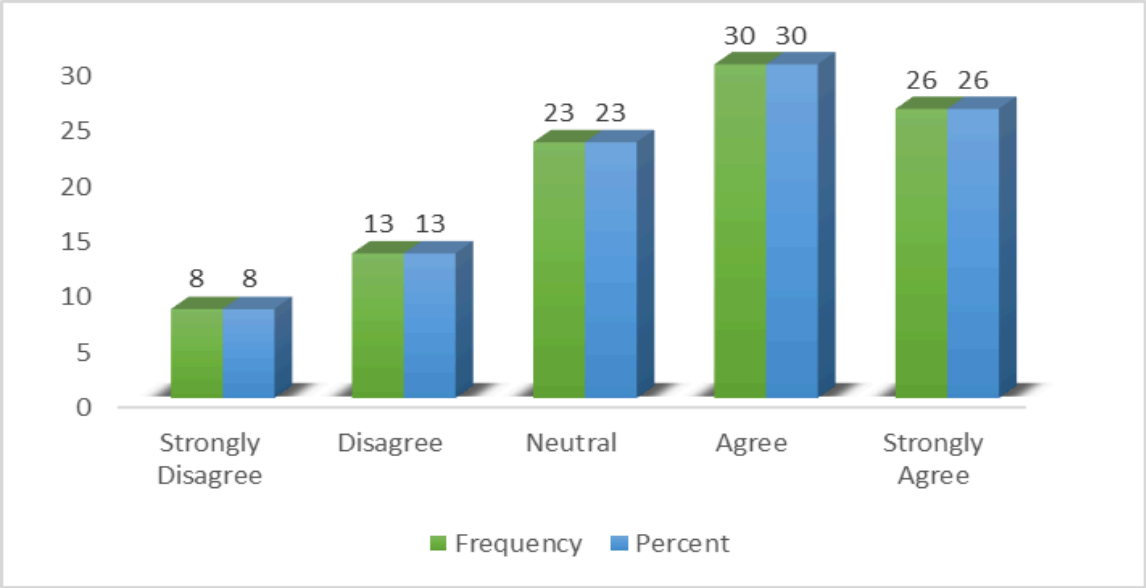

Figure 4.32

I am concerned about being locked into a specific cloud vendor's ecosystem.

This indicates that vendor lock-in is quite significant issue with 56% A or SA, 23% N and 21% D. This means that although the majority of companies are aware of the danger of surviving off a single provider, a significant part either dismisses the matter or does not know yet whether it could have a big effect or not.

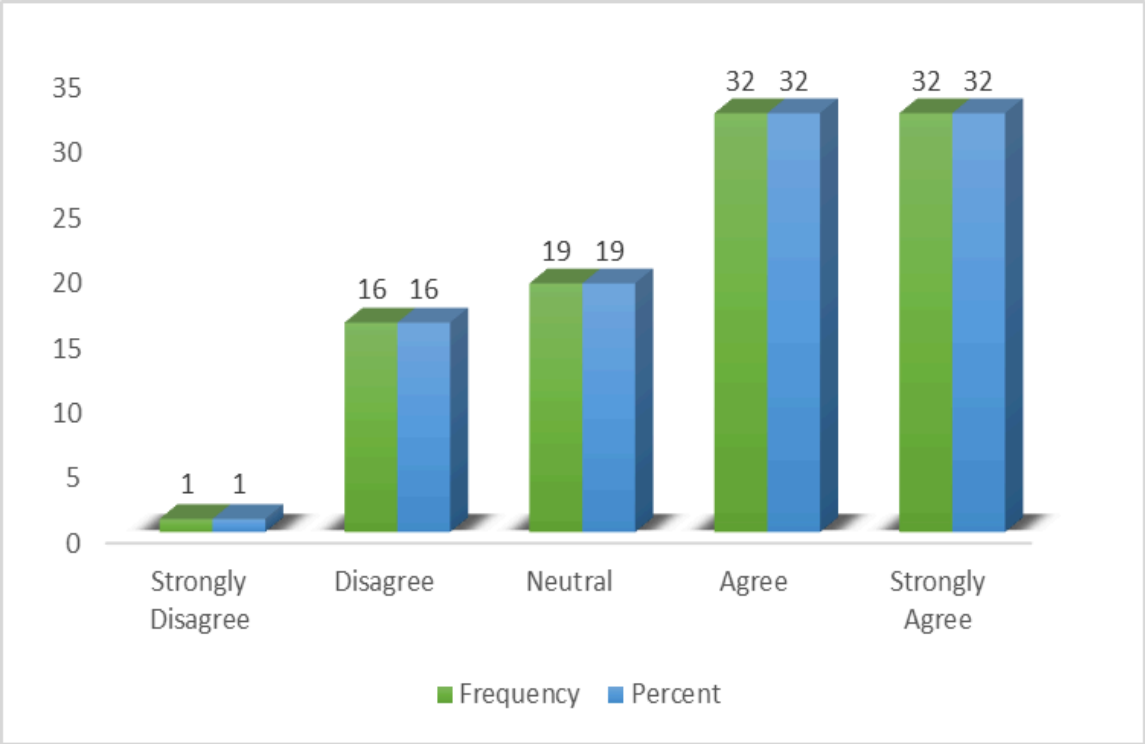

Figure 4.33

Vendor lock-in limits our ability to switch providers without significant cost or effort.

This showcases a deep consensus over the shortcomings of vendor lock-in. The responses came in with 64% A or SA, 19% N, and merely 17% D. Thus, the survey takers consider changing suppliers to be a pricey and complicated process, which in turn strengthens the view that vendor lock-in is a major obstacle in the cloud adoption plans.

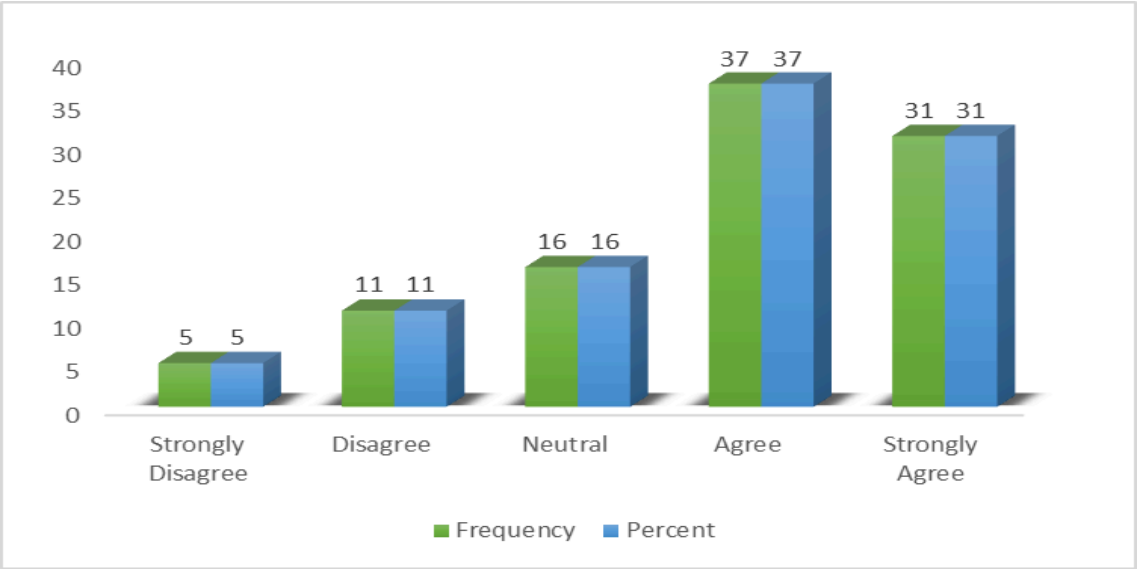

Figure 4.34

Frequent downtime or outages are a major concern with cloud services.

Frequent downtimes or outages are indicated as a major issue by the data presented in Figure 4.34. The percentages are as follows: 68% A or SA, 16% were neutral, and 16% D. Thus, it is clear that reliability of the service is an important demand, and interruptions might considerably hurt the trust of companies in using cloud computing.

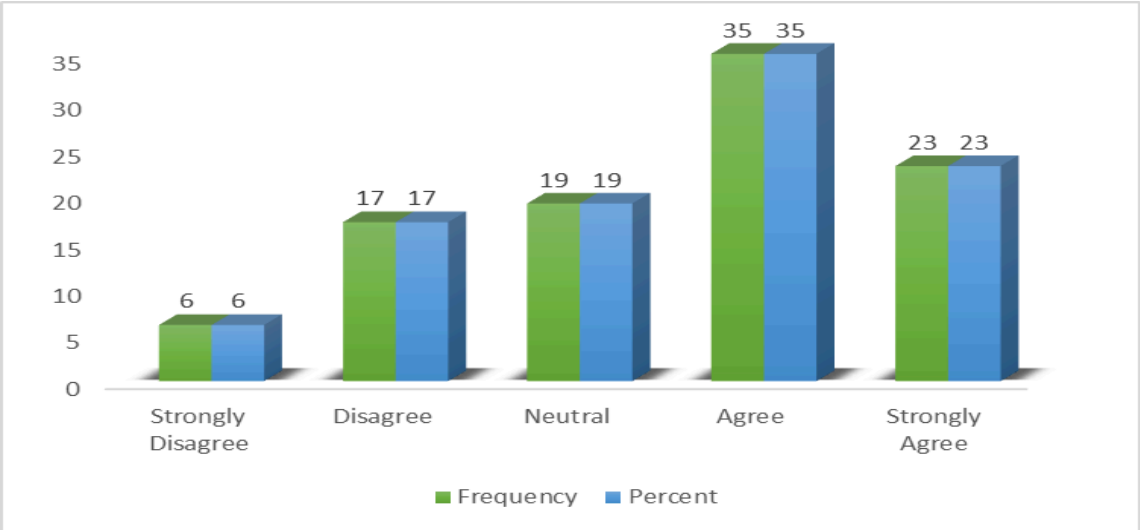

Figure 4.35

The reliability of cloud services affects our willingness to adopt them.

This indicates decisively that the trust placed in cloud services has a very strong impact on the willingness to use them. Approximately 58% expressed complete agreement or strong agreement with this statement, 19% were neutral, and 23% disagreed. This situation mirrors the fact that although the majority of the firms consider reliability to be a key factor, a significant part of them is still very careful, thus implying that there are different degrees of tolerances towards possible interruptions of service.

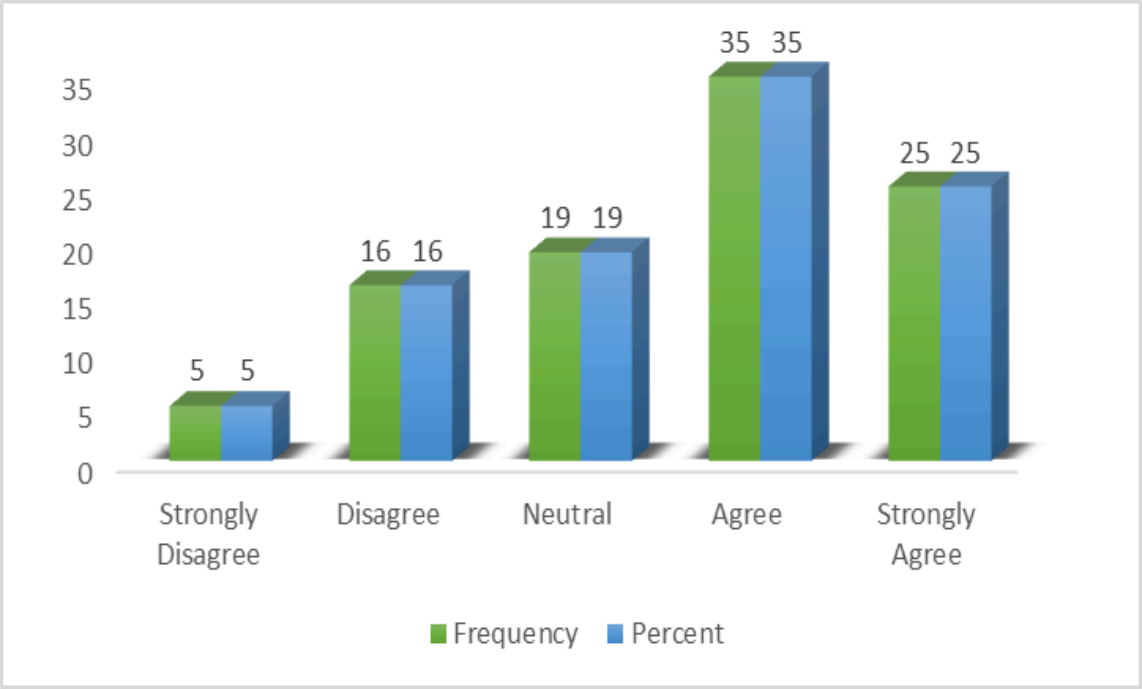

Figure 4.36

I am concerned about losing control over data stored in the cloud.

This clearly shows worries about not being able to manage data that is stored in the cloud. A whopping 60% were A or SA, 19% were N, and 21% were D. This is a clear case of many companies being nervous about giving up control over their data which leads to a demand for cloud providers to implement even better security measures and practice more transparency in their operations.

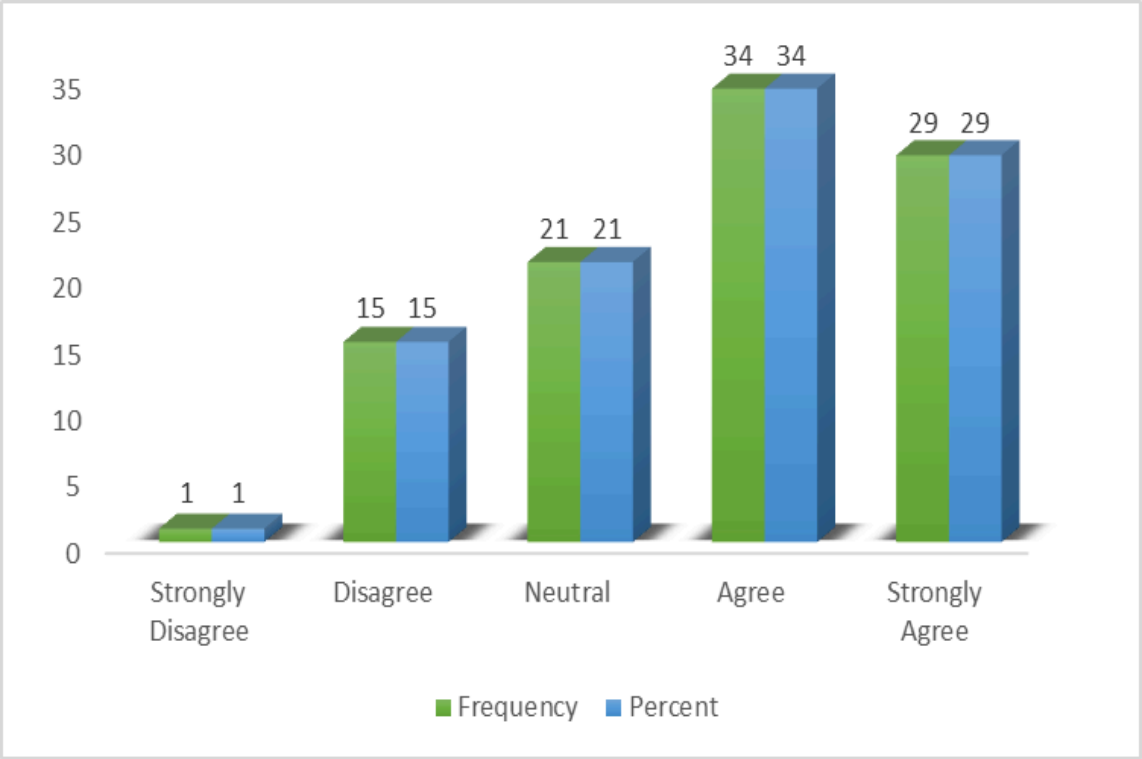

Figure 4.37

Using cloud services compromises our ability to manage and secure our data effectively.

This is indicative of cloud adoption creating fears concerning data management and security. To be more specific, around 63% A or SA, 21% were N, and 16% D. These findings imply that, even though companies are aware of the advantages of the cloud, they are still hesitant to think that they could have total control over and secure handling of data in a cloud-based environment.

4.7 Findings on Perceived Usefulness and Benefits

The study looked into the opinions of the respondents about the advantages and the usefulness of cloud computing; this included reduction in costs, scalability, operational efficiency, ease of adoption, and user-friendliness. Respondents' vaccinations tosix core assertions are depicted in Table 4.7 through frequency and percentage.

Table 4.7

Perceived Usefulness and Benefits

Statement		SD	D	N	A	SA
Cloud computing helps reduce overall IT costs for our organisation.	Frequency	6	8	30	30	26
	Percent	6	8	30	30	26
Adopting cloud services leads to better cost management.	Frequency	3	22	24	29	22
	Percent	3	22	24	29	22
Cloud computing provides the flexibility to scale resources as needed.	Frequency	5	12	22	41	20
	Percent	5	12	22	41	20
The scalability of cloud services enhances operational efficiency.	Frequency	3	18	29	27	23
	Percent	3	18	29	27	23
Cloud computing is easy to adopt and integrate into existing business operations.	Frequency	0	12	29	34	25
	Percent	0	12	29	34	25
Employees find cloud-based tools and services user-friendly and efficient.	Frequency	6	14	15	40	25
	Percent	6	14	15	40	25

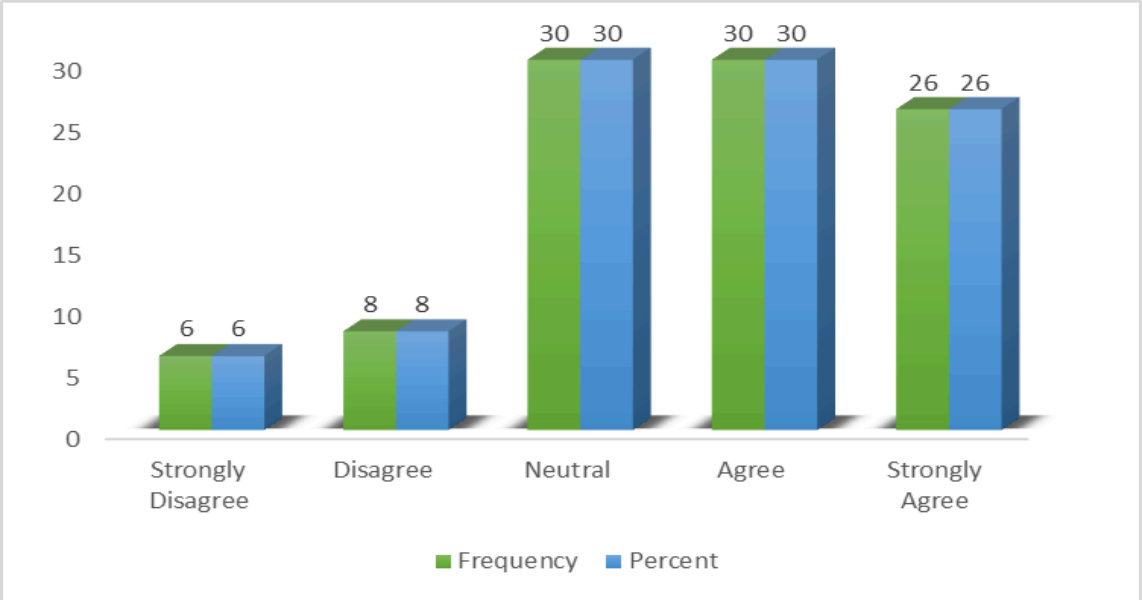

Figure 4.38

Cloud computing helps reduce overall IT costs for our organisation.

It is evident from this that the majority of the people associate cloud computing with a decrease in costs. Approximately 56% of the respondents marked A or SA, 30% marked N, while just 14% marked D. Therefore, it can be said that the majority of the

individuals surveyed acknowledge the cost advantages of switching to the cloud, but the fairly large number of N responses points to the situation where not all companies have fully realized or accounted for their savings.

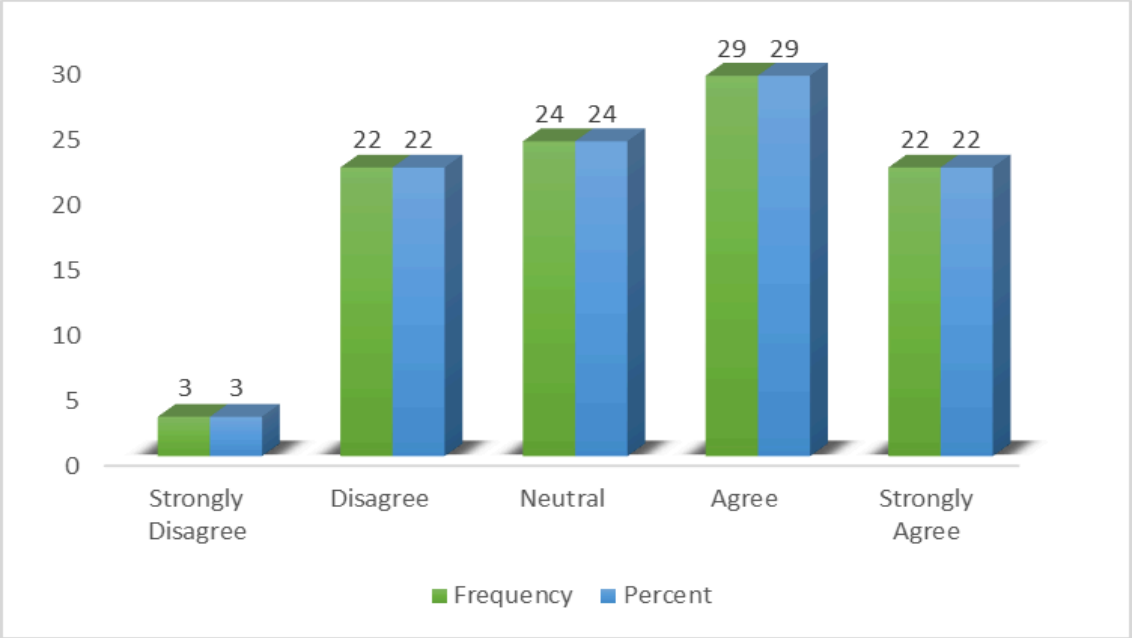

Figure 4.39

Adopting cloud services leads to better cost management.

A mixed picture emerges regarding the effect of cloud services on cost management. 51% of the respondents have given either A or SA rating while 25% have marked N and a considerable 25% have rated D. This indicates that most organizations consider cloud adoption as giving better financial control but there are still areas of doubt and disbelief which point to different practical experiences with budget management.

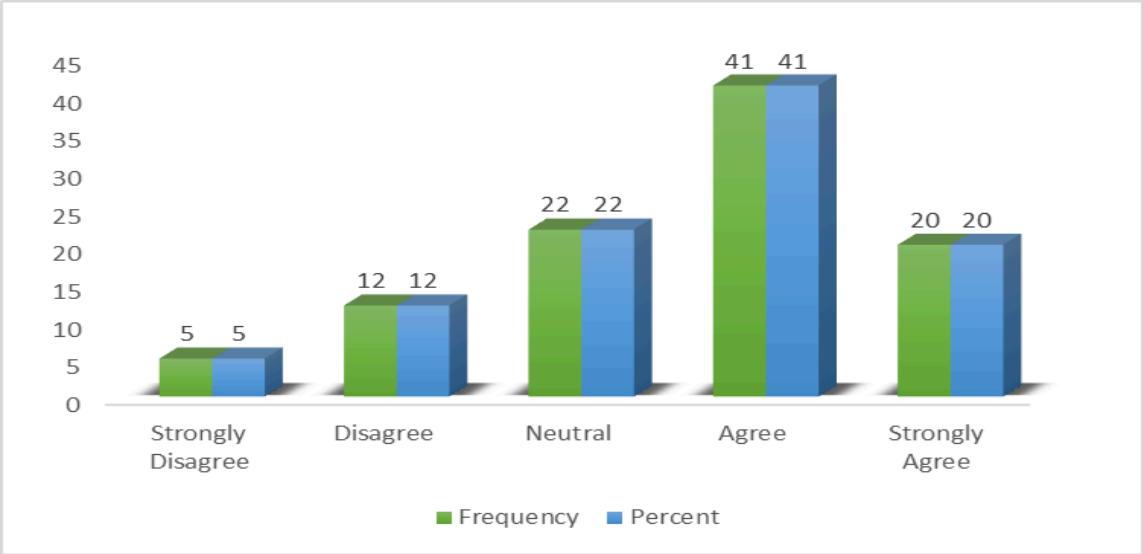

Figure 4.40

Cloud computing provides the flexibility to scale resources as needed.

This reveals an enormous trust in scalability as a major benefit of cloud computing. A. or SA, 61% and B, C, D - 39%: That is how the opinions were divided. The results indicate that the ability to easily scale up and down is one of the most important factors for companies choosing to use the cloud, which, in turn, boosts their adaptability to demand fluctuations.

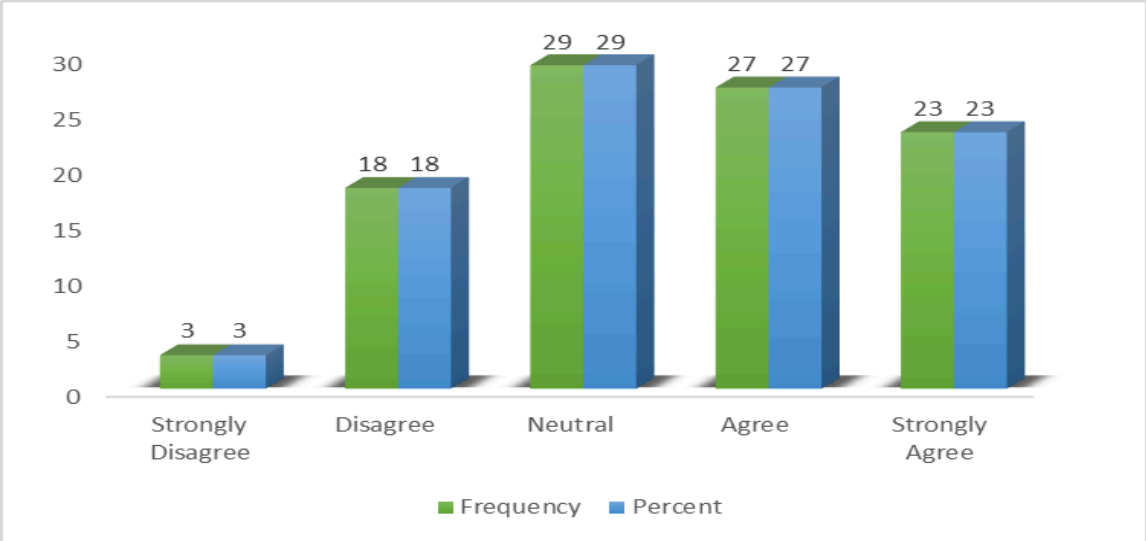

Figure 4.41

The scalability of cloud services enhances operational efficiency.

Scalability is thereby proved to be associated with improvement of operational efficiency. Approximately 50% were A or SA, 29% were N and 21% were D. It indicates that although a lot of companies recognize the benefits, the big N indicates that the operational scalability impact is still not equally felt among the companies.

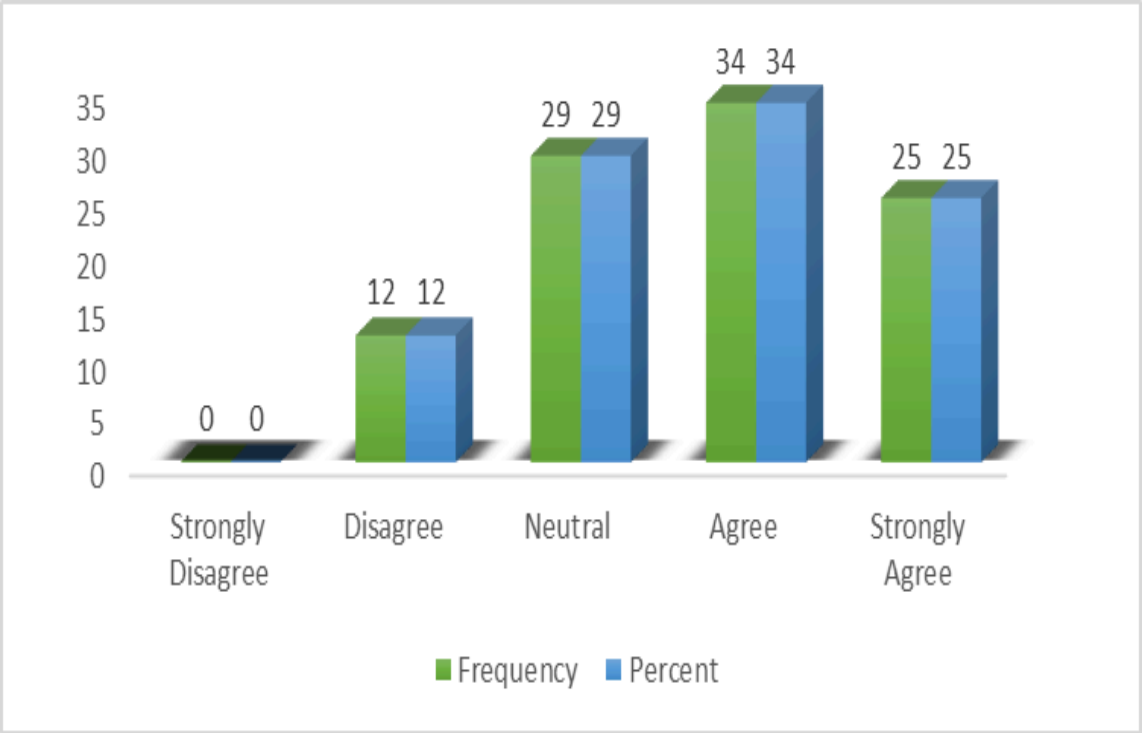

Figure 4.42

Cloud computing is easy to adopt and integrate into existing business operations.

This is indicative of a positive view concerning the simplicity of cloud integration. Almost 59% rated it as A or SA, 29% were neutral, and merely 12% disagreed. Thus, a majority of the people surveyed consider the process of moving to the cloud quite easy, however, the significant number of neutral opinions indicates that some companies are still struggling with the integration or have not completely moved to the cloud.

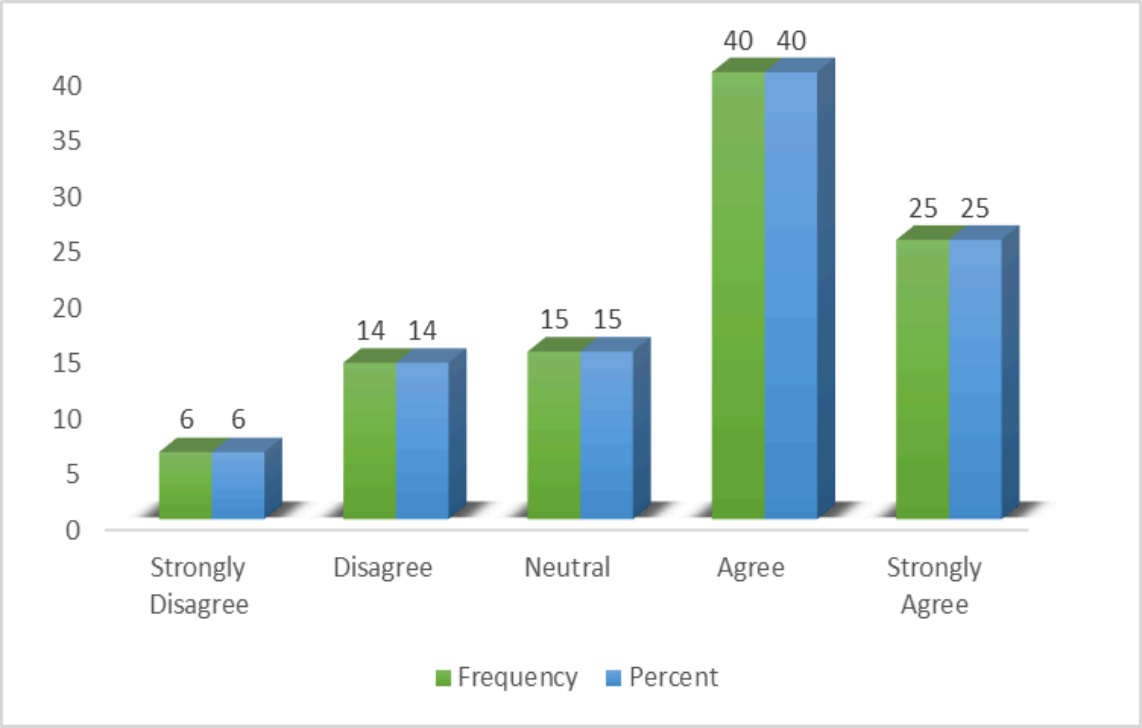

Figure 4.43

Employees find cloud-based tools and services user-friendly and efficient.

The results indicate that the majority of employees consider the alternative tools through the cloud as easy to use and efficient. Thus, approximately 65% agreed or strongly agreed, 15% stayed neutral and 20% disagreed. It is a good sign for companies that the majority of their staff using the internet are improving their performance and productivity, but still, some are having a hard time getting used to the digital tools.

4.8 Findings of Trust in Cloud Service Providers

The investigation looked into how the participants viewed the trust factor in cloud service providers, narrowing down the factors to reputation, compliance with security standards, transparency, and communication of security policies, among others. The frequency and percentage of answers to four important statements are shown in Table 4.8.

Table 4.8

Trust in Cloud Service Providers

Statement	SD	D	N	A	SA
The reputation of cloud service providers influences our trust in their services.	Frequency	6	17	19	28
	Percent	6	17	19	28
Compliance with industry security standards enhances trust in cloud providers.	Frequency	6	15	19	31
	Percent	6	15	19	31
Cloud service providers are transparent about how they handle and protect data.	Frequency	1	16	23	30
	Percent	1	16	23	30
Providers' clear communication about security policies builds trust.	Frequency	5	13	26	36
	Percent	5	13	26	36

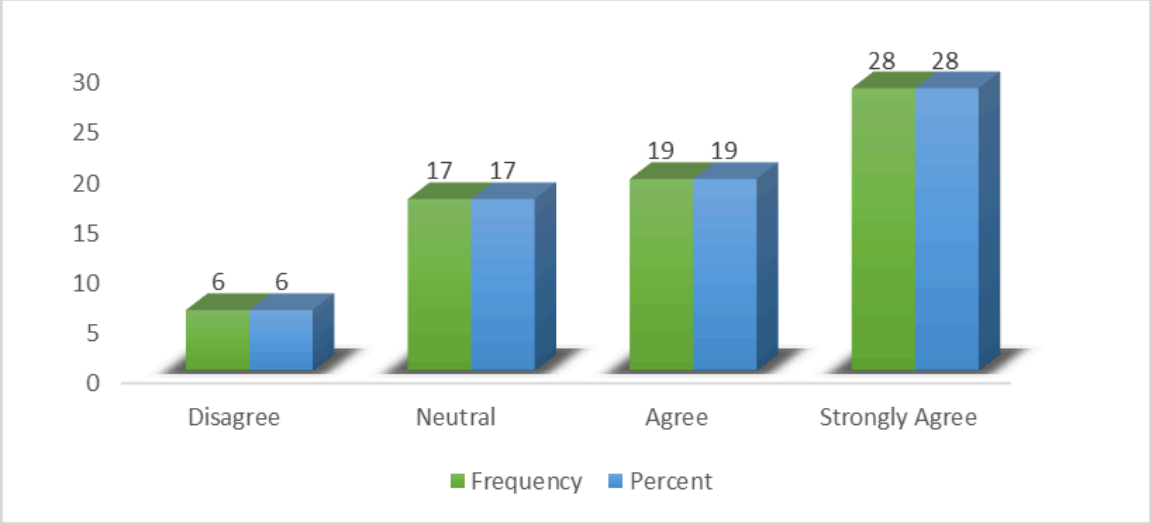

Figure 4.44

The reputation of cloud service providers influences our trust in their services.

The trustworthiness is very much dependent on the reputation of the cloud service providers as the data indicates. Nearly half of the respondents (47%) either agreed (A) or strongly agreed (SA), whereas 19% opted for neutral (N) and 23% disagreed (D) with the statement. This infers that provider reputation is a major trust factor for most of the organisations, still, there are some who wait and see, thus, inferring that the trust should not solely be based on the provider's reputation.

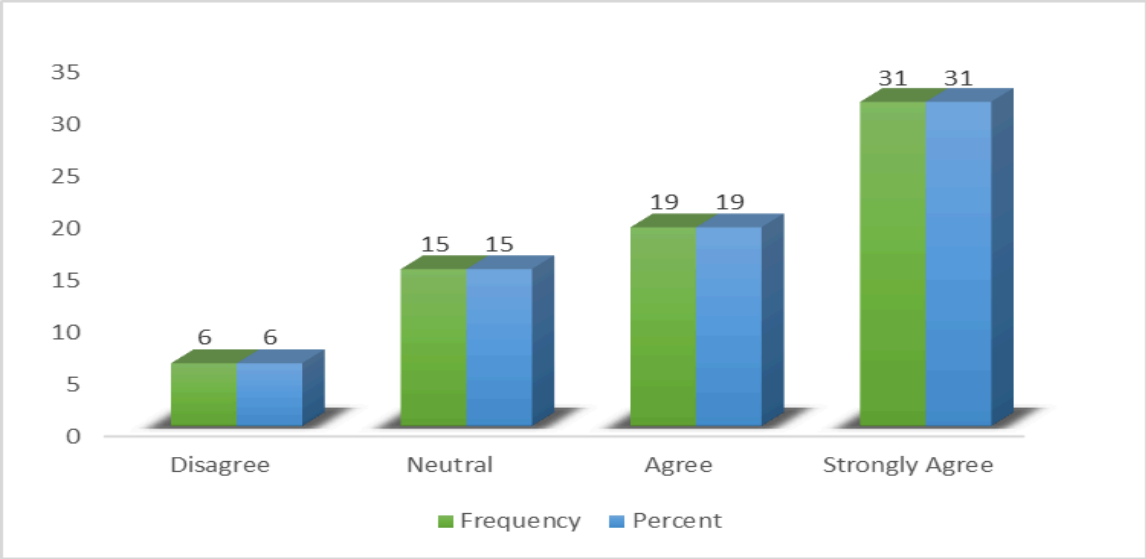

Figure 4.45

Compliance with industry security standards enhances trust in cloud providers.

It is pointed out that following the security standards of the industry leads to a significant increase in trust. Approximately 50% A or SA, 19% were N, and 21% D. The results imply that accepted standards give security, but still some companies are in doubt or not convinced that the mere fact of compliance is enough to secure and trustworthy the provider.

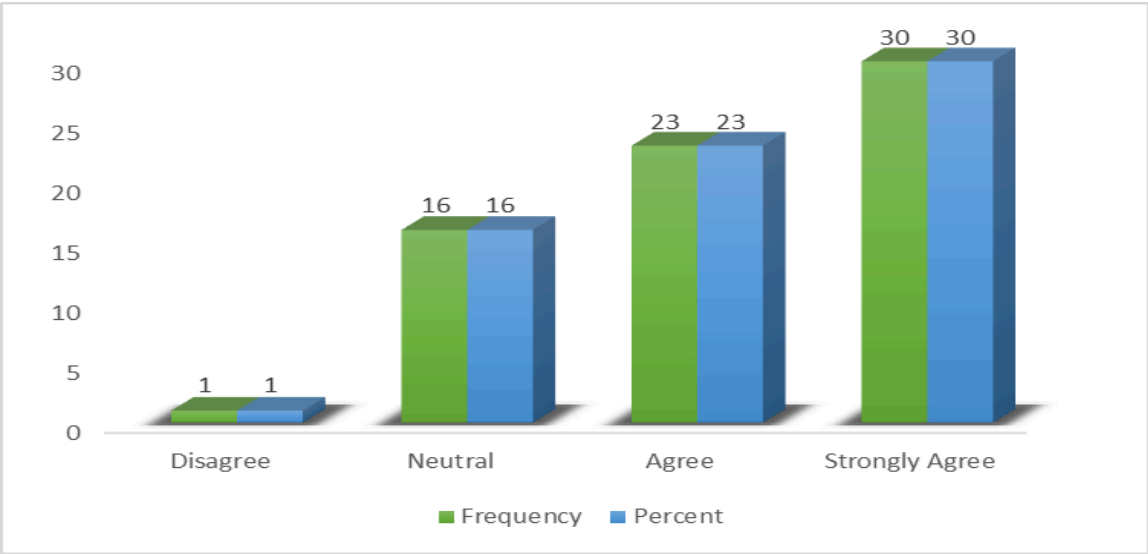

Figure 4.46

Cloud service providers are transparent about how they handle and protect data.

It is shown that data handling's transparency is regarded as a factor to build trust. Roughly 53% agreed strongly or simply agreed, 23% remained neutral, and 17% disagreed. It means that although the majority of the respondents are in favour of openness in data practices, the neutrality indicates that not all organisations are considering providers as being fully transparent in practice.

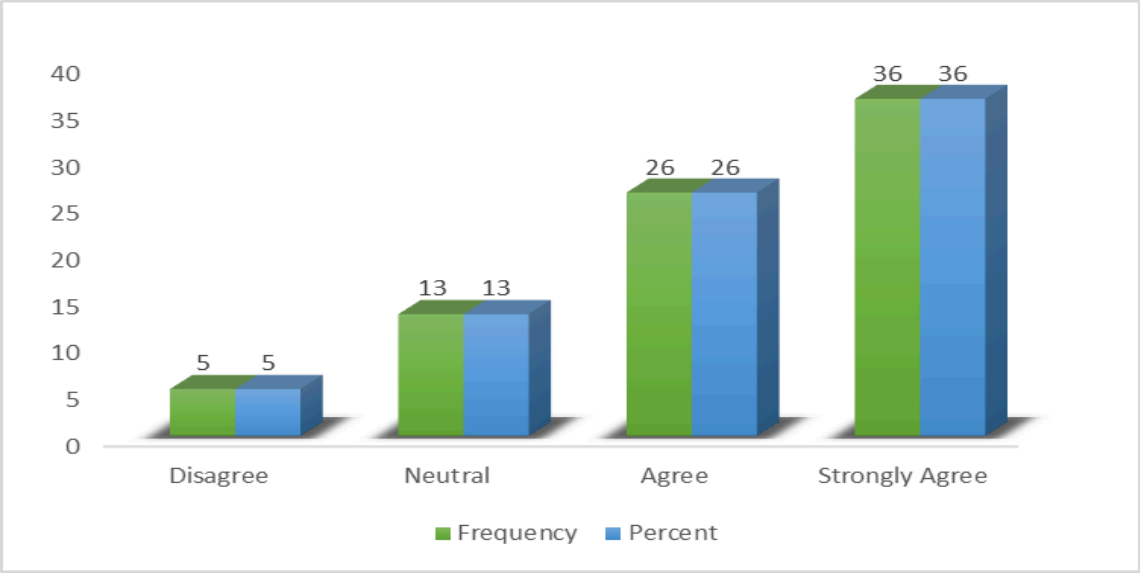

Figure 4.47

Providers' clear communication about security policies builds trust.

The communication of security policies has been rated as the number one factor contributing to trust. A large percentage of respondents, comprising 62% who were A or SA, 26% who were N, and only 18% who were D. This underscores the importance of communication as a means of handling or conferring trust, just as technical measures, where the clarity of policies is considered the trust builder, are indispensable.

4.9 Findings on Adoption of Cloud Computing

In this part, the opinions of the respondents concerning the usage of cloud computing in their firms are indicated. Organisational Readiness, Benefits, Reliability, Flexibility, Skills, Collaboration, Trust, and Leadership Support are the factors that are

being discussed in connection to the adoption of cloud computing in the organisations. The responses related to the ten crucial statements are presented in terms of their frequency and percentages in Table 4.9.

Table 4.9

Adoption of Cloud Computing

Statement		SD	D	N	A	SA
Our organisation is actively considering adopting cloud computing.	Frequency	6	10	24	32	28
	Percent	6	10	24	32	28
Cloud computing offers significant advantages for our business operations.	Frequency	4	10	27	34	25
	Percent	4	10	27	34	25
The adoption of cloud computing will help us reduce IT infrastructure costs.	Frequency	3	16	19	39	23
	Percent	3	16	19	39	23
Cloud computing services are reliable and meet our business needs.	Frequency	4	14	23	33	26
	Percent	4	14	23	33	26
We are concerned about data security when using cloud computing services.	Frequency	3	13	23	32	29
	Percent	3	13	23	32	29
The flexibility and scalability of cloud computing are important for our business.	Frequency	4	13	20	40	23
	Percent	4	13	20	40	23
Our staff has the necessary skills and knowledge to adopt cloud computing.	Frequency	6	15	22	32	25
	Percent	6	15	22	32	25
Cloud computing helps improve collaboration and communication within our organisation.	Frequency	7	12	20	32	29
	Percent	7	12	20	32	29
We trust cloud service providers to handle our sensitive data securely.	Frequency	3	16	26	30	25
	Percent	3	16	26	30	25
Our organisation's leadership is supportive of adopting cloud computing technologies.	Frequency	5	16	19	33	27
	Percent	5	16	19	33	27

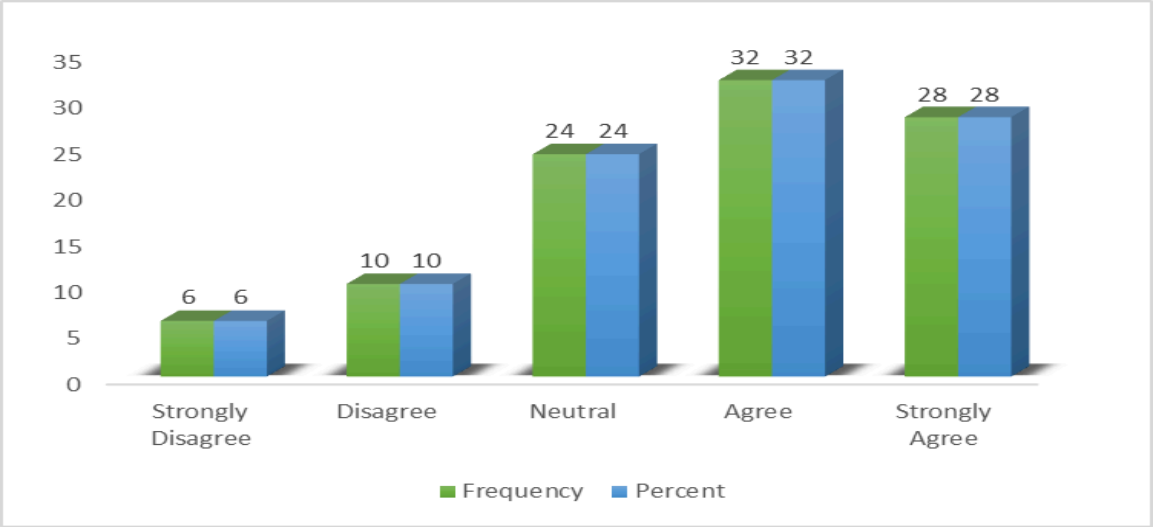

Figure 4.48

Our organisation is actively considering adopting cloud computing.

The results reveal that a large number of organisations are contemplating cloud implementation and the percentages giving their opinions are as follows: 60% A or SA, 24% N, and only 16% D. This signals a very strong tendency to use cloud services, but at the same time a considerable part is still unsure, hence it might be the case that providing information on the advantages and the risks would turn the undecided ones into the adopting ones.

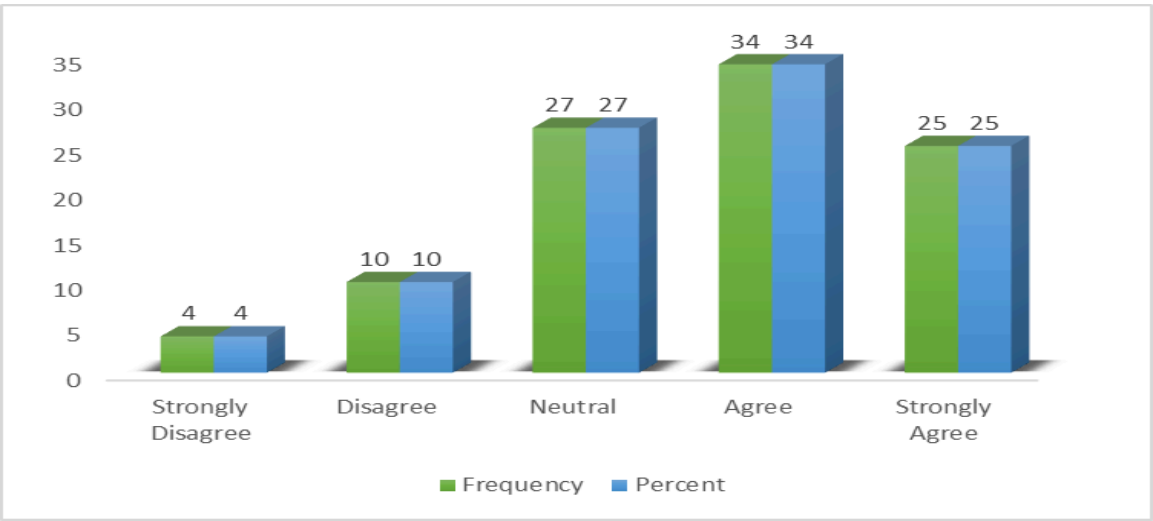

Figure 4.49

The adoption of cloud computing will help us reduce IT infrastructure costs.

This shows that most respondents have a very high opinion of cloud computing as a very advantageous solution. 59% A or SA, 27% were N, and 14% D. This implies that there is a clear acceptance of the business value of cloud solutions, but the neutrality signifies that some companies are still considering how these advantages relate to their situation.

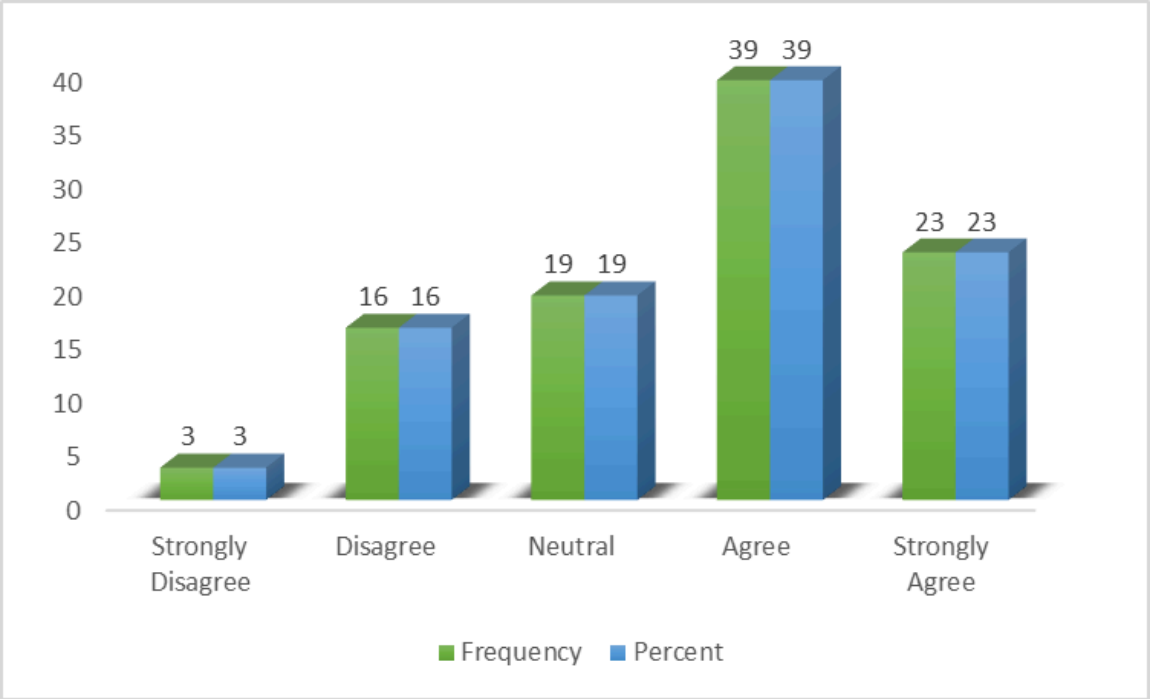

Figure 4.50

The adoption of cloud computing will help us reduce IT infrastructure costs.

The fact that cost reduction is seen as a major benefit of going to the cloud is reflected in this. Out of the total respondents, 62% were A or SA, 19% were N, and 19% were D. It can be concluded from these findings that financial efficiency is a key factor in cloud adoption, yet still, there are a few who doubt whether the savings will be real or not.

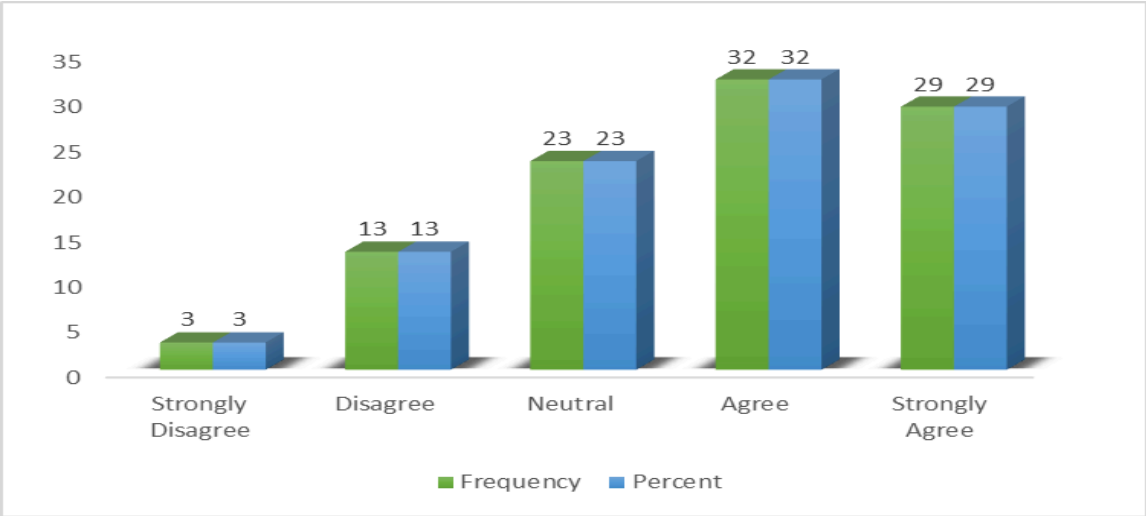

Figure 4.51

Cloud computing services are reliable and meet our business needs.

This indicates that the respondents believe in the trustworthiness of cloud services. The distribution of responses was as follows: 59% A or SA, 23% N, and 18% D. It can be concluded that a majority of the organizations trust the cloud providers, but still a big part is concerned about the fulfilment of their operational requirements by the services.

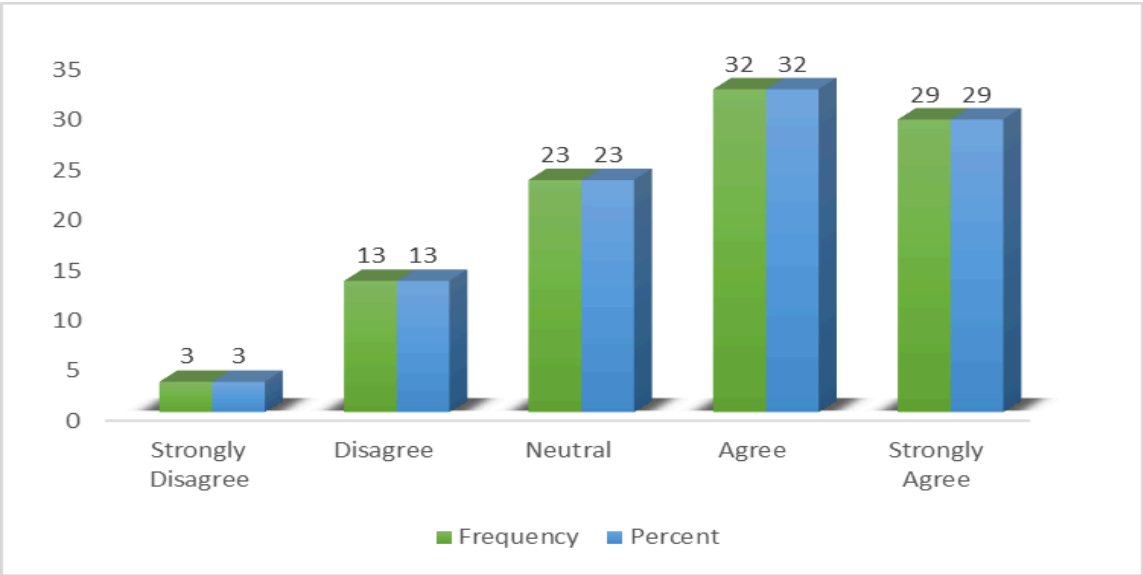

Figure 4.52

We are concerned about data security when using cloud computing services.

Drawing such conclusions will not be easy, as there will still be talks about the security of cloud systems. To make it clearer, 61% of the people chose A or SA, 23% voted N, and 16% indicated D, which means that even if the cloud is adopted, the data protection issues are still a major concern when organizations decide and they want better security guarantees from the suppliers.

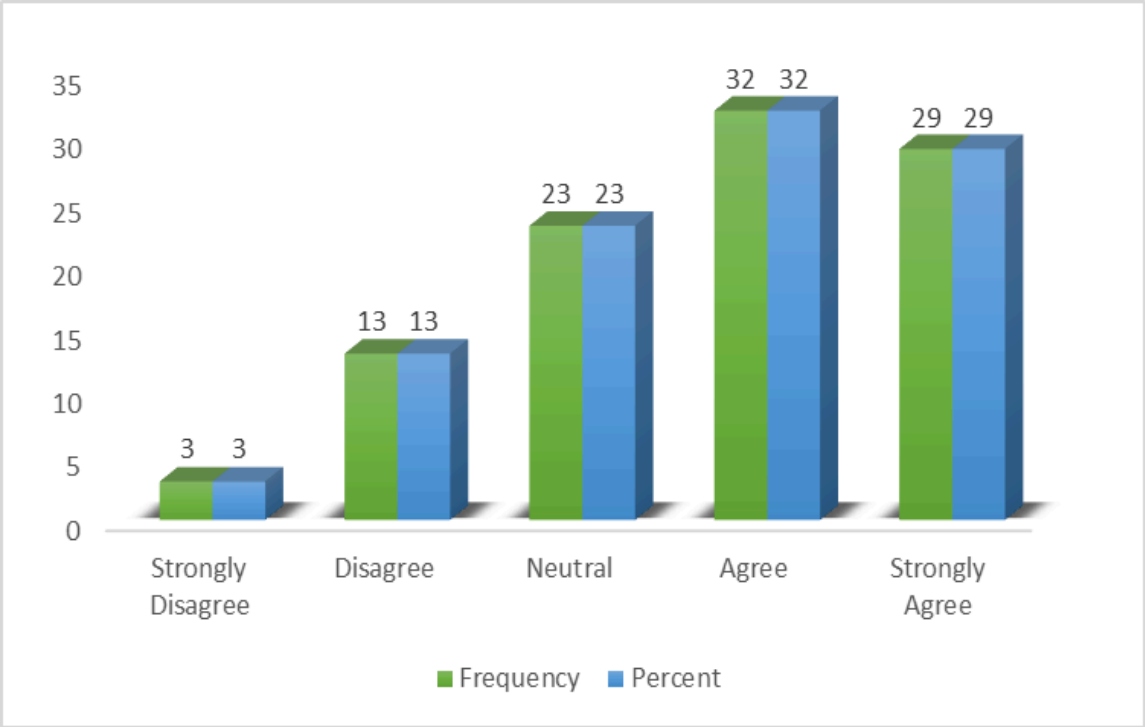

Figure 4.53

The flexibility and scalability of cloud computing are important for our business.

It is revealed by the figures that the trust in cloud agility and scalability is very high, 63% A or SA, 20% N, and 17% D. This indicates that among the users' viewpoints about the cloud services, the moldability is at the top place, which supports the argument that flexibility is the primary factor in the direct service of changing business requirements.

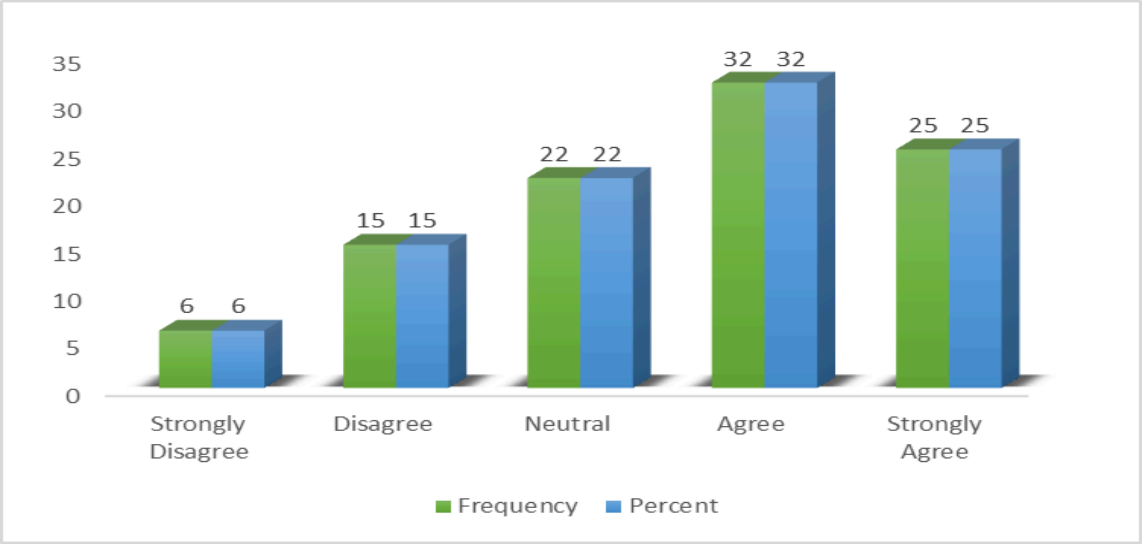

Figure 4.54

Our staff has the necessary skills and knowledge to adopt cloud computing.

This illuminates' perceptions of the personnel readiness for the adoption of cloud services. A little more than half, specifically 57%, reported agreement (A or SA), 22% were N, while 21% D. The implication is that although the majority think that the employees have the right skills, still a big part of the population either doubts the readiness of the staff or points out the need for further training and skill development.

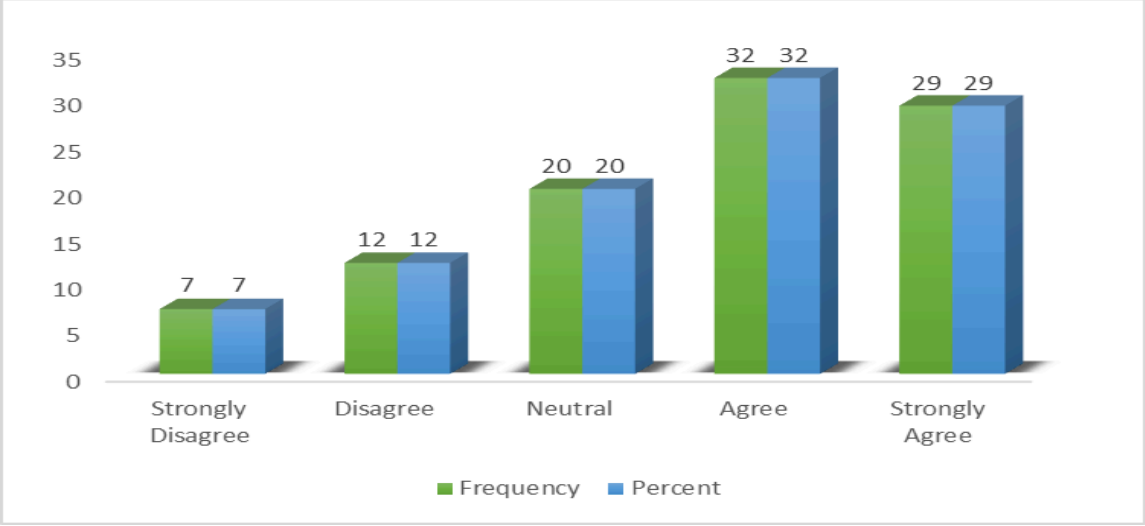

Figure 4.55

Cloud computing helps improve collaboration and communication within our organisation.

This is a clear display of positive attitudes towards collaboration, which are considered to be the main benefits. 61% of respondents were in agreement (A or SA), 20% N, and 19% D. It means that a majority of companies are recognizing the role of cloud-based tools in fostering teamwork and communication, while at the same time a small group is not convinced, possibly because of their past difficulties with implementation or integration.

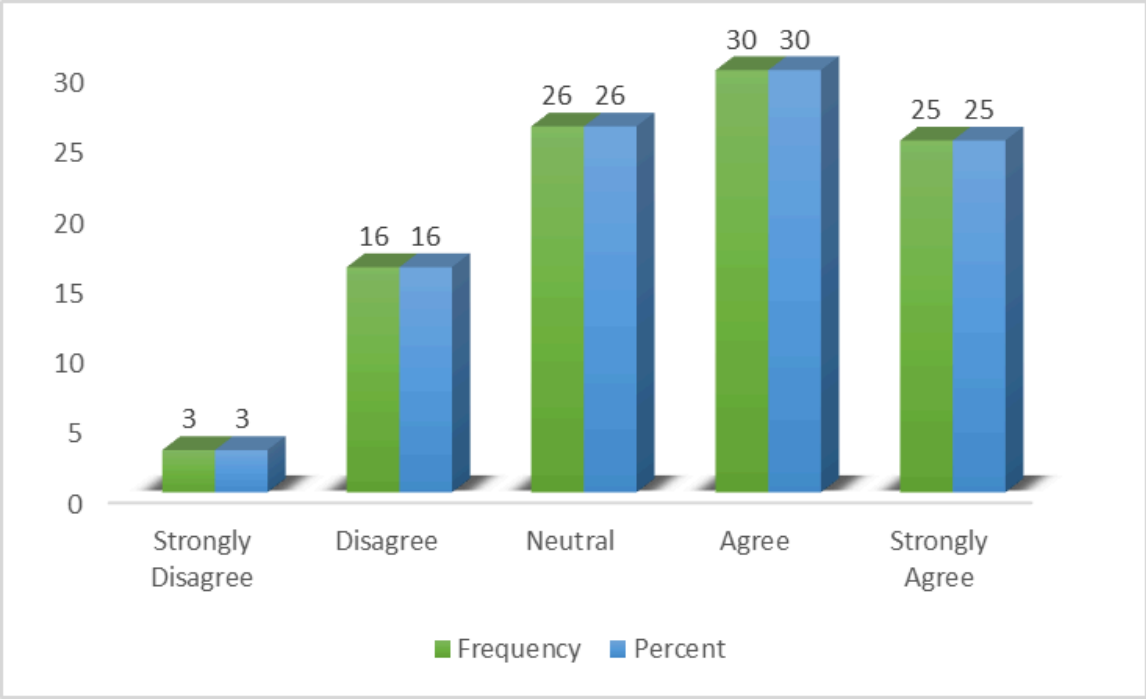

Figure 4.56

We trust cloud service providers to handle our sensitive data securely.

This indicates a moderate level of trust in the ability of service providers to manage sensitive data. Approximately 55% A or SA, 26% were N, and 19% D. Although trust is present for most, the great neutrality and disagreement show that there are still issues regarding data privacy and thus stronger provider transparency and guarantee become even more prominent.

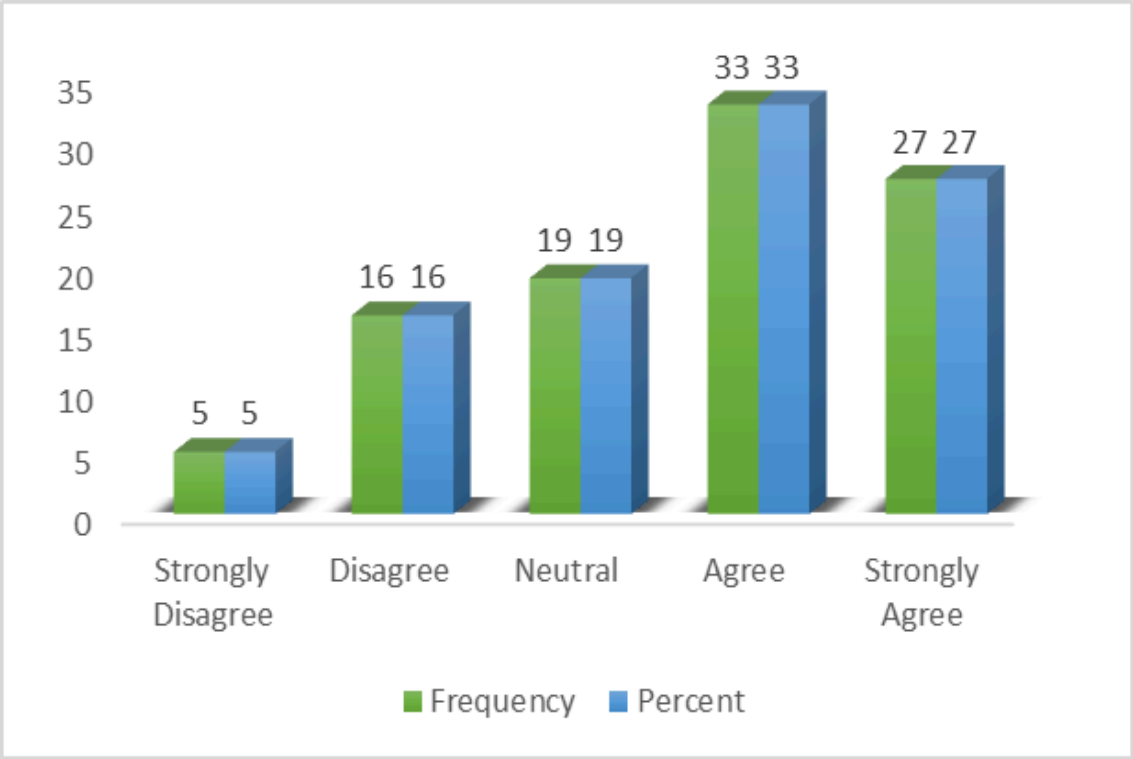

Figure 4.57

Our organisation's leadership is supportive of adopting cloud computing technologies.

The above-mentioned data exhibit a positive sign of leadership influence on the cloud adoption process. To be precise, 60% of the participants responded with A or SA, 19% were N, and 21% D. Therefore, it can be concluded that the leadership support is usually strong but not everywhere, thus, suggesting that commitment at the executive level might still be a barrier for some organizations' migrations to the cloud.

4.10 Descriptive Analysis

Table 4.10 includes the descriptive statistics of the study variables (N = 100), comprising the participants' demographic traits and main variables associated with cloud computing adoption.

Table 4.10

Descriptive Statistics

	N	Mean		Std. Deviation
	Statistic	Statistic	Std. Error	Statistic
What is your age?	100	2.08	.106	1.061
What is your gender?	100	1.45	.050	.500
What is your current employment status?	100	2.53	.153	1.534
Which industry do you currently work in?	100	2.83	.168	1.676
What is your highest level of education?	100	3.60	.091	.910
How many years of experience do you have in the field of AI or Machine Learning?	100	2.39	.107	1.072
Which AI/Machine Learning techniques have you used in your work?	100	3.40	.142	1.421
Which programming languages do you frequently use in your AI/ML projects?	100	2.77	.164	1.638
Cybersecurity Concerns	100	4.1400	.06966	.69660
Organizational Factors	100	4.0400	.07095	.70953
Environmental Factors	100	4.1400	.06360	.63596
Perceived Risks and Barriers	100	4.0900	.07667	.76667
Perceived Usefulness and Benefits	100	3.9800	.07245	.72446
Trust in Cloud Service Providers	100	3.9300	.08319	.83188
Adoption of Cloud Computing	100	4.0500	.07160	.71598
Valid N (listwise)	100			

The summary statistics (N = 100) show that the people who took part in the study gave their opinions that were mostly in the middle or even a bit above the middle for all the important constructs. The mean scores of cybersecurity concerns and environmental factors (4.14) were the highest ones, so it can be deduced that the respondents had a strong understanding of security issues and environmental factors affecting the cloud adoption to a large extent. Organisational factors (4.04) and the use of cloud computing (4.05) were also evaluated as positive, while perceived usefulness and benefits (3.98), as well as trust in cloud service providers (3.93), obtained slightly lower but still good scores. All in all, the data clearly show a positive opinion towards cloud adoption, which

is indicated by the relatively low standard deviation that confirms the uniformity of the responses.

4.11 Hypothesis Testing

H1: There is a significant effect of cybersecurity concerns (data privacy, confidentiality, integrity, availability, perceived risk of data breaches) and the adoption of cloud computing.

Table 4.11

Logistic Regression Model Fit and Goodness-of-Fit Statistics for Cloud Computing Adoption

Category	Statistic	Value	df	Sig.
Model Fitting Information	-2 Log Likelihood (Intercept Only)	189.202	–	–
	-2 Log Likelihood (Final)	158.693	–	–
	Chi-Square	30.509	5	0
Goodness-of-Fit	Pearson	216.883	217	0.489
	Deviance	141.423	217	1
Pseudo R-Square	Cox and Snell	0.263	–	–
	Nagelkerke	0.299	–	–
	McFadden	0.144	–	–

Interpretation

The outcomes from logistic regression point out a good model for predicting the adoption of cloud computing. The model fitting details present a significant enhancement compared to the intercept-only model ($\chi^2 = 30.509$, df = 5, $p < .001$), which indicates that the variables play a significant role. Goodness-of-fit tests (Pearson $\chi^2 = 216.883$, p = .489; Deviance $\chi^2 = 141.423$, p = 1.000) suggest the model fits the data well. Cox & Snell = .263, Nagelkerke = .299, and McFadden = .144) suggest a moderate to strong explanatory power of the model. In general, the results confirm the hypotheses, showing that the three types of factors (organisational, environmental, and security) play a crucial role in adoption decisions.

Table 4.12

Parameter Estimates for Logistic Regression Predicting Cloud Computing Adoption

		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval Lower Bound	Upper Bound
Threshold	[ACC = 2.00]	1.214	1.713	.503	1	.478	-2.142	4.571
	[ACC = 3.00]	4.770	1.488	10.273	1	.001	1.853	7.687
	[ACC = 4.00]	7.732	1.642	22.167	1	.000	4.513	10.951
Location	DP	-.056	.229	.061	1	.805	-.505	.392
	C	-.030	.292	.011	1	.918	-.603	.542
	I	.361	.221	2.676	1	.102	-.072	.795
	AD	1.197	.304	15.509	1	.000	.601	1.792
	PRDB	.190	.245	.600	1	.439	-.290	.669

Link function: Logit.

Interpretation

The results of the parameter estimates show that adoption decisions (AD) ranked among the predictors have a very strong positive impact on the adoption of cloud computing (Estimate = 1.197, Wald = 15.509, $p < .001$), this means that it is the case that the stronger the forces for adoption, the greater the chances of the highest levels of adoption being reached. The other variables like data privacy (DP), cost (C), infrastructure (I), and perceived risks and barriers (PRDB) weren't able to show any statistically significant effects ($p > .05$), yet infrastructure (I) was able to exhibit a marginal trend ($p = .102$). The significant threshold values give a strong indication of the model's predictive ability and also help to affirm the meaningful distinctions made between the different adoption levels.

H2: There is a significant effect of organisational factors (technological readiness, financial resources, top management support, awareness of cloud computing benefits) on the adoption of cloud computing.

Table 4.13

Logistic Regression Model Fit and Goodness-of-Fit Statistics for Organisational Factors Affecting Cloud Computing Adoption

Category	Statistic	Value	df	Sig.
Model Fitting Information	-2 Log Likelihood (Intercept Only)	169.112	–	–

	-2 Log Likelihood (Final)	116.859	–	–	
	Chi-Square	52.253	4	0	
Goodness-of-Fit	Pearson	105.937	149	0.997	
	Deviance	90.79	149	1	
Pseudo R-Square	Cox and Snell	0.407	–	–	
	Nagelkerke	0.462	–	–	
	McFadden	0.246	–	–	

Interpretation

The logistic regression model is a great predictor of cloud computing adoption in terms of explanation and quality of fit. The fitting of the model points out a significant enhancement over the intercept-only model ($\chi^2 = 52.253$, df = 4, $p < .001$), thereby verifying the inclusion of the predictors as significant. Goodness-of-fit measures (Pearson $\chi^2 = 105.937$, p = .997; Deviance $\chi^2 = 90.790$, p = 1.000) reveal that the model is in a perfect position to yield the same results as the observed data. Pseudo R-square values (Cox & Snell = .407, Nagelkerke = .462, McFadden = .246) give a hint of the model's strong or moderate explanatory power. At the end of the day, this model delivers convincing proof of the impact of key factors on adoption choices.

Table 4.14

Parameter Estimates for Logistic Regression of Organisational Factors on Cloud Computing Adoption

Parameter Estimates									
			Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
								Lower Bound	Upper Bound
Threshold	[ACC 2.00]	=	5.296	1.858	8.128	1	.004	1.655	8.937
	[ACC 3.00]	=	9.182	1.725	28.321	1	.000	5.800	12.564
	[ACC 4.00]	=	12.695	2.019	39.543	1	.000	8.739	16.652
Location	TR		.997	.310	10.386	1	.001	.391	1.604
	FR		.623	.253	6.082	1	.014	.128	1.118
	TMS		.525	.287	3.343	1	.067	-.038	1.087
	ACCB		.680	.286	5.659	1	.017	.120	1.239

Link function: Logit.

Interpretation

The parameter estimates present that a number of predictors have a significant effect on the adoption of cloud computing. Trust (TR) has a very strong positive impact (Estimate = 0.997, Wald = 10.386, p = .001), which means that if the trust in providers is higher, the adoption will be more likely. In the same way, financial resources (FR) (Estimate = 0.623, p = .014) and adoption cost–benefit perception (ACCB) (Estimate = 0.680, p = .017) are, in fact, positive and significantly predicting the adoption as well. Top management support (TMS) was positive but only marginally significant (p = .067). The threshold values that were deemed significant happen to be additionally confirming the clear-cut and thus meaningful distinctions between the levels of adoption. Alongside the trust built, the main reason for cloud computing to become more widespread is financial readiness and cost–benefit considerations, overall.

H3: There is a significant influence of environmental factors (competitive pressure, internet reliability and speed, geographical location) on the adoption of cloud computing.

Table 4.15

Logistic Regression Model Fit and Goodness-of-Fit Statistics for Environmental Factors Affecting Cloud Computing Adoption

Category	Statistic	Value	df	Sig.
Model Fitting Information	-2 Log Likelihood (Intercept Only)	139.723	–	–
	-2 Log Likelihood (Final)	106.524	–	–
	Chi-Square	33.199	3	0
Goodness-of-Fit	Pearson	89.409	96	0.67
	Deviance	74.336	96	0.951
Pseudo R-Square	Cox and Snell	0.283	–	–
	Nagelkerke	0.321	–	–
	McFadden	0.156	–	–

Interpretation

The logistic regression model significantly improves over the intercept-only model ($\chi^2 = 33.199$, df = 3, $p < .001$), confirming the relevance of the predictors. Goodness-of-fit results (Pearson $\chi^2 = 89.409$, p = .670; Deviance $\chi^2 = 74.336$, p = .951)

indicate that the model fits the data well, with no evidence of lack of fit. The pseudo-R-square values (Cox & Snell = .283, Nagelkerke = .321, McFadden = .156) suggest moderate explanatory power. Overall, the model demonstrates a reliable ability to explain variation in cloud adoption decisions.

Table 4.16

Parameter Estimates for Logistic Regression of Environmental Factors on Cloud Computing Adoption

		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Threshold	[ACC = 2.00]	2.553	1.666	2.348	1	.125	-.712	5.818
	[ACC = 3.00]	6.245	1.483	17.726	1	.000	3.338	9.152
	[ACC = 4.00]	9.245	1.668	30.732	1	.000	5.976	12.513
Location	CP	.869	.272	10.211	1	.001	.336	1.402
	IRS	.857	.278	9.534	1	.002	.313	1.401
	GL	.246	.256	.922	1	.337	-.256	.747

Link function: Logit.

The results show that thresholds for ACC = 3 and ACC = 4 are highly significant, indicating strong separation between higher ACC categories, while ACC = 2 is not significant. Among predictors, CP and IRS have significant positive effects, increasing the likelihood of higher ACC levels, whereas GL shows no significant influence on ACC.

H4: There is a significant impact of perceived risks and barriers (vendor lock-in, service reliability, lack of control over data) on the adoption of cloud computing.

Table 4.17

Logistic Regression Model Fit and Goodness-of-Fit Statistics for Perceived Risks and Barriers Affecting Cloud Computing Adoption

Section	Statistic / Measure	Value	df	Sig.
Model Fitting	Intercept Only (-2LL)	144.057		
	Final (-2LL)	112.499	3	0
	Chi-Square	31.557	3	0
Goodness-of-Fit	Pearson Chi-Square	194.614	102	0
	Deviance Chi-Square	79.312	102	0.953
Pseudo R-Square	Cox & Snell	0.271		
	Nagelkerke	0.307		

	McFadden	0.149

The model fitting results indicate a significant improvement from the intercept-only model ($\chi^2 = 31.557$, $p < .001$), confirming good explanatory power. Goodness-of-fit tests show a non-significant deviance statistic ($p = .953$), suggesting the model fits well, though Pearson's χ^2 is significant. Pseudo R^2 values (Nagelkerke = .307) indicate a moderate level of explained variance.

Table 4.18

Parameter Estimates for Logistic Regression of Perceived Risks and Barriers on Cloud Computing Adoption

		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Threshold	[ACC = 2.00]	.957	1.456	.432	1	.511	-1.896	3.810
	[ACC = 3.00]	4.477	1.168	14.696	1	.000	2.188	6.767
	[ACC = 4.00]	7.521	1.368	30.213	1	.000	4.839	10.203
Location	VL	1.070	.305	12.324	1	.000	.472	1.667
	SR	.192	.251	.584	1	.445	-.300	.683
	LCOD	.329	.239	1.890	1	.169	-.140	.797

Link function: Logit.

The results show that thresholds for ACC = 3 and ACC = 4 are highly significant, confirming clear separation between higher categories, while ACC = 2 is not significant. Among predictors, VL has a strong and significant positive effect, increasing the odds of higher ACC levels, whereas SR and LCOD show no statistically significant influence.

H5: There is a significant influence of perceived usefulness and benefits (cost reduction, flexibility and scalability, ease of use) and the adoption of cloud computing.

Table 4.19

Logistic Regression Model Fit and Goodness-of-Fit Statistics for Perceived Usefulness and Benefits Affecting Cloud Computing Adoption

Section	Statistic / Measure	Value	df	Sig.
Model Fitting	Intercept Only (-2LL)	156.479		
	Final (-2LL)	94.735	3	0
	Chi-Square	61.744	3	0
Goodness-of-Fit	Pearson Chi-Square	59.692	114	1

	Deviance Chi-Square	64.034	114	1
Pseudo R-Square	Cox & Snell	0.461		
	Nagelkerke	0.523		
	McFadden	0.291		

The model shows a significant improvement over the intercept-only model (χ^2 = 61.744, $p < .001$), indicating strong explanatory power. Goodness-of-fit statistics (Pearson and Deviance, $p = 1.000$) confirm excellent model fit. Pseudo R^2 values, particularly Nagelkerke (.523), suggest that the model explains a substantial proportion of the variance, reflecting strong predictive capability.

Table 4.20

Parameter Estimates for Logistic Regression of Perceived Usefulness and Benefits on Cloud Computing Adoption

			Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
								Lower Bound	Upper Bound
Threshold	[ACC 2.00]	=	4.399	1.578	7.771	1	.005	1.306	7.493
	[ACC 3.00]	=	8.581	1.524	31.699	1	.000	5.594	11.568
	[ACC 4.00]	=	12.350	1.828	45.621	1	.000	8.766	15.934
Location	CR		.658	.269	5.969	1	.015	.130	1.185
	FS		1.425	.302	22.228	1	.000	.833	2.018
	EU		.698	.253	7.604	1	.006	.202	1.194

Link function: Logit.

The results indicate that all thresholds (ACC = 2, 3, 4) are significant, showing clear separation between categories. Among predictors, FS has the strongest positive effect on higher ACC levels, followed by EU and CR, which are also significant. This suggests that increases in FS, EU, and CR substantially raise the likelihood of being in higher ACC categories.

H6: There is a significant effect of trust in cloud service providers (reputation, compliance with security standards, transparency in data handling) on the adoption of cloud computing.

Table 4.21

Logistic Regression Model Fit and Goodness-of-Fit Statistics for Trust in Cloud Service Providers Affecting Cloud Computing Adoption

Section	Statistic / Measure	Value	df	Sig.
Model Fitting	Intercept Only (-2LL)	117.318		
	Final (-2LL)	74.245	2	0
	Chi-Square	43.073	2	0
Goodness-of-Fit	Pearson Chi-Square	117.151	43	0
	Deviance Chi-Square	42.668	43	0.486
Pseudo R-Square	Cox & Snell	0.35		
	Nagelkerke	0.398		
	McFadden	0.203		

The model significantly improves over the intercept-only model ($\chi^2 = 43.073$, $p < .001$), demonstrating strong explanatory power. Goodness-of-fit tests indicate adequate fit (Deviance $p = .486$), though Pearson's test is significant. Pseudo R^2 values, particularly Nagelkerke (.398), suggest the model explains a moderate proportion of variance, reflecting reasonable predictive capability.

Table 4.22

Parameter Estimates for Logistic Regression of Trust in Cloud Service Providers on Cloud Computing Adoption

			Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
								Lower Bound	Upper Bound
Threshold	[ACC 2.00]	=	1.550	1.381	1.259	1	.262	-1.158	4.258
	[ACC 3.00]	=	5.334	1.172	20.712	1	.000	3.037	7.631
	[ACC 4.00]	=	8.679	1.423	37.177	1	.000	5.889	11.469
Location	RCSS		.932	.251	13.791	1	.000	.440	1.424
	TDH		.956	.259	13.574	1	.000	.447	1.464

Link function: Logit.

The results show that thresholds for ACC = 3 and ACC = 4 are highly significant, indicating clear separation between higher ACC categories, while ACC = 2 is not significant. Both predictors, RCSS and TDH, have significant positive effects, meaning higher values in these variables substantially increase the likelihood of being in higher ACC categories.

4.12 Summary of Findings

Evaluating six hypotheses, it is possible to state that various elements play a significant role in determining whether medium-sized enterprises (MSEs) in India accept cloud computing. In the case of H1, the results of cybersecurity issues were ambivalent: although adoption decisions (AD) were a significant predictor of adoption, other factors such as data privacy and perceived risks were not, but the infrastructure had a marginal impact. H2 showed that organizational variables, especially, technological readiness (TR), financial resources (FR), and cost-benefit awareness (ACCB), exerted a positive influence that was strong but the top management support (TMS) had a minor positive influence. H3 identified environmental variables with competitive pressure (CP) and internet reliability and speed (IRS) playing a major role in enhancing the likelihood of adoption whereas geographical location (GL) had no effect.

In the case of H4, the perceived risks and perceived barriers indicated that the vendor lock-in (VL) was a significant factor in adoption but service reliability (SR) and the inability to control data (LCOD) were not. H5 reported that the perceived usefulness factors such as the flexibility and scalability (FS), ease of use (EU) and reduction in cost (CR) were all significant and FS factors had the most significant positive impact on adoption. Lastly, H6 demonstrated that confidence in cloud service vendors based on reputation and compliance with security standards (RCSS) and transparency in data processing (TDH) have a potential effect on cloud adoption. All in all, the adoption of technology readiness, monetary assistance, perceived advantage, trust in the vendor, and rivalry pressure became the most imperative factors that defined the cloud adoption behaviour of Indian MSEs.

4.13 Conclusion

The research finds that the organisational, environmental, technological, and perceptual factors together determine the adoption of cloud computing by Indian medium-sized enterprises. The results indicate that although cybersecurity issues are apparent, organisational preparedness, particularly technological and financial resources, is more determinant in the adoption decisions. The competitor pressure and the availability of the internet are other environmental factors that encourage adoption even faster and it is important to note that the external market factors are crucial. In the same way, the perceived usefulness, cost efficiency, scalability, and ease of use are strongly predicted to be adopted, representing the practical advantages of cloud computing.

In addition, confidence in the cloud service providers, particularly reputation, adherence to the security limits, and transparent data management, are also the key success factors boosting adoption, which is one of the most significant obstacles to MSEs. Conversely, other risks such as service reliability and lack of control of data did not significantly affect the outcome, indicating that the enterprises could focus on the benefits of operations they get rather than the risks associated with the adoption of the cloud. Comprehensively, the paper highlights that MSEs need to work on the enhancement of technology preparedness, financial resources, and cooperation with reliable service providers in the context of which policymakers and vendors strive to enhance internet infrastructure, security provisions, and awareness efforts to promote the uptake of clouds.

CHAPTER V:
DISCUSSION

5.1 Discussion of Results

According to the results of the proposed study, the problem of cybersecurity can be seen as one of the areas of concern that condition the adoption of cloud computing among medium-sized enterprises (MSEs) in India. Even though such aspects as confidentiality, privacy, and integrity were investigated, availability and continuity of services proved to be the most critical ones. It means that MSEs attach greater importance to the reliability of operations and business continuity than to abstract risks such as privacy breaches because they rely on continuous digital services in their daily operations. Interestingly, data privacy and confidentiality did not have any significant predictive value, which implies that the current provider-provided defences might be sufficient to be considered adequate by many MSEs. This finding demonstrates a practical, conditional method because companies take the dangers of cybersecurity in a rational perspective with regard to the facts of their business. It also has a positive association with the literature that suggests organisations in emerging markets are more likely to think about cloud adoption, depending on the level of risk taken, and resources available, rather than technical issues alone.

In addition to the security-related factors, organisational ones and environmental ones were also determined to have a large impact on the outcome of the adoption. The

capability of an enterprise to handle its perceived cybersecurity threats was enhanced by the technological preparedness, finances, and awareness of the benefits of the cloud. Individuals who had robust IT systems and funding were better assured of their capacity to breach barriers to entry and competition. The reliability of the internet was another factor that affected adoption. Geographical location, however, did not play a major role in adoption; this would imply that cloud services in India are becoming increasingly available. These results indicate that the process of adoption does not rely on the issues of cybersecurity, but on the model of organisational preparedness, external market, and infrastructure. Perceived threat diminishes with the internal preparedness and external pressures in the scenario of Indian MSEs, and better-informed and confident decisions could be made on behalf of cloud technologies.

It is also revealed that strategic issues, benefits, issues of trust and security play very high roles in the adoption decision. Vendor lock-in was the most pressing barrier, and it implied that the MSEs wanted to be flexible and autonomous in relating to its providers. Nevertheless, the benefits of scalability, cost-effectiveness and user-friendliness were powerful, and potential threats were often overshadowed. Trust in the cloud service providers, based on reputation, transparency, and security standards, further lowered the concerns and enabled the enterprises to be more assured and embrace it. This risk-benefit-trust equilibrium means that MSEs will be unwilling to implement cloud technologies with the single objective of solving any technical problem, but instead improve the overall business performance and competitiveness. Lastly, the paper also sheds light on the perception of risks, organisational preparedness, and provider trust as the dynamic aspects that influence the adoption of secure clouds by the Indian MSEs. The information presented by the research is beneficial to both policymakers and providers of the services.

5.2 Discussion of Research Question One

These outcomes validate the fact that secured networks and data protection in general are the main obstacles in the Indian cloud computing adoption process for medium-sized enterprises (MSEs). There was a hypothesis that the dimensions of data

privacy, confidentiality, integrity, availability, and the perceived risk of data breach are interdependent with the adoption decision (Mishra *et al.*, 2018). The current evidence bears out the hypothesis as it shows that the implementation of clouds by MSEs is not dependent on all the factors equally, but rather on all. This is in line with the literature that it takes a security preparedness and risk/taking capacity of the organization factor for a business in developing economies to be more likely to consider the cloud as an option (Golightly *et al.*, 2022).

Among the listed issues, one of the most visible ones, which the research reveals, is the issue of data availability that can shape the adoption decision. The risk of service failure or disruptions appears to be more a problem to Indian MSEs than the risks such as confidentiality or privacy (Singh, Yadav and Dang, 2017). This implies a pragmatic attitude, i.e., business issues are addressed with the reality of operational survival, rather than with more abstract security considerations. This priority can be expressed as discontinuity in these organisations, particularly in customer relationship, financial transactions, and the supply chain processes (C V and Agrawal, 2024). Going to the matter of availability, MSEs demonstrate that they are likely to consider cloud computing as not a completely technical solution but as a business enabler (Nagahawatta *et al.*, 2021).

Interestingly, the outcomes show that it is the matter of data integrity that was moderately affected. However, no statistically significant predictors of adoption have been identified with the concerns of privacy and confidentiality issues. This result contradicts the widespread story of much of the literature on cloud security, in which data privacy and confidentiality are assumed to be universal security obstacles (Abdulsalam and Hedabou, 2021). In the case of Indian MSEs, this can be attributed to the fact that there are fewer regulatory pressures compared to larger companies, or the perception that simpler data protection measures provided by cloud service providers can be relied upon (Alugoju, 2024). It also implies that these businesses might not be equipped with sophisticated technical expertise to understand the consequences of data breaches to the extent that they overestimate risks regarding privacy.

The results are a valuable addition to the subtle perception of cybersecurity in the adoption of cloud services by Indian MSEs. They demonstrate how concerns are not prioritised equally, but rather prioritised based on organisational realities, the availability of resources, and perceived business risks (Priyadarshinee, Raut, Jha and Kamble, 2017). As much as availability and integrity influence decision-making, other matters such as privacy and confidentiality are not overlooked but considered to be of secondary nature. This means that to have an effective cloud adoption strategy, both the policymakers and the service providers must customise security assurances to suit MSEs. The idea of reliability, continuity in services, and clear incident response procedures might be more convincing than the emphasis on privacy, as it is guaranteed, which will eventually cause more people to use secure cloud technologies (Rawindaran *et al.*, 2023).

The preceding result indicated that adoption decisions (AD) played a significant role in cloud adoption compared to data privacy (DP), cost (C), infrastructure (I) and perceived risks and barriers (PRDB). This implies that although issues of cybersecurity are important, aspects of adoption decision have strong influence on cloud adoption among MSEs in India.

These results **partially support H1**, as only AD was significant, while the others were not.

5.3 Discussion of Research Question Two

The results indicate that the organisational factors have a significant role to play in dealing with cybersecurity concerns when adopting the cloud between the Indian medium-sized enterprises (Poehlmann *et al.*, 2021). This was the hypothesis; other criteria, such as technology preparedness, financial opportunities, top management support, and awareness of the benefits of cloud computing, would be significant in adoption (Zaman, 2024). These assumptions are based on the fact that the outcome has indicated that most of these factors are strong predictors (Aiyebelehin *et al.*, 2020). It implies that those companies possessing the appropriate infrastructure, funds and understanding of the advantages of the cloud will be better placed to resolve cybersecurity problems (Sarkar *et al.*, 2022). The findings support the past studies that

indicated that the threats related to technology adoption in the business do not hinder successful adoption, but rather internal readiness and the dedication of the leadership.

The technological readiness and financial resources were identified two organisational dimensions that had the strongest influence in adoption. Companies with a robust IT and reliable infrastructure appear to be more confident about the cloud security concerns (Godoe and Johansen, 2012). In the same vein, adequate financial resources would prepare organisations to invest further in protective measures, cybersecurity tools, or specialised training, which would lower the perceived risks. Cloud computing awareness was also relevant and indicated that a company, which is conscious of the potential value of cloud services, may be more inclined to accept inherent risks (Dutta and McCrohan, 2002). Interestingly, the support of top management, although positively related, was not as salient, indicating that the readiness of the leadership alone could not be effective without viable preparation and financial capability.

The research also discussed environmental influences, which include competitive forces, internet reliability, and geographical location. The results indicate that competitive pressure and good internet connectivity are strong factors that result in cloud adoption, as compared to geographical location, which did not portray any significant influence (Ibrahim, Ahmad and Sallehudin, 2025). This means that organisations and their perception of cybersecurity issues are directly influenced by the external market forces and availability of stable connections. Competitive conditions appear to create a sense of urgency in the implementation of innovative solutions, and it makes Indian MSEs better equipped to deal with the risks of such solutions (Singh, 2019). Similarly, the question of internet reliability is a pillar since in the absence of consistent access to services, organizations would not invest in the cloud platforms. These results underscore the fact that the environment must be prepared to supplement organisational aspects of overcoming security-related problems.

The overall conclusions point out that the organizational and environmental aspects jointly influence the cloud adoption, and not just the concern about security (Durst, Hinteregger and Zieba, 2024). Market presence and competition along with

reliable internet access put the industries that are well equipped with the technology and financial resources in a better place to manage the security risks related to clouds. This can be justified by the fact that the geographical location factor could have lesser impact due to the rising accessibility of cloud services in other regions of India and would make it less impactful as a factor (Al-Sharafi *et al.*, 2023). Competition and a good internet connection position industries that can easily access technological and financial resources at a vantage position when dealing with security threats to clouds. This could be due to the fact that the geographical location factor can bring about a small effect seeing the growing availability of cloud services in the various sections of India would make it a minor factor (Younus *et al.*, 2025).

Cloud adoption was not dependent on the organizational conditions such as technological preparedness (TR), financial preparedness (FR) or the perception of cost-benefit of adoption (ACCB) and the support of the top management (TMS). That means that the decisions to adopt are triggered by technological and financial preparedness and clear understanding of costs and advantages.

These findings support H2.

The environment factors that have a strong impact on the decision to adopt were widely used as competitive pressure (CP) and internet reliability and speed (IRS) rather than the geographical location (GL). This highlights the fact that the geography is not a decisive transporting force in comparison to infrastructural dependability and competition.

Hypothesis Link: These findings support H3.

5.4 Discussion of Research Question Three

The reading shows that the adoption of cloud computing in Indian medium-scale enterprises (MSEs) is largely affected by the perceived risks and barriers. The hypothesis was that the effects of vendor lock-in, service reliability and lack of the ability to control data would all impact the adoption decision (Joshi and Matai, 2023). The findings confirm this assumption, but there is a significant nuance; not all factors affect the same extent. The most prominent concern of vendors' lock-in was pointed out by the group

which means the companies are worried about (Opara-Martins, Sahandi and Tian, 2016b). This is representative of a more significant concern which is less flexibility, higher costs, and problems with data or service migration to other platforms, which is very much relatable to the Indian MSE scenario.

The dominance of vendor lock-in as a barrier indicates that companies regard independence and adaptability in their IT strategies as key features. Not being able to switch providers easily might be a tactical weakness for micro and small enterprises (MSEs) with limited resources working under resource constraints (Kumar and Kumar, 2022). This problem is often more significant than security concerns traditional businesses feel that if they get locked with one vendor they would lose bargaining power, control over prices and the ability to roll-out innovations in the future (Kelly and Chicksand, 2024). This is what the literature tells us as well, since lock-in risks have been pointed out as the biggest reason for cloud refusal in the first place, especially in new markets where vendor ecosystems are still unformed, competition may be not accessible and the risks of being stuck with a vendor are very high.

Interestingly, lack of control over data and reliability of the service did not turn out to be statistically significant obstacles in the current research. This discovery deviates somewhat from the traditional literature, where these dimensions are usually highlighted as the fundamental risks of cloud services (Abdulsalam and Hedabou, 2021). The most likely reason is that Indian MSEs are becoming more confident about the baseline reliability guarantees offered by the large cloud providers, particularly when these are more established. Similarly, although loss of control over data is an abstract danger, it might not be seen as an imminent danger as much as the concrete danger of dependency on a vendor through a contract (Apaloo and Bright, 2022). This means the MSEs practically assess risks whose focal point is direct effects on operational and financial independence.

Based on the research, it must be emphasized that the factors perceived as barriers are very much dependent on the specific situation and at the same time are shaped by the priorities and realities of the market of the organization. One big reason for the resistance

of Indian MSEs to the cloud adoption is the lock-in with the vendor which they consider a strategic risk and it is more pronounced than, for example, issues like reliability or data control which are more widely mentioned (Ayepola and Abos, 2024). This situation calls for the cloud service providers to come up with flexible contract support, interoperability, and clear exit plans as a way to reduce client concerns. To the regulators, it suggests setting up legal frameworks to guard businesses against locking-in practices that may turn out to be exploitative and thus slow down the adoption process (Brender and Markov, 2013b). The whole picture, the findings grant the researchers a deeper comprehension of risk perception in relation to cloud computing, and they imply that the adoption decisions are influenced not only by security but also by overall strategy and structure of the organization.

The perceived risks and barriers with significant effects on adoption included only vendor lock-in (VL) and the insignificance of service reliability (SR) and lack of control over data (LCOD). It means that the biggest risk factor experienced by MSEs is the affiliation to a single provider.

Hypothesis Link: These findings **partially support H4**, as only VL was significant.

5.5 Discussion of Research Question Four

The study has pointed out that perceived usefulness and benefits are critical in adoption of cloud technologies in Indian medium-sized enterprises (MSEs), despite cybersecurity concerns. The hypothesis further presupposed that cost-cutting, flexibility, scalability and ease of use would be great incentives to adoption. The findings have confirmed this fact since the results indicate that these benefits are very strong motivation factors that outshine the perceived dangers (Kumar, Samalia and Verma, 2017). This finding is not isolated to the existing technology acceptance models, where perceived usefulness is likely to be the strongest element in the adoption behaviour. When it comes to MSEs in India, which typically do not necessarily have large financial means to fall back on and might be interested in the utility of the competitive effectiveness of the cloud solutions, the potential of the latter to provide tangible cost savings and operational

advantages makes the adoption of cloud solutions an attractive option, even at that time, back when the lack of privacy, data breach, and dependency-on-vendors issues were not of particular concern (Choudhury, Shetty and Panda, 2020).

Among the mentioned pros, flexibility and scalability were the most important benefits of using the cloud. Enterprises love the ability to expand IT resources rapidly in line with the requirements of the business without the need to incur massive capital investments. The scalability will be strategic to the MSEs as it will also allow them to respond to market and demand variations promptly (Johnson *et al.*, 2024). It is also worth noting that flexibility has been identified as a key factor that highlights the weaknesses of traditional in-house IT infrastructure, which could be quite expensive to invest in and maintain in the long run. Cloud-based solutions offer flexibility by comparison, and MSEs can now compete with larger organisations (Banger, K and Shetty, 2022). This observation indicates that convergence of cloud systems is reactive to the dynamism of the operating environment of Indian firms in a fast-changing digital economy.

The cost-reduction element also plays a very important role in determining the adoption decisions. MSEs tend to have a limited budget and are highly sensitive in the cost of IT infrastructure opportunities. Cloud computing prevents the need to invest enormous sums of money in initial investments in hardware and reduces on the continued costs of system advancement and upkeep and the costs of IT staff (Alghofaili *et al.*, 2021). Such financial efficiency enables the organisation to invest in other strategic areas, such as marketing or innovation, thus increasing the overall competitiveness of the organisation. The importance of cost reduction as a motivation justifies the point that in resource-starving businesses, the economic gains tend to overwhelm the security threats. MSEs will have greater tolerance of uncertainties in data privacy, reliability, or control by viewing cloud computing as a relatively inexpensive transaction (Iftikhar *et al.*, 2023).

It was also discovered that ease of use plays an important role in adoption, and therefore, user-friendly interfaces and straightforward deployment procedures can motivate organisations to adopt cloud technologies. Most MSEs do not have specialised IT teams, and usability is therefore a decisive step towards limiting entry barriers

(Omowole *et al.*, 2024). Cloud platforms that are user-friendly and do not require a high level of technical skills enable businesses to implement the solutions without a large amount of training or the use of third-party consultants. This shows that perceived risks can be compensated by simplicity in implementation since organisations no longer worry about being able to handle cloud systems on their own (Kulshreshtha and Jain, 2015). Their combination leads to the assumption that the benefits in flexibility, cost-effectiveness, and usability offer MSEs enough incentive to adopt cloud technologies, regardless of cybersecurity, and that a benefit-based approach is the priority to deploy cloud-based technologies.

The perceived usefulness parameters which consisted of flexibility and scalability (FS), ease of use (EU) and a decline in costs (CR) played an important role in the decision to adopt the cloud. The maxim effect was the largest in FS which presupposes that MSEs value agility and cost-effectiveness in the stage of cloud adoption.

Hypothesis Link: These findings support H5.

5.6 Discussion of Research Question Five

The findings of this paper research uphold the idea that trust in the cloud service providers is an essential element that helps to reduce cybersecurity concerns and achieve the acceptance among Indian medium-sized enterprises (MSEs). It was hypothesised that the levels of trust and subsequent adoption outcomes would be a combined outcome of provider reputation, compliance with security standards, and transparency in data handling (Isabirye, 2024) Cloud Adoption and Digital Transformation Cybersecurity Considerations for SMEs. This assumption is strongly supported by the results, which reveal that the elements of trust play a significant role in reducing the perceived risk weight in the decision-making process. This supports the point that organisational trust in the provider is also as important as technical safeguards (Agburu, Anza and Iyortsuun, 2017). The responsibility of outsourcing to trusted providers in the context of MSEs, which often lack the highest levels of internal security expertise, as is common in places such as India, becomes a viable approach to overcoming the barriers posed by security issues to adoption.

Among the dimensions of trust, the reputation of the provider was among the key drivers of using a cloud. Providers who have a proven track record, international presence or familiarity with the industry have higher chances of the enterprise adopting their solutions. Reputation serves as a proxy of reliability and safety and assures MSEs that their data and operations are in sound hands (Hasani *et al.*, 2023). This is especially pertinent in contexts where smaller businesses lack the resources to implement a security audit or evaluation on their own. MSEs use reputation signals to decrease uncertainty, based on indicators like market leadership or customer testimonials, and become more comfortable with the idea of long-term cloud relationships (Perera *et al.*, 2022). This demonstrates that, at times, intangible aspects of trust become more important than technical factors when businesses assess the risks associated with adoption.

Data handling transparency was also a very important aspect in developing trust and adoption. Open communication about data storage, processing, and protection is highly appreciated by businesses, as it helps to eliminate doubts about potential misuse or unauthorised access. The cloud providers with comprehensive security policies, incident reporting, and data management guidelines appear to be more confident than the future users (Sengupta, Kaulgud and Sharma, 2011). Transparency is an advantage in the Indian MSE context where the cybersecurity literacy level may vary widely, as it allows for overcoming the knowledge difference by being put in simple and verifiable terms. This finding corresponds with the existing literature, which implies that information clarity reduces uncertainty and increases the perception of provider trustworthiness, thereby diminishing the psychological barriers to cloud adoption (Ali, Wood-Harper and Ramlogan, 2020).

The findings indicate that adherence to agreed-upon security standards enhances trust even further, thereby providing organisations with formal guarantees of reliability. The presence of certifications and compliance with global or national security frameworks serves as an assurance of best practices, and MSEs feel safer adopting the cloud. Combined, reputation, transparency, and compliance create a three-pronged component of trust-building that can effectively reduce cybersecurity issues. This

highlights to policymakers and service providers (Chauhan and Shiaeles, 2023)the need to enhance trust by regulating, certifying, and practising with transparency. Whether it is the technical risks or the business trust, with trust on the agenda, the providers are able to resolve the disjuncture between these two components, and thus, make the adoption of cloud computing a possibility among Indian MSEs (Raut *et al.*, 2017). This underlines the fact that trust is a characterising trait in the risk versus program balance and can cause the balance to swing towards the cloud in adoption decision-making.

One of the elements of trust such as reputation and complying with security standards (RCSS) and data handling transparency (TDH) that proved to be a strong predictor of adoption and which indicated that in the context of MSEs migrating to the cloud reliability and visibility of the providers were crucial.

Hypothesis Link: These findings support H6.

Table 5.1

Summary of Hypothesis

Hypothesis	Description (Simplified)	Decision
H1	Cybersecurity concerns (DP, AD, C, I, PRDB) affect cloud adoption	**Partially Accepted** (only AD significant)
H2	Organisational factors (TR, FR, ACCB, TMS) affect cloud adoption	**Accepted**
H3	Environmental factors (CP, IRS, GL) affect cloud adoption	**Accepted** (CP, IRS significant; GL not)
H4	Perceived risks & barriers (VL, SR, LCOD) affect cloud adoption	**Partially Accepted** (only VL significant)
H5	Perceived usefulness & benefits (FS, EU, CR) affect cloud adoption	**Accepted**
H6	Trust in providers (RCSS, TDH) affects cloud adoption	**Accepted**

CHAPTER VI:
SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

6.1 Summary

The study examined the uptake of secure cloud computing among the medium-sized enterprises (MSEs) in India and the role of cybersecurity issues in the uptake process. It discussed numerous issues regarding the effects of security issues, organisation preparedness, perceived risk and obstacles, perceived value and confidence in cloud providers. The results showed that the issue of cybersecurity is of high interest but fails to be a deterrent. Instead of that, businesses perceive these risks in the light of real benefits of cost-effectiveness, scalability, and flexibility. Also, the analysis established that organisational preparation, such as awareness and technical skills, is necessary in easing the burden of moving to the cloud and enabling firms to move to cloud platforms without any trouble.

Simultaneously, the research has come to the conclusion that the perceived risks including lock-in with vendors, data control restrictions and reliability of the services continue to be obstacles to adoption. Nonetheless, according to the research, another effective countering aspect is trust in the cloud service providers particularly, their reputation, adherence to security policies and transparency in their data processing. These

observations suggest that the Indian MSEs are taking a moderate approach where they are critically examining the risk and opportunities. The results, by and large, point out that the adoption of cloud computing is not merely a technological matter but a strategic one that is significantly influenced by attitudes towards risk, trust and perceived organisational value.

6.2 Implications

The findings of the study have a very significant impact on the management of the Indian MSEs. The results suggest that security problems are very much there and besides that, they can be tackled in a tactical way through the adoption of good policies and training. The cloud should not be seen by managers as a technology change but rather a business change that needs to be monitored and has risk minimisation as a requirement. Data privacy, confidentiality, and availability are the areas that companies can focus on in order to reduce the number of vulnerabilities and have a security culture. This will help MSEs to utilize the scale and elasticity of cloud solutions that do not come with the risks that hinder implementation.

From the technical aspect, the article reaches the point that cloud service providers must encompass solutions that can be rendered more objective to MSE needs. The quite important factors of adoption were reliability of the services provided, transparency of data processing and international security standards. By paying special attention to those aspects, providers can be more trusted by potential customers and, in turn, facilitate the adoption. In the case of the MSEs this entails not just the assessment of the providers as regards to the cost but also their capability to be highly secure and responsible. The establishment of these trust-based relationships will assist business in operating between risks and benefits, and in implementing cloud solutions, which facilitate long-term development and innovation.

The research has policy implications on the regulators and the government agencies. Due to the fact that cloud computing is among the key drivers of digital

transformation, there must be clear guidelines and industry-specific security models. In order to minimise the perceived risks and lock-in of vendors as an obstacle to the implementation of cloud computing, policymakers can assist MSEs by providing standard measures of compliance and fiscal incentive measures in order to implement the cloud in a safe and cost-effective way. Awareness campaigns funded by the government and subsidies on the use of secure cloud services can assist in moving more small and medium-sized enterprises to the use of digital tools without the fear of the perceived risks. Therefore, regulatory support, along with industrial cooperation, can offer a more stable ecosystem that addresses obstacles without negatively impacting the level of innovation and competitiveness of Indian MSEs.

Lastly, the study has both academic and theoretical implications, as it addresses current knowledge gaps about cloud adoption among MSEs in emerging economies. Earlier research has mostly concentrated on big businesses, which has not provided much information on the specific challenges that small businesses may encounter. The present study offers a novel view to the established paradigms by showing how the interplay of issues related to cybersecurity, the perceived benefits, and the level of trust influences the decisions made. In addition to this, it gives a richer viewpoint that the future researchers can take further with time-frame or sector differential studies. This study will contribute to the development of balanced adoption models by identifying both the barriers and enabling factors. Such insights can serve as a basis for comparative research across industries and regions, promoting discourse on cloud adoption.

6.3 Recommendations for Future Research

According to the study analysis and results, there are some recommendations on how future research should be conducted to further elaborate on the topic of cloud adoption, security issues with cybersecurity, and organisational preparedness among Indian MSEs:

- Investigate the longitudinal impact of cloud adoption to monitor the changing cybersecurity risks and organisational changes over time.

- Explore specialised patterns of adoption by industry, including healthcare, retail, and manufacturing, to gain a distinctive range of constraints and advantages.
- Examine the role of governmental policies and rules, and regulations contribute to secure cloud adoption by small businesses.
- Study the interplay between organisational culture and trust building in alleviating cybersecurity issues in cloud implementation.
- Compare across countries to determine the differences among emerging economies in the drivers of adoption and barriers.
- Evaluate the role of the latest technologies, such as AI, blockchain, and zero-trust models, in improving cloud security among MSEs.
- Explore the perceptions and behavioural determinants of employee level towards acceptance of cloud technologies in organisations.
- Develop meaningful hybrid models integrating the technological, organisational, environmental and behavioural factors to offer comprehensive models of adoption.

Future studies need to expand the case of this research by studying cloud adoption among the MSEs using longitudinal methods. Because adoption is not a time-limited event, but an ongoing process, future research may explore how cybersecurity issues change as companies develop their use of cloud services. More detailed examinations would still be based on sectors, and as a result, they would generate deeper comprehension of such industries as healthcare and retail, where the regulatory and operational environment poses quite different hurdles. Also, it could be analyzed to show how the government solutions, subsidies, and regulations affected the user decision in the adoption process. These research works would aid policymakers in coming up with more targeted tactics for assisting small business organisations. The further studies in this area would broaden our knowledge about the safe and smooth implementation of the cloud

technology across different business situations and would also touch upon both the technological and the human challenges.

A further research direction that could be pursued in the future is the aspect of trust and the cultural aspects of cloud adoption. Although this research has emphasised the significance of organisational readiness and perceived usefulness, additional research should be conducted on the effect of organisational culture, leadership styles, and employee-level perceptions on adoption outcomes. Cross-country comparative research can also illuminate the differences in how emerging economies respond to cybersecurity threats. Furthermore, it may be explored to implement advanced technologies, including blockchain, artificial intelligence, and zero-trust architectures, to recognise how these technologies perform in terms of vendor lock-in, service reliability, and data privacy concerns. The researcher also has the chance to focus on the development of more complex models that could factor technological, organisational, environmental, and behavioural variables into a single model. This kind of interdisciplinary research would not only contribute to the academic discussions but also have empirical applications and offer business practical recommendations to follow along the path of digital transformation.

6.4 Conclusion

The study concludes the research by concluding that the shift in the use of secure cloud computing by medium-sized enterprises (MSEs) in India is affected by a provisional estimation of the perceived benefits and cybersecurity issues. Although the most observable threat to adoption has been breach of data, vendor lock-in, and derailing of the services, it does not completely discourage adoption. Instead, MSEs offset these risks with the tangible advantages of cloud solutions such as cost reduction, scalable nature and operational flexibility. This indicates that the drive towards adoption is not accompanied only by the security concerns, but the strategic value of digital transformation as understood by the organisations. In identifying risk and opportunities, Indian MSEs apply realistic decision process to grow and remain competitive through a responsible way of responding to weaknesses.

Meanwhile, the results demonstrate the importance of organisational preparedness for effective adoption. The companies which invest in technological infrastructures, create qualified human resources and create awareness of the advantages of the cloud, have a higher chance of counteracting cybersecurity risks. It has been demonstrated that internal preparedness is still more likely to overwhelm external risks, as the better an organisation is compared to its resources and governance, the more confident it is about adopting the cloud solutions. This brings out the issues of leadership, training and financial planning in the provision of safe adoption. In the case of MSEs, cloud computing does not entail an upgrade, but paradigm change that involves of alignment of people, processes and policies to long-term digital strategies.

The study also indicates that the level of trust on the cloud service providers is a key determinant in overcoming the obstacle faced under the security factor. The reputation of the provider, adherence to the security standards, and transparency of information management are the aspects that decrease the perceived risk. MSEs are typically interested in these trust signals since they themselves are not able to check technical safeguards. In this dependency, the providers are required to be responsible and trustworthy in order to provide high standards. When it comes to businesses, it is good to select those providers that are transparent and compliant so that mass adoption can be achieved. The policymakers also have a role to play in creating a trust by coming up with regulatory frameworks that have the capacity to police such practices to a safer and more friendly digital environment of MSEs.

Lastly, the research also contributes to theoretical and practical knowledge as it provides a subtle perspective on the adoption of cloud within the emerging economies. It fills a research gap as it focuses on medium-sized businesses that face various challenges as opposed to large firms. The findings emphasise the importance of the role of interaction of cybersecurity issues, organisational preparedness, perceived utility and confidence in adoption decision-making. This holistic view not just adds value to theoretical models, but also provides practical knowledge to managers, service providers and policymakers. By identifying the obstacles and opportunities that the research offers,

it will provide a roadmap for encouraging the adoption of secure clouds that will enable MSEs to maximise the advantages of digital technologies and become the driver of growth and innovation.

References

Abbadi, I.M. and Martin, A. (2011) 'Trust in the Cloud', *Information Security Technical Report*, 16(3–4), pp. 108–114. Available at: https://doi.org/10.1016/j.istr.2011.08.006.

Abdulsalam, Y.S. and Hedabou, M. (2021) 'Security and Privacy in Cloud Computing: Technical Review', *Future Internet*, 14(1). Available at: https://doi.org/10.3390/fi14010011.

Adian, I. *et al.* (2020) *Small and Medium Enterprises in the Pandemic : Impact, Responses and the Role of Development Finance*, *Small and Medium Enterprises in the Pandemic : Impact, Responses and the Role of Development Finance*. Available at: https://doi.org/10.1596/1813-9450-9414.

Adjei, J.K. (2015) 'Explaining the role of trust in cloud computing services', *info*, 17(1),

pp. 54–67. Available at: https://doi.org/10.1108/info-09-2014-0042.

Agburu, J.I., Anza, N.C. and Iyortsuun, A.S. (2017) 'Effect of outsourcing strategies on the performance of small and medium scale enterprises (SMEs)', *Journal of Global Entrepreneurship Research*, 7(1), p. 26. Available at: https://doi.org/10.1186/s40497-017-0084-0.

Aggarwal, V. (2017) 'Cloud Computing to help generate 1.1 mn jobs in India by 2022: Study'.

Agrawal, S., Mustafi, A. and Sharma, V. (2016) 'Cloud based Manufacturing: A Tool for Competitive Edge for Indian SMEs', in.

Aharony, N. (2015) 'An exploratory study on factors affecting the adoption of cloud computing by information professionals', *The Electronic Library*, 33(2), pp. 308–323. Available at: https://doi.org/10.1108/EL-09-2013-0163.

Ahmad, W. *et al.* (2022) 'Cyber security in IoT-based cloud computing: A comprehensive survey', *Electronics (Switzerland)* [Preprint]. Available at: https://doi.org/10.3390/electronics11010016.

Ahmed, M. *et al.* (2018) 'A Survey on Socially Aware Device-to-Device Communications', *IEEE Communications Surveys & Tutorials*, 20(3), pp. 2169–2197. Available at: https://doi.org/10.1109/COMST.2018.2820069.

Ahmed, T. (2016) 'Cloud Computing a Solution for Globalization', *International Journal of Education and Management Engineering* [Preprint]. Available at: https://doi.org/10.5815/ijeme.2016.04.04.

Aiyebelehin, A. *et al.* (2020) 'Awareness and Use of Cloud Computing Services and Technologies by Librarians in Selected Universities in Edo State', *International Journal of Knowledge Content Development & Technology*, 10, pp. 7–20. Available at: https://doi.org/10.5865/IJKCT.2020.10.3.007.

Akpan, I.J., Udoh, E.A.P. and Adebisi, B. (2022) 'Small business awareness and adoption of state-of-the-art technologies in emerging and developing markets, and lessons from the COVID-19 pandemic', *Journal of Small Business & Entrepreneurship*,

34(2), pp. 123–140. Available at: https://doi.org/10.1080/08276331.2020.1820185.

Al-rawahna, A.S.M., Hung, C.-W. and Chen, S.-C. (2018) 'Readiness of Government Organizations for Cloud-Computing Age: An Empirical Evidence from Jordan', *Journal of Business and Management Sciences*, 6(4), pp. 152–162. Available at: https://doi.org/10.12691/jbms-6-4-3.

Al-Sharafi, M.A. *et al.* (2019) 'The Effect of Sustained Use of Cloud-Based Business Services on Organizations' Performance: Evidence from SMEs in Malaysia', in *2019 5th International Conference on Information Management (ICIM)*. IEEE, pp. 285–291. Available at: https://doi.org/10.1109/INFOMAN.2019.8714699.

Al-Sharafi, M.A. *et al.* (2023) 'Determinants of cloud computing integration and its impact on sustainable performance in SMEs: An empirical investigation using the SEM-ANN approach', *Heliyon*, 9(5), p. e16299. Available at: https://doi.org/10.1016/j.heliyon.2023.e16299.

AL-Shboul, M.A. (2019) 'Towards better understanding of determinants logistical factors in SMEs for cloud ERP adoption in developing economies', *Business Process Management Journal* [Preprint]. Available at: https://doi.org/10.1108/BPMJ-01-2018-0004.

Alali, F.A. and Yeh, C.-L. (2012) 'Cloud Computing: Overview and Risk Analysis', *Journal of Information Systems*, 26(2), pp. 13–33. Available at: https://doi.org/10.2308/isys-50229.

Alawida, M. *et al.* (2022) 'A deeper look into cybersecurity issues in the wake of Covid-19: A survey', *Journal of King Saud University - Computer and Information Sciences*, 34(10), pp. 8176–8206. Available at: https://doi.org/10.1016/j.jksuci.2022.08.003.

AlBar, A.M. and Hoque, M.R. (2019) 'Factors affecting cloud ERP adoption in Saudi Arabia: An empirical study', *Information Development* [Preprint]. Available at: https://doi.org/10.1177/0266666917735677.

Alghofaili, Y. *et al.* (2021) ‘Secure Cloud Infrastructure: A Survey on Issues, Current Solutions, and Open Challenges’, *Applied Sciences*, 11(19), p. 9005. Available at: https://doi.org/10.3390/app11199005.

Alguliev, R.M. and Abdullayeva, F.C. (2013) ‘Identity management based security architecture of cloud computing on multi-agent systems’, in *Third International Conference on Innovative Computing Technology (INTECH 2013)*. IEEE, pp. 123–126. Available at: https://doi.org/10.1109/INTECH.2013.6653643.

Alharbi, F., Atkins, A. and Stanier, C. (2016) ‘Understanding the determinants of Cloud Computing adoption in Saudi healthcare organisations’, *Complex & Intelligent Systems* [Preprint]. Available at: https://doi.org/10.1007/s40747-016-0021-9.

Ali, M., Wood-Harper, T. and Ramlogan, R. (2020) ‘A Framework Strategy to Overcome Trust Issues on Cloud Computing Adoption in Higher Education’, in, pp. 162–183. Available at: https://doi.org/10.4018/978-1-7998-1082-7.ch008.

Ali, O. *et al.* (2020) ‘Cloud computing technology adoption: an evaluation of key factors in local governments’, *Information Technology & People*, 34(2), pp. 666–703. Available at: https://doi.org/10.1108/ITP-03-2019-0119.

Ali, O., Soar, J. and Yong, J. (2016) ‘An investigation of the challenges and issues influencing the adoption of cloud computing in Australian regional municipal governments’, *Journal of Information Security and Applications* [Preprint]. Available at: https://doi.org/10.1016/j.jisa.2015.11.006.

Ali, P. and Younas, A. (2021) ‘Understanding and interpreting regression analysis’, *Evidence Based Nursing*, 24(4), pp. 116–118. Available at: https://doi.org/10.1136/ebnurs-2021-103425.

Aljumah, A. and Ahanger, T.A. (2020) ‘Cyber security threats, challenges and defence mechanisms in cloud computing’, *IET Communications*, 14(7), pp. 1185–1191. Available at: https://doi.org/10.1049/iet-com.2019.0040.

Alkhater, N., Walters, R. and Wills, G. (2018) ‘An empirical study of factors influencing cloud adoption among private sector organisations’, *Telematics and Informatics*

[Preprint]. Available at: https://doi.org/10.1016/j.tele.2017.09.017.

Alouffi, B. *et al.* (2021) 'A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies', *IEEE Access*, 9, pp. 57792–57807. Available at: https://doi.org/10.1109/ACCESS.2021.3073203.

Alsmadi, D. *et al.* (2022) 'Intention, trust and risks as core determinants of cloud computing usage behavior', *Journal of Systems and Information Technology* [Preprint]. Available at: https://doi.org/10.1108/JSIT-09-2020-0180.

Alugoju, N.R. (2024) 'Data Protection in the Cloud: Ensuring Security and Compliance for Organizational Data', *International Journal for Research in Applied Science and Engineering Technology*, 12(12), pp. 1590–1596. Available at: https://doi.org/10.22214/ijraset.2024.66087.

Amankwah-Amoah, J. *et al.* (2021) 'COVID-19 and digitalization: The great acceleration', *Journal of Business Research*, 136, pp. 602–611. Available at: https://doi.org/10.1016/j.jbusres.2021.08.011.

Amoore, L. (2018) 'Cloud geographies', *Progress in Human Geography*, 42(1), pp. 4–24. Available at: https://doi.org/10.1177/0309132516662147.

Anselmi, J., Ardagna, D. and Passacantando, M. (2014) 'Generalized Nash equilibria for SaaS/PaaS Clouds', *European Journal of Operational Research*, 236(1), pp. 326–339. Available at: https://doi.org/10.1016/j.ejor.2013.12.007.

Apaloo, S. and Bright, D. (2022) 'The Effect of Risk Management Practices on Performance of Small and Medium Scale Enterprises', *Enterprise Risk Management*, 7(1), p. 1. Available at: https://doi.org/10.5296/erm.v7i1.19287.

Arpaci, I. (2016) 'Understanding and predicting students' intention to use mobile cloud storage services', *Computers in Human Behavior* [Preprint]. Available at: https://doi.org/10.1016/j.chb.2015.12.067.

Arpaci, I. (2017) 'Antecedents and consequences of cloud computing adoption in education to achieve knowledge management', *Computers in Human Behavior* [Preprint]. Available at: https://doi.org/10.1016/j.chb.2017.01.024.

Asadi, S. *et al.* (2017) ‘Customers perspectives on adoption of cloud computing in banking sector’, *Information Technology and Management* [Preprint]. Available at: https://doi.org/10.1007/s10799-016-0270-8.

Attaran, M. and Woods, J. (2019) ‘Cloud computing technology: improving small business performance using the Internet’, *Journal of Small Business and Entrepreneurship* [Preprint]. Available at: https://doi.org/10.1080/08276331.2018.1466850.

Ayepola, G. and Abos, P. (2024) ‘Vendor Lock-In and Interoperability: Importance of interoperability among cloud services’.

Banger, N., K, P. and Shetty, S.J. (2022) ‘A Review Paper on Cloud Computing Architecture, Types, Advantages and Disadvantages’, *International Journal of Advanced Research in Science, Communication and Technology*, pp. 14–22. Available at: https://doi.org/10.48175/IJARSCT-3144.

Battisti, E., Alfiero, S. and Leonidou, E. (2022) ‘Remote working and digital transformation during the COVID-19 pandemic: Economic–financial impacts and psychological drivers for employees’, *Journal of Business Research*, 150, pp. 38–50. Available at: https://doi.org/10.1016/j.jbusres.2022.06.010.

Bayramusta, M. and Nasir, V.A. (2016) ‘A fad or future of IT?: A comprehensive literature review on the cloud computing research’, *International Journal of Information Management* [Preprint]. Available at: https://doi.org/10.1016/j.ijinfomgt.2016.04.006.

Behl, A. (2011) ‘Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation’, in *2011 World Congress on Information and Communication Technologies*. IEEE, pp. 217–222. Available at: https://doi.org/10.1109/WICT.2011.6141247.

Behrend, T.S. *et al.* (2011) ‘Cloud computing adoption and usage in community colleges’, *Behaviour & Information Technology*, 30(2), pp. 231–240. Available at: https://doi.org/10.1080/0144929X.2010.489118.

Bello, S.A. *et al.* (2021) 'Cloud computing in construction industry: Use cases, benefits and challenges', *Automation in Construction*, 122, p. 103441. Available at: https://doi.org/10.1016/j.autcon.2020.103441.

Bookstaver, M. (2021) 'Secondary Data Analysis', in *The Encyclopedia of Research Methods in Criminology and Criminal Justice: Volume II: Parts 5-8*. Available at: https://doi.org/10.1002/9781119111931.ch107.

Botta, A. *et al.* (2016) 'Integration of Cloud computing and Internet of Things: A survey', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/10.1016/j.future.2015.09.021.

Bowen, P.L., Cheung, M.-Y.D. and Rohde, F.H. (2007) 'Enhancing IT governance practices: A model and case study of an organization's efforts', *International Journal of Accounting Information Systems*, 8(3), pp. 191–221. Available at: https://doi.org/10.1016/j.accinf.2007.07.002.

Brender, N. and Markov, I. (2013a) 'Risk perception and risk management in cloud computing: Results from a case study of Swiss companies', *International Journal of Information Management* [Preprint]. Available at: https://doi.org/10.1016/j.ijinfomgt.2013.05.004.

Brender, N. and Markov, I. (2013b) 'Risk perception and risk management in cloud computing: Results from a case study of Swiss companies', *International Journal of Information Management*, 33(5), pp. 726–733. Available at: https://doi.org/10.1016/j.ijinfomgt.2013.05.004.

Buyya, R. *et al.* (2009) 'Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility', *Future Generation Computer Systems*, 25(6), pp. 599–616. Available at: https://doi.org/10.1016/j.future.2008.12.001.

Buyya, R., Broberg, J. and Goscinski, A. (2011) *Cloud Computing*, *Cloud Computing: Principles and Paradigms*. Edited by R. Buyya, J. Broberg, and A. Goscinski. Wiley. Available at: https://doi.org/10.1002/9780470940105.

C V, S.K. and Agrawal, R. (2024) ‘Developing customer convenience and experience through increased competency and efficiency: A strategic approach to retail operations mastery’, *Heliyon*, 10(16), p. e36395. Available at: https://doi.org/https://doi.org/10.1016/j.heliyon.2024.e36395.

Carlos, R.C. *et al.* (2017) ‘The Role of Cloud Computing in the Development of Information Systems for SMEs’, *Journal of Cloud Computing* [Preprint]. Available at: https://doi.org/10.5171/2017.736545.

Chan, W., Leung, E. and Pili, H. (2012) ‘Enterprise Risk Management for Cloud Computing’, *The Committee of Sponsoring Organizations of the Treadway Commission (COSO)* [Preprint].

Chang, V., Walters, R.J. and Wills, G.B. (2016) ‘Organisational sustainability modelling—An emerging service and analytics model for evaluating Cloud Computing adoption with two case studies’, *International Journal of Information Management*, 36(1), pp. 167–179. Available at: https://doi.org/10.1016/j.ijinfomgt.2015.09.001.

Chauhan, M. and Shiaeles, S. (2023) ‘An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions’, *Network* [Preprint]. Available at: https://doi.org/10.3390/network3030018.

Chemjor, E., Charles, L. and Maru, L. (2017) ‘Effects of Technology Context on Cloud Computing Adoption in Small and Medium Enterprises in Nairobi County, Kenya’, *IOSR Journal of Business and Management*, 19, pp. 70–80. Available at: https://doi.org/10.9790/487X-1905057080.

Chen, L. and Kimura, F. (2020) ‘Improving Digital Connectivity for E-Commerce: A Policy Framework and Empirical Note’, *E-commerce Connectivity in ASEAN* [Preprint].

Choi, C.Y. and Lee, C.H. (2012) ‘Transposition of anterior choroidal artery and posterior communicating artery origin’, *Journal of Korean Neurosurgical Society* [Preprint]. Available at: https://doi.org/10.3340/jkns.2012.52.3.240.

Chong, S.-K. *et al.* (2014) 'Enhancing Trust Management in Cloud Environment', *Procedia - Social and Behavioral Sciences*, 129, pp. 314–321. Available at: https://doi.org/10.1016/j.sbspro.2014.03.682.

Choudhury, D., Shetty, J.P. and Panda, R. (2020) 'MSME initiatives to support Cloud adoption in India', *International Journal of Indian Culture and Business Management*, 1(1), p. 1. Available at: https://doi.org/10.1504/IJICBM.2020.10028605.

Church, K.S., Schmidt, P.J. and Ajayi, K. (2020) 'Forecast cloudy—fair or stormy weather: Cloud computing insights and issues', *Journal of Information Systems* [Preprint]. Available at: https://doi.org/10.2308/isys-18-037.

Corrales, M. (2016) '"Plan-Like Architectures" for Mutual Trust in the Cloud', in *Flexibility in Modern Business Law*. Tokyo: Springer Japan, pp. 199–225. Available at: https://doi.org/10.1007/978-4-431-55787-6_10.

Creswell, W.J. and Creswell, J.D. (2018) *Research Design: Qualitative, Quantitative adn Mixed Methods Approaches*, *Journal of Chemical Information and Modeling*.

Dawood, M. *et al.* (2023) 'Cyberattacks and Security of Cloud Computing: A Complete Guideline', *Symmetry* [Preprint]. Available at: https://doi.org/10.3390/sym15111981.

Díaz-Arancibia, J. *et al.* (2024) 'Navigating Digital Transformation and Technology Adoption: A Literature Review from Small and Medium-Sized Enterprises in Developing Countries', *Sustainability*, 16(14), p. 5946. Available at: https://doi.org/10.3390/su16145946.

Dingel, J.I. and Neiman, B. (2020) 'How many jobs can be done at home?', *Journal of Public Economics*, 189, p. 104235. Available at: https://doi.org/10.1016/j.jpubeco.2020.104235.

Dixit, A. *et al.* (2021) 'A brief review of Data Analytics approach for Small and Medium Scale Enterprises over Clouds', in *2021 International Conference on Computational Performance Evaluation (ComPE)*. IEEE, pp. 878–885. Available

at: https://doi.org/10.1109/ComPE53109.2021.9752320.

Dixit, A., Sharma, S.K. and Sharma, D.P. (2021) 'Impetus on Big Data to Boost Indian MSME Sector and Economy using Cloud Storage', *International Journal of Computer Applications* [Preprint]. Available at: https://doi.org/10.5120/ijca2021921110.

Djemame, K. *et al.* (2013) 'Legal issues in clouds: towards a risk inventory', *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 371(1983), p. 20120075. Available at: https://doi.org/10.1098/rsta.2012.0075.

Du, Z. *et al.* (2017) 'Robot Cloud: Bridging the power of robotics and cloud computing', *Future Generation Computer Systems*, 74, pp. 337–348. Available at: https://doi.org/10.1016/j.future.2016.01.002.

Duncan, A., Creese, S. and Goldsmith, M. (2015) 'An overview of insider attacks in cloud computing', *Concurrency and Computation: Practice and Experience*, 27(12), pp. 2964–2981. Available at: https://doi.org/10.1002/cpe.3243.

Durst, S., Hinteregger, C. and Zieba, M. (2024) 'The effect of environmental turbulence on cyber security risk management and organizational resilience', *Computers & Security*, 137, p. 103591. Available at: https://doi.org/10.1016/j.cose.2023.103591.

Dutta, A. and McCrohan, K. (2002) 'Management's Role in Information Security in a Cyber Economy', *California Management Review*, 45(1), pp. 67–87. Available at: https://doi.org/10.2307/41166154.

Dutta, A., Peng, G.C.A. and Choudhary, A. (2013) 'Risks in Enterprise Cloud Computing: The Perspective of it Experts', *Journal of Computer Information Systems*, 53(4), pp. 39–48. Available at: https://doi.org/10.1080/08874417.2013.11645649.

Dyubele, S., Cele, N.P. and Mbangata, L. (2020) 'Assessing the challenges that are confronted rural-based SMEs on the implementation of cloud services', in

Proceedings of the 2nd International Conference on Intelligent and Innovative Computing Applications. New York, NY, USA: ACM, pp. 1–8. Available at: https://doi.org/10.1145/3415088.3415100.

Efiong, J.E. *et al.* (2024) 'A contrived dataset of substation automation for cybersecurity research in the smart grid networks based on IEC61850', *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 22(5), p. 1320. Available at: https://doi.org/10.12928/telkomnika.v22i5.26000.

El-Gazzar, R., Hustad, E. and Olsen, D.H. (2016) 'Understanding cloud computing adoption issues: A Delphi study approach', *Journal of Systems and Software* [Preprint]. Available at: https://doi.org/10.1016/j.jss.2016.04.061.

El-Haddadeh, R. (2020) 'Digital Innovation Dynamics Influence on Organisational Adoption: The Case of Cloud Computing Services', *Information Systems Frontiers* [Preprint]. Available at: https://doi.org/10.1007/s10796-019-09912-2.

Ervural, B.C. and Ervural, B. (2018) 'Overview of Cyber Security in the Industry 4.0 Era', in *Springer Series in Advanced Manufacturing*. Available at: https://doi.org/10.1007/978-3-319-57870-5_16.

Eskrootchi, R. *et al.* (2020) 'Key factors influencing the adoption of Cloud Computing Technology in the Medical Sciences University libraries', *Library Philosophy and Practice* [Preprint].

Espadas, J. *et al.* (2013) 'A tenant-based resource allocation model for scaling Software-as-a-Service applications over cloud computing infrastructures', *Future Generation Computer Systems*, 29(1), pp. 273–286. Available at: https://doi.org/10.1016/j.future.2011.10.013.

Etikan, I. (2016) 'Comparison of Convenience Sampling and Purposive Sampling', *American Journal of Theoretical and Applied Statistics* [Preprint]. Available at: https://doi.org/10.11648/j.ajtas.20160501.11.

Fernando, N., Loke, S.W. and Rahayu, W. (2013) 'Mobile cloud computing: A survey', *Future Generation Computer Systems* [Preprint]. Available at:

https://doi.org/10.1016/j.future.2012.05.023.

Field, A. (2013) 'Discovering Statistics Using IBM SPSS Statistics: And Sex and Drugs and Rock', *4th Edition* [Preprint].

Furner, C.P. (2013) 'Getting heads into the cloud: Pre-adoption beliefs and attitudes regarding a cloud-based platform shift at a public university.', *Journal of International Technology & Information Management* [Preprint].

Ganesan, N. (2013) 'Migration of an E-Learning Model to the Cloud N. Ganesan ©', *Journal of International Technology and Information Management* [Preprint]. Available at: https://doi.org/10.58729/1941-6679.1013.

Gangwar, H., Date, H. and Ramaswamy, R. (2015) 'Understanding determinants of cloud computing adoption using an integrated TAM-TOE model', *Journal of Enterprise Information Management*, 28(1), pp. 107–130. Available at: https://doi.org/10.1108/JEIM-08-2013-0065.

Gani, A. *et al.* (2014) 'A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing', *Journal of Network and Computer Applications*, 43, pp. 84–102. Available at: https://doi.org/10.1016/j.jnca.2014.04.009.

Gao, L. and Brink, A.G. (2019) 'A Content Analysis of the Privacy Policies of Cloud Computing Services', *Journal of Information Systems*, 33(3), pp. 93–115. Available at: https://doi.org/10.2308/isys-52188.

Garg, A., Jajodia, M. and Singh, S. (2023) 'A Study of Cloud Computing in Msmes', *International Journal of Creative Research Thoughts (IJCRT)*, 11(2).

Garg, S.K., Versteeg, S. and Buyya, R. (2013) 'A framework for ranking of cloud computing services', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/10.1016/j.future.2012.06.006.

Gartner (2016) 'Gartner Says by 2020 "Cloud Shift" Will Affect More Than $1 Trillion in IT Spending'.

George, G., Lakhani, K.R. and Puranam, P. (2020) 'What has changed? The Impact of

Covid Pandemic on the Technology and Innovation Management Research Agenda', *Journal of Management Studies* [Preprint]. Available at: https://doi.org/10.1111/joms.12634.

Ghobaei-Arani, M., Jabbehdari, S. and Pourmina, M.A. (2018) 'An autonomic resource provisioning approach for service-based cloud applications: A hybrid approach', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/10.1016/j.future.2017.02.022.

Gide, E. and Sandu, R. (2015) 'A Study to Explore the Key Factors Impacting on Cloud Based Service Adoption in Indian SMEs', in *2015 IEEE 12th International Conference on e-Business Engineering*. IEEE, pp. 387–392. Available at: https://doi.org/10.1109/ICEBE.2015.72.

Godoe, P. and Johansen, T.S. (2012) 'Understanding adoption of new technologies: Technology readiness and technology acceptance as an integrated concept', *Journal of European Psychology Students*, 3, p. 38. Available at: https://doi.org/10.5334/jeps.aq.

Golightly, L. *et al.* (2022) 'Adoption of cloud computing as innovation in the organization', *International Journal of Engineering Business Management* [Preprint]. Available at: https://doi.org/10.1177/18479790221093992.

Guillén, M.Á.D. de L., Morales-Rocha, V. and Martínez, L.F.F. (2020) 'A systematic review of security threats and countermeasures in SaaS', *Journal of Computer Security*, 28(6), pp. 635–653. Available at: https://doi.org/10.3233/JCS-200002.

Gupta, A. *et al.* (2021) 'Role of cloud computing in management and education', *Materials Today ...* [Preprint].

Gupta, P., Seetharaman, A. and Raj, J.R. (2013) 'The usage and adoption of cloud computing by small and medium businesses', *International Journal of Information Management* [Preprint]. Available at: https://doi.org/10.1016/j.ijinfomgt.2013.07.001.

Gupta, R. (2023) 'The Influence of Technology on Accounting Practices in India: A

Survey of Accounting Software Utilization by Micro Enterprises in Delhi', *European Journal of Theoretical and Applied Sciences* [Preprint]. Available at: https://doi.org/10.59324/ejtas.2023.1(6).101.

Gupta, S., Saxena, K.B.C. and Saini, A.K. (2016) 'Towards risk managed cloud adoption a conceptual framework', in *Proceedings of the International Conference on Industrial Engineering and Operations Management*.

Gutierrez, A., Boukrami, E. and Lumsden, R. (2015) 'Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK', *Journal of Enterprise Information Management* [Preprint]. Available at: https://doi.org/10.1108/JEIM-01-2015-0001.

Habib, S. and Hamadneh, N.N. (2021) 'Impact of Perceived Risk on Consumers Technology Acceptance in Online Grocery Adoption amid COVID-19 Pandemic', *Sustainability*, 13(18), p. 10221. Available at: https://doi.org/10.3390/su131810221.

Hajare, R. *et al.* (2021) 'Data Security in Cloud', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 08(03).

Hanks, C. (2009) 'Technology and Values: Essential Readings'.

Hasan, M. (2023) 'The impact of cloud computing on small and medium-sized businesses'.

Hasani, T. *et al.* (2023) 'Evaluating the adoption of cybersecurity and its influence on organizational performance', *SN Business & Economics*, 3(5), p. 97. Available at: https://doi.org/10.1007/s43546-023-00477-6.

Haselmann, T. and Vossen, G. (2013) 'Hybrid Cloud Intermediaries - Facilitating Cloud Sourcing for Small and Medium-sized Enterprises', in *Proceedings of the 3rd International Conference on Cloud Computing and Services Science*. SciTePress - Science and and Technology Publications, pp. 13–25. Available at: https://doi.org/10.5220/0004354500130025.

Hashim, H.S., Hassan, Z. Bin and Hashim, A.S. (2015) 'Factors Influence the Adoption

of Cloud Computing : A Comprehensive Review', *International Journal of Education and Research* [Preprint].

Hassan, H. (2017) 'Organisational factors affecting cloud computing adoption in small and medium enterprises (SMEs) in service sector', in *Procedia Computer Science*. Available at: https://doi.org/10.1016/j.procs.2017.11.126.

Hassan, W. *et al.* (2020) 'Cloud computing survey on services, enhancements and challenges in the era of machine learning and data science', *International Journal of Informatics and Communication Technology (IJ-ICT)* [Preprint]. Available at: https://doi.org/10.11591/ijict.v9i2.pp117-139.

Heidari, A. and Jafari Navimipour, N. (2022) 'Service discovery mechanisms in cloud computing: a comprehensive and systematic literature review', *Kybernetes*, 51(3), pp. 952–981. Available at: https://doi.org/10.1108/K-12-2020-0909.

Helaimia, R. (2023) 'Cloud Computing In Higher Education Institutions: Pros and Cons', pp. 132–141.

Hentschel, R., Leyh, C. and Baumhauer, T. (2019) 'Critical success factors for the implementation and adoption of cloud services in SMEs', in *Proceedings of the Annual Hawaii International Conference on System Sciences*. Available at: https://doi.org/10.24251/hicss.2019.882.

Hossain, E. *et al.* (2019) 'Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review', *IEEE Access* [Preprint]. Available at: https://doi.org/10.1109/ACCESS.2019.2894819.

Hsu, C.-L. and Lin, J.C.-C. (2016) 'Factors affecting the adoption of cloud services in enterprises', *Information Systems and e-Business Management*, 14(4), pp. 791–822. Available at: https://doi.org/10.1007/s10257-015-0300-9.

Hsu, P.-F., Ray, S. and Li-Hsieh, Y.-Y. (2014) 'Examining cloud computing adoption intention, pricing mechanism, and deployment model', *International Journal of Information Management*, 34(4), pp. 474–488. Available at: https://doi.org/10.1016/j.ijinfomgt.2014.04.006.

Huang, J. and Nicol, D.M. (2013) 'Trust mechanisms for cloud computing', *Journal of Cloud Computing: Advances, Systems and Applications*, 2(1), p. 9. Available at: https://doi.org/10.1186/2192-113X-2-9.

Ibrahim, H.M., Ahmad, K. and Sallehudin, H. (2025) 'Impact of organisational, environmental, technological and human factors on cloud computing adoption for university libraries', *Journal of Librarianship and Information Science*, 57(2), pp. 311–330. Available at: https://doi.org/10.1177/09610006231214570.

Iftikhar, A. *et al.* (2023) 'Security, trust and privacy risks, responses, and solutions for high-speed smart cities networks: A systematic literature review', *Journal of King Saud University - Computer and Information Sciences*, 35(9), p. 101788. Available at: https://doi.org/10.1016/j.jksuci.2023.101788.

Ikuero, F.E. and Zeng, W. (2022) 'Improving cybersecurity incidents reporting in Nigeria: micro and small enterprises perspectives', *Nigerian Journal of Technology* [Preprint]. Available at: https://doi.org/10.4314/njt.v41i3.10.

Isa, W.A.R.W.M. *et al.* (2020) 'Factors influencing cloud computing adoption in higher education institution', *Indonesian Journal of Electrical Engineering and Computer Science*, 17(1), p. 412. Available at: https://doi.org/10.11591/ijeecs.v17.i1.pp412-419.

Isabirye, E. (2024) 'Cloud Adoption and Digital Transformation Cybersecurity Consideration for SMEs', *IRE Transactions on Engineering Management*, Volume 7 I.

Isma', S. Al *et al.* (2016) 'Cloud computing adoption decision modelling for SMEs: a conjoint analysis', *International Journal of Web and Grid Services*, 12(3), p. 296. Available at: https://doi.org/10.1504/IJWGS.2016.079157.

Ismail, N. (2017) 'The importance of creating a cyber security culture'.

Jäger, J. *et al.* (2016) 'Advanced Complexity Management Strategic Recommendations of Handling the "Industrie 4.0" Complexity for Small and Medium Enterprises', *Procedia CIRP*, 57, pp. 116–121. Available at:

https://doi.org/10.1016/j.procir.2016.11.021.

Jain, P. (2024) ‘Cloud Adoption Strategies for Small and Medium Enterprises (SMEs): A Comprehensive Guide to Overcoming Challenges and Maximizing Benefits’, *Scholars Journal of Engineering and Technology* [Preprint]. Available at: https://doi.org/10.36347/sjet.2024.v12i01.003.

Jianwen, C. and Wakil, K. (2019) ‘A model for evaluating the vital factors affecting cloud computing adoption’, *Kybernetes*, 49(10), pp. 2475–2492. Available at: https://doi.org/10.1108/K-06-2019-0434.

Johnson, E. *et al.* (2024) ‘Developing scalable data solutions for small and medium enterprises: Challenges and best practices’.

Johnson, J. (2022) ‘Average Organizational Cost to a Business in the United States’.

Jones, S. *et al.* (2019) ‘Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies’, *Information systems frontiers*, 21, pp. 359–382.

Jørgensen, M. and Moløkken-Østvold, K. (2006) ‘How large are software cost overruns? A review of the 1994 CHAOS report’, *Information and Software Technology* [Preprint]. Available at: https://doi.org/10.1016/j.infsof.2005.07.002.

Joshi, A. *et al.* (2015) ‘Likert Scale: Explored and Explained’, *British Journal of Applied Science & Technology* [Preprint]. Available at: https://doi.org/10.9734/bjast/2015/14975.

Joshi, A.K. and Matai, R. (2023) ‘A Literature Review on Cloud Computing Adoption in the Indian SME Manufacturing Sector and the Future Agenda’, in *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*. IEEE, pp. 1–5. Available at: https://doi.org/10.1109/SMARTGENCON60755.2023.10442048.

Kajiyama, T., Jennex, M. and Addo, T. (2017) ‘To cloud or not to cloud: how risks and threats are affecting cloud adoption decisions’, *Information & Computer Security*, 25(5), pp. 634–659. Available at: https://doi.org/10.1108/ICS-07-2016-0051.

Kamarudin, S. *et al.* (2022) 'Exploring of Potential of Cloud Computing for Small and Medium Enterprises', *Indonesian Journal of Information Systems* [Preprint]. Available at: https://doi.org/10.24002/ijis.v4i2.5487.

Katsikatsou, M. *et al.* (2012) 'Pairwise likelihood estimation for factor analysis models with ordinal data', *Computational Statistics & Data Analysis*, 56(12), pp. 4243–4258. Available at: https://doi.org/10.1016/j.csda.2012.04.010.

Kaur, S. and Sharma, T. (2017) 'A Review on Cloud Computing', *International Journal of Computer Applications*, 178(02).

Keesookpun, C. and Mitomo, H. (2014) 'Cloud computing adoption and determining factors in different industries: a case study of Thailand', *International Journal of Information Technology and Management*, 13(4), p. 243. Available at: https://doi.org/10.1504/IJITM.2014.065631.

Kelly, S. and Chicksand, D. (2024) 'A Critical Exploration of Bargaining in Purchasing and Supply Management: A Systematic Literature Review', *Group Decision and Negotiation*, 33(3), pp. 617–646. Available at: https://doi.org/10.1007/s10726-024-09879-9.

Keshanchi, B., Souri, A. and Navimipour, N.J. (2017) 'An improved genetic algorithm for task scheduling in the cloud environments using the priority queues: Formal verification, simulation, and statistical testing', *Journal of Systems and Software*, 124, pp. 1–21. Available at: https://doi.org/10.1016/j.jss.2016.07.006.

Khan, M.A. (2016) 'A survey of security issues for cloud computing', *Journal of Network and Computer Applications* [Preprint]. Available at: https://doi.org/10.1016/j.jnca.2016.05.010.

Khan, N. and Al-Yasiri, A. (2015) 'Framework for Cloud Computing Adoption: A Roadmap for Smes to Cloud Migration', *International Journal on Cloud Computing: Services and Architecture* [Preprint]. Available at: https://doi.org/10.5121/ijccsa.2015.5601.

Khayer, A. *et al.* (2020) 'Cloud computing adoption and its impact on SMEs'

performance for cloud supported operations: A dual-stage analytical approach', *Technology in Society*, 60, p. 101225.

Khoda Parast, F. *et al.* (2022) 'Cloud computing security: A survey of service-based models', *Computers & Security*, 114, p. 102580. Available at: https://doi.org/https://doi.org/10.1016/j.cose.2021.102580.

Kim, M. and Park, S.O. (2013) 'Trust management on user behavioral patterns for a mobile cloud computing', *Cluster Computing*, 16(4), pp. 725–731. Available at: https://doi.org/10.1007/s10586-013-0248-9.

Kim, S.H., Jang, S.Y. and Yang, K.H. (2017) 'Analysis of the Determinants of Software-as-a-Service Adoption in Small Businesses: Risks, Benefits, and Organizational and Environmental Factors', *Journal of Small Business Management* [Preprint]. Available at: https://doi.org/10.1111/jsbm.12304.

Krishnamurthy, S. (2020) 'The future of business education: A commentary in the shadow of the Covid-19 pandemic', *Journal of Business Research* [Preprint]. Available at: https://doi.org/10.1016/j.jbusres.2020.05.034.

Kulshreshtha, K. and Jain, U. (2015) 'Adoption of Cloud Computing By Smes – a Swot Analysis', 3(31), pp. 500–510.

Kumar, D., Samalia, H.V. and Verma, P. (2017) 'Factors Influencing Cloud Computing Adoption by Small and Medium-Sized Enterprises (SMEs) In India', *Pacific Asia Journal of the Association for Information Systems*, pp. 25–48. Available at: https://doi.org/10.17705/1pais.09302.

Kumar, D., Samalia, H.V. and Verma, P. (2018) 'Assessing the Relevance of Cloud Computing for Micro, Small and Medium Enterprises in the Northern Region of India', *Studia i Materiały Wydziału Zarządzania UW*, 1(26), pp. 127–136. Available at: https://doi.org/10.7172/1733-9758.2018.26.12.

Kumar, P.R., Raj, P.H. and Jelciana, P. (2018) 'Exploring Data Security Issues and Solutions in Cloud Computing', *Procedia Computer Science*, 125, pp. 691–697. Available at: https://doi.org/10.1016/j.procs.2017.12.089.

Kumar, Purushottam and Kumar, Prakash (2022) 'Vendor Lock-In Situation and Threats in Cloud Computing', *International Journal of Innovative Science and Research Technology*, 7(9), pp. 1437–1441.

KUMAR, R. and GOYAL, R. (2019) 'Assurance of Data Security and Privacy in the Cloud: A Three-Dimensional Perspective.', *Software Quality Professional* [Preprint].

Kumar, V. and Nanda, P. (2023) 'Determinants of the success of MSMEs in India: a policy vs. technology perspective', *International Journal of Technology, Policy and Management* [Preprint]. Available at: https://doi.org/10.1504/IJTPM.2023.129471.

Kuo, A.M.-H. (2011) 'Opportunities and Challenges of Cloud Computing to Improve Health Care Services', *Journal of Medical Internet Research*, 13(3), p. e67. Available at: https://doi.org/10.2196/jmir.1867.

L Tian, C Lin, Y.N. (2010) 'Evaluation of user behavior trust in cloud computing'.

Lacity, M.C. and Reynolds, P. (2014) 'Cloud services practices for small and medium-sized enterprises', *MIS Quarterly Executive* [Preprint].

Laurindo, F.J.B., Kissimoto, K.O. and Escorcia, J. (2022) 'Software-as-a-Service Adoption for Increasing Organizational Performance on Sme: An Approach from Knowledge Management Practices', *International Conference on Information Systems and Technology Management* [Preprint].

Lee, C.A. (2010) 'A perspective on scientific cloud computing', in *Proceedings of the 19th ACM International Symposium on High Performance Distributed Computing*. New York, NY, USA: ACM, pp. 451–459. Available at: https://doi.org/10.1145/1851476.1851542.

Lee, L.S. and Brink, W.D. (2020) 'Trust in Cloud-Based Services: A Framework for Consumer Adoption of Software as a Service', *Journal of Information Systems*, 34(2), pp. 65–85. Available at: https://doi.org/10.2308/isys-52626.

Li, L. (2017) 'Cloud Computing Strategy Analysis in Small and Medium-Sized

Enterprises', in *Proceedings of The 7th International Conference on Computer Engineering and Networks — PoS(CENet2017)*. Trieste, Italy: Sissa Medialab, p. 067. Available at: https://doi.org/10.22323/1.299.0067.

Lin, A. and Chen, N.-C. (2012) 'Cloud computing as an innovation: Percepetion, attitude, and adoption', *International Journal of Information Management*, 32(6), pp. 533–540. Available at: https://doi.org/10.1016/j.ijinfomgt.2012.04.001.

Liu, F. *et al.* (2011) 'NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and', *NIST Special Publication 500-292* [Preprint].

Liu, S. *et al.* (2018) 'Understanding the effect of cloud computing on organizational agility: An empirical examination', *International Journal of Information Management* [Preprint]. Available at: https://doi.org/10.1016/j.ijinfomgt.2018.07.010.

Liu, Y. *et al.* (2020) 'Cloud-based big data analytics for customer insight-driven design innovation in SMEs', *International Journal of Information Management*, 51, p. 102034. Available at: https://doi.org/10.1016/j.ijinfomgt.2019.11.002.

Lokuge, S. and Sedera, D. (2017) 'Turning dust to gold: How to increase inimitability of enterprise systems', in *Proceedings ot the 21st Pacific Asia Conference on Information Systems: '"Societal Transformation Through IS/IT"', PACIS 2017*.

Lokuge, S. and Sedera, D. (2018) 'The Role of Enterprise Systems in Fostering Innovation in Contemporary Firms', *Journal of Information Technology Theory and Application* [Preprint].

Lu, Y. *et al.* (2020) 'The perceived impact of the Covid-19 epidemic: evidence from a sample of 4807 SMEs in Sichuan Province, China', *Environmental Hazards* [Preprint]. Available at: https://doi.org/10.1080/17477891.2020.1763902.

Lunardi, G.L. *et al.* (2014) 'The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms', *International Journal of Accounting Information Systems* [Preprint]. Available at:

https://doi.org/10.1016/j.accinf.2013.02.001.

Lutfi, M. *et al.* (2020) 'The impact of social distancing policy on small and medium-sized enterprises (SMEs) in Indonesia', *Problems and Perspectives in Management*, 18(3), pp. 492–503. Available at: https://doi.org/10.21511/ppm.18(3).2020.40.

Lynn, T. *et al.* (2018) 'Understanding the determinants of cloud computing adoption for high performance computing', in *Proceedings of the Annual Hawaii International Conference on System Sciences*. Available at: https://doi.org/10.24251/hicss.2018.489.

Maalem Lahcen, R.A. *et al.* (2020) 'Review and insight on the behavioral aspects of cybersecurity', *Cybersecurity* [Preprint]. Available at: https://doi.org/10.1186/s42400-020-00050-w.

Mahmood, Z. (2011) 'Cloud Computing for Enterprise Architectures: Concepts, Principles and Approaches', in. Available at: https://doi.org/10.1007/978-1-4471-2236-4_1.

Malecki, E.J. (1977) 'Firms and Innovation Diffusion: Examples from Banking', *Environment and Planning A: Economy and Space* [Preprint]. Available at: https://doi.org/10.1068/a091291.

Mani, A.C. and Malviya, A.K. (2019) 'Security Challenges in Cloud Computing Networks', *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/ssrn.3350319.

Manuel, P. (2015) 'A trust model of cloud computing based on Quality of Service', *Annals of Operations Research*, 233(1), pp. 281–292. Available at: https://doi.org/10.1007/s10479-013-1380-x.

Marston, S. *et al.* (2011) 'Cloud computing — The business perspective', *Decision Support Systems*, 51(1), pp. 176–189. Available at: https://doi.org/10.1016/j.dss.2010.12.006.

Mary Matthew, K. and Quadir Md, A. (2017) 'An Effective Way of Evaluating Trust in Inter-cloud Computing', *International Journal of Computer Network and*

Information Security [Preprint]. Available at: https://doi.org/10.5815/ijcnis.2017.02.05.

McKinsey (2022) 'Projecting the global value of cloud: $3 trillion is up for grabs for companies that go beyond adoption'.

Mehmi, S., Verma, H.K. and Sangal, A.L. (2017) 'Simulation modeling of cloud computing for smart grid using CloudSim', *Journal of Electrical Systems and Information Technology*, 4(1), pp. 159–172. Available at: https://doi.org/10.1016/j.jesit.2016.10.004.

Mell, P. and Grance, T. (2011) 'The NIST definition of cloud computing', in *Cloud Computing and Government: Background, Benefits, Risks*. Available at: https://doi.org/10.1016/b978-0-12-804018-8.15003-x.

Mell, P. and Grance, T. (2012) 'The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology', in *Public Cloud Computing: Security and Privacy Guidelines*.

Meritalk (2021) 'Do You Know Who is Responsible for Disaster Recovery in the Cloud?'

Meyer, B.H., Prescott, B. and Sheng, X.S. (2022) 'The impact of the COVID-19 pandemic on business expectations', *International Journal of Forecasting* [Preprint]. Available at: https://doi.org/10.1016/j.ijforecast.2021.02.009.

Michael, K. (2008) 'Social and Organizational Aspects of Information Security Management', *Faculty of Informatics-Papers* [Preprint].

Mijnhardt, F., Baars, T. and Spruit, M. (2016) 'Organizational Characteristics Influencing SME Information Security Maturity', *Journal of Computer Information Systems*, 56(2), pp. 106–115. Available at: https://doi.org/10.1080/08874417.2016.1117369.

Ministry of Ports (2022) *Annual Report 2021-22*.

Mishra, A.A. *et al.* (2018) 'Effectiveness of Confidentiality, Integrity and Availability in the Security of Cloud Computing: A Review', in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*. IEEE, pp. 1–5. Available at: https://doi.org/10.1109/CCAA.2018.8777537.

Misra, S.C. and Mondal, A. (2011) ‘Identification of a company’s suitability for the adoption of cloud computing and modelling its corresponding Return on Investment’, *Mathematical and Computer Modelling* [Preprint]. Available at: https://doi.org/10.1016/j.mcm.2010.03.037.

Modisane, P. and Jokonya, O. (2021) ‘Evaluating the benefits of Cloud Computing in Small, Medium and Micro-sized Enterprises (SMMEs)’, in *Procedia Computer Science*. Available at: https://doi.org/10.1016/j.procs.2021.01.231.

Moeuf, A. *et al.* (2018) ‘The industrial management of SMEs in the era of Industry 4.0’, *International Journal of Production Research*, 56(3), pp. 1118–1136. Available at: https://doi.org/10.1080/00207543.2017.1372647.

Morrow, T. and Faatz, D. (2018) ‘12 Risks, Threats, & Vulnerabilities in Moving to the Cloud’, *Carnegie Mellon University* [Preprint].

Moustafa, A.A., Bello, A. and Maurushat, A. (2021) ‘The Role of User Behaviour in Improving Cyber Security Management’, *Frontiers in Psychology* [Preprint]. Available at: https://doi.org/10.3389/fpsyg.2021.561011.

Al Mudawi, N., Beloff, N. and White, M. (2019) ‘Cloud computing in government organizations-towards a new comprehensive model’, in *Proceedings - 2019 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Internet of People and Smart City Innovation, SmartWorld/UIC/ATC/SCALCOM/IOP/SCI 2019*. Available at: https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00266.

Muhati, E. (2018) ‘Factors affecting cyber-security in Kenya – A Case of Small Medium Enterprises’, *Strathmore University* [Preprint].

Muhss, F., Neumann, R. and Schmietendorf, A. (2011) ‘The commoditization of IT services with cloud computing’.

Mukherjee, S. (2018) ‘Challenges to Indian micro small scale and medium enterprises in the era of globalization’, *Journal of Global Entrepreneurship Research* [Preprint].

Available at: https://doi.org/10.1186/s40497-018-0115-5.

MUNIR, N. (2024) ‘The Impact of ISO 27001 Compliance on Employees’ Information Security Awareness and Behaviors in Medium Sized Enterprises (MSEs)’, *Luleå University of Technology Department of Computer Science, Electrical and Space Engineering* [Preprint].

Nafea, R. Al and Amin Almaiah, M. (2021) ‘Cyber Security Threats in Cloud: Literature Review’, in *2021 International Conference on Information Technology (ICIT)*, pp. 779–786. Available at: https://doi.org/10.1109/ICIT52682.2021.9491638.

Nagahawatta, R. *et al.* (2021) ‘Security concerns influencing the adoption of cloud computing by SMEs: A literature review’, in *27th Annual Americas Conference on Information Systems, AMCIS 2021*, pp. 1–10.

Nagahawatta, R.T.S., Warren, M. and Yeoh, W. (2020) ‘Ethical Issues Relating to Cyber Security in Australian SMEs’, *Aice* [Preprint].

Narwane, V.S. *et al.* (2019) ‘Factors affecting the adoption of cloud of things’, *Journal of Systems and Information Technology*, 21(4), pp. 397–418. Available at: https://doi.org/10.1108/JSIT-10-2018-0137.

Navimipour, N.J. and Zareie, B. (2015) ‘A model for assessing the impact of e-learning systems on employees’ satisfaction’, *Computers in Human Behavior*, 53, pp. 475–485. Available at: https://doi.org/10.1016/j.chb.2015.07.026.

Nguyen, G.T. and Liaw, S.-Y. (2022) ‘Understanding the Factors Affecting the Small and Medium Enterprises Adoption of Cloud computing: A Literature Review’, *International Journal of Business, Management and Economics* [Preprint]. Available at: https://doi.org/10.47747/ijbme.v3i2.635.

Niekerk, J.. Van and Solms, R. Von (2010) ‘Information security culture: A management perspective’, *Computers & Security*, 29(4), pp. 476–486. Available at: https://doi.org/10.1016/j.cose.2009.10.005.

Nita, S.L. and Mihailescu, M.I. (2018) ‘On Artificial Neural Network used in Cloud Computing Security - A Survey’, in *2018 10th International Conference on*

Electronics, Computers and Artificial Intelligence (ECAI). IEEE, pp. 1–6. Available at: https://doi.org/10.1109/ECAI.2018.8679086.

Nkwinika, E. and Akinola, S. (2023) 'The importance of financial management in small and medium-sized enterprises (SMEs): an analysis of challenges and best practices', *Technology audit and production reserves*, 5(4(73)), pp. 12–20. Available at: https://doi.org/10.15587/2706-5448.2023.285749.

Nowotarski, P. and Paslawski, J. (2017) 'Industry 4.0 Concept Introduction into Construction SMEs', in *IOP Conference Series: Materials Science and Engineering*. Available at: https://doi.org/10.1088/1757-899X/245/5/052043.

Oliveira, T., Thomas, M. and Espadanal, M. (2014) 'Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors', *Information & Management*, 51(5), pp. 497–510. Available at: https://doi.org/10.1016/j.im.2014.03.006.

Omowole, B.M. *et al.* (2024) 'Barriers and drivers of digital transformation in SMEs: A conceptual analysis', *International Journal of Scholarly Research in Science and Technology*, 5(2), pp. 019–036. Available at: https://doi.org/10.56781/ijsrst.2024.5.2.0037.

ONIK, M.M.H., KIM, C.-S. and YANG, J. (2019) 'Personal Data Privacy Challenges of the Fourth Industrial Revolution', in *2019 21st International Conference on Advanced Communication Technology (ICACT)*. IEEE, pp. 635–638. Available at: https://doi.org/10.23919/ICACT.2019.8701932.

Ooi, K.-B. *et al.* (2018) 'Cloud computing in manufacturing: The next industrial revolution in Malaysia?', *Expert Systems with Applications*, 93, pp. 376–394. Available at: https://doi.org/10.1016/j.eswa.2017.10.009.

Opara-Martins, J., Sahandi, R. and Tian, F. (2016a) 'Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective', *Journal of Cloud Computing* [Preprint]. Available at: https://doi.org/10.1186/s13677-016-0054-z.

Opara-Martins, J., Sahandi, R. and Tian, F. (2016b) 'Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective', *Journal of Cloud Computing*, 5(1), p. 4. Available at: https://doi.org/10.1186/s13677-016-0054-z.

Osborn, E. and Simpson, A. (2018) 'Risk and the Small-Scale Cyber Security Decision Making Dialogue - A UK Case Study', *Computer Journal* [Preprint]. Available at: https://doi.org/10.1093/comjnl/bxx093.

Otman, K. (2021) 'Small and Medium Enterprises in the Middle East and North Africa Region', *International Journal of Business and Management* [Preprint]. Available at: https://doi.org/10.5539/ijbm.v16n5p55.

P.S, S., S, N. and M, S. (2018) 'Overview of Cyber Security', *IJARCCE*, 7(11), pp. 125–128. Available at: https://doi.org/10.17148/IJARCCE.2018.71127.

Palos-Sanchez, P.R., Arenas-Marquez, F.J. and Aguayo-Camacho, M. (2017) 'Cloud Computing (SaaS) Adoption as a Strategic Technology: Results of an Empirical Study', *Mobile Information Systems*, 2017, pp. 1–20. Available at: https://doi.org/10.1155/2017/2536040.

Parsons, K.M. *et al.* (2015) 'The Influence of Organizational Information Security Culture on Information Security Decision Making', *Journal of Cognitive Engineering and Decision Making*, 9(2), pp. 117–129. Available at: https://doi.org/10.1177/1555343415575152.

Pathan, Z.H. *et al.* (2017) 'Essential factors in cloud-computing adoption by smes', *Human Systems Management* [Preprint]. Available at: https://doi.org/10.3233/HSM-17133.

Perera, S. *et al.* (2022) 'Factors Affecting Reputational Damage to Organisations Due to Cyberattacks', *Informatics*, 9(1), p. 28. Available at: https://doi.org/10.3390/informatics9010028.

Perwej, Y. *et al.* (2021) 'A Systematic Literature Review on the Cyber Security', *International Journal of Scientific Research and Management*, 9(12), pp.

669–710. Available at: https://doi.org/10.18535/ijsrm/v9i12.ec04.

Phaphoom, N. *et al.* (2015) 'A survey study on major technical barriers affecting the decision to adopt cloud services', in *Journal of Systems and Software*. Available at: https://doi.org/10.1016/j.jss.2015.02.002.

Pikaray, J., Mohapatra, S. and Kumar Rath, S. (2015) 'A New Approach toward Locating ERP Components on Cloud Computing Architecture', *Journal of Computer Sciences and Applications*. [Preprint].

Poehlmann, N. *et al.* (2021) 'The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review', in, pp. 377–395. Available at: https://doi.org/10.1007/978-3-030-71017-0_27.

Pollini, A. *et al.* (2022) 'Leveraging human factors in cybersecurity: an integrated methodological approach', *Cognition, Technology & Work*, 24(2), pp. 371–390. Available at: https://doi.org/10.1007/s10111-021-00683-y.

Priyadarshinee, P., Raut, R.D., Jha, M.K. and Kamble, S.S. (2017) 'A cloud computing adoption in Indian SMEs: Scale development and validation approach', *The Journal of High Technology Management Research*, 28(2), pp. 221–245. Available at: https://doi.org/10.1016/j.hitech.2017.10.010.

Priyadarshinee, P., Raut, R.D., Jha, M.K. and Gardas, B.B. (2017) 'Understanding and predicting the determinants of cloud computing adoption: A two staged hybrid SEM - Neural networks approach', *Computers in Human Behavior*, 76, pp. 341–362. Available at: https://doi.org/10.1016/j.chb.2017.07.027.

PWC (2021) *It's time to reimagine where and how work will get done*, *PwC's US Remote Work Survey*.

Ramachandra, G., Iftikhar, M. and Khan, F.A. (2017) 'A Comprehensive Survey on Security in Cloud Computing', in *Procedia Computer Science*. Available at: https://doi.org/10.1016/j.procs.2017.06.124.

Rao, S. (2018) 'Cloud computing: Face and shape in 2018'.

Raut, R.D. *et al.* (2017) 'Examining the critical success factors of cloud computing

adoption in the MSMEs by using ISM model', *The Journal of High Technology Management Research*, 28(2), pp. 125–141. Available at: https://doi.org/10.1016/j.hitech.2017.10.004.

Raut, R.D. *et al.* (2018) 'Analyzing the factors influencing cloud computing adoption using three stage hybrid SEM-ANN-ISM (SEANIS) approach', *Technological Forecasting and Social Change* [Preprint]. Available at: https://doi.org/10.1016/j.techfore.2018.05.020.

Rawindaran, N. *et al.* (2023) 'Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom', *Digital*, 3(3), pp. 200–231. Available at: https://doi.org/10.3390/digital3030014.

Reid, R. and Niekerk, J. Van (2014) 'From Information Security to Cyber Security Cultures Organizations to Societies', in *Information Security South Africa (ISSA)*. Available at: https://doi.org/978-1-4799-3383-9.

Rekik, M., Boukadi, K. and Abdallah, H. Ben (2019) 'An end-to-end system to enhance business process performance through new outsourcing to the cloud strategies', *International Journal of Business and Systems Research*, 13(1), p. 1. Available at: https://doi.org/10.1504/IJBSR.2019.096358.

Reyes, E.F.V. (2021) 'Critical Factors for ICT Adoption in Industrial Sector Micro and Small Enterprises (MSEs)', 24(2).

Riera, C. and Iijima, J. (2019) 'The Role of IT and Organizational Capabilities on Digital Business Value', *Pacific Asia Journal of the Association for Information Systems* [Preprint]. Available at: https://doi.org/10.17705/1pais.11204.

Ruaro, A.F. and Rabelo, R.J. (2016) 'Do cloud computing tools support the needs of virtual enterprises?', in *IFIP Advances in Information and Communication Technology*. Available at: https://doi.org/10.1007/978-3-319-45390-3_41.

Sabi, H.M. *et al.* (2016) 'Conceptualizing a model for adoption of cloud computing in education', *International Journal of Information Management*, 36(2), pp.

183–191. Available at: https://doi.org/10.1016/j.ijinfomgt.2015.11.010.

Sallehudin, H. *et al.* (2020) 'Performance and key factors of cloud computing implementation in the public sector', *International Journal of Business and Society* [Preprint].

Sandu, R. and Gide, E. (2018) 'Technological, Organisational and Environmental (TOE) Factors that Influence the Adoption of Cloud Based Service SMEs in India', in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, pp. 866–870. Available at: https://doi.org/10.1109/CLOUD.2018.00123.

Sarkar, S. *et al.* (2022) 'Security of Zero Trust Networks in Cloud Computing: A Comparative Review', *Sustainability*, 14(18), p. 11213. Available at: https://doi.org/10.3390/su141811213.

Schoenmakers, K. *et al.* (2023) 'The security mindset: characteristics, development, and consequences', *Journal of Cybersecurity* [Preprint]. Available at: https://doi.org/10.1093/cybsec/tyad010.

Scholtz, B., Govender, J. and Gomez, J.M. (2016) 'Technical and Environmental Factors Affecting Cloud Computing Adoption in the South African Public Sector'.

Senarathna, I. *et al.* (2018) 'Factors That Influence Adoption of Cloud Computing: An Empirical Study of Australian SMEs', *Australasian Journal of Information Systems*, 22. Available at: https://doi.org/10.3127/ajis.v22i0.1603.

Sengupta, S., Kaulgud, V. and Sharma, V.S. (2011) 'Cloud Computing Security--Trends and Research Directions', in *2011 IEEE World Congress on Services*. IEEE, pp. 524–531. Available at: https://doi.org/10.1109/SERVICES.2011.20.

Senyo, P.K., Addae, E. and Boateng, R. (2018) 'Cloud computing research: A review of research themes, frameworks, methods and future research directions', *International Journal of Information Management* [Preprint]. Available at: https://doi.org/10.1016/j.ijinfomgt.2017.07.007.

Senyo, P.K., Effah, J. and Addae, E. (2016) 'Preliminary insight into cloud computing adoption in a developing country', *Journal of Enterprise Information*

Management [Preprint]. Available at: https://doi.org/10.1108/JEIM-09-2014-0094.

Shanbhag, R.R. *et al.* (2020) 'Overview of Cloud Computing in the Process Control Industry', *International Journal of Computer Science and Mobile Computing*, 9(10), pp. 121–146. Available at: https://doi.org/10.47760/ijcsmc.2020.v09i10.016.

Sharma, S.K. *et al.* (2016) 'Predicting motivators of cloud computing adoption: A developing country perspective', *Computers in Human Behavior* [Preprint]. Available at: https://doi.org/10.1016/j.chb.2016.03.073.

Shen, Jian *et al.* (2018) 'Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks', *Journal of Network and Computer Applications* [Preprint]. Available at: https://doi.org/10.1016/j.jnca.2018.01.003.

Shetty, J.P., Choudhury, D. and Panda, R. (2020) 'MSME initiatives to support cloud adoption in India', *International Journal of Indian Culture and Business Management* [Preprint]. Available at: https://doi.org/10.1504/ijicbm.2020.109751.

Shetty, J.P. and Rajesh, P. (2021) 'An overview of cloud computing in SMEs', *Journal of Global Entrepreneurship Research*, 11. Available at: https://doi.org/10.1007/s40497-021-00273-2.

Shiau, W.-L. and Chau, P.Y.K. (2016) 'Understanding behavioral intention to use a cloud computing classroom: A multiple model comparison approach', *Information & Management*, 53(3), pp. 355–365. Available at: https://doi.org/10.1016/j.im.2015.10.004.

Singh, D. (2019) 'Implementation of technology innovation in MSMEs in India', *Journal of Science and Technology Policy Management*, 10(3), pp. 769–792. Available at: https://doi.org/10.1108/JSTPM-06-2018-0065.

Singh, M., Yadav, R. and Dang, P. (2017) 'The Adoption of Cloud Computing by Indian SME - an Exploratory Study', *11th INDIACom; 4th International Conference on 'Computing for Sustainable Global Development', INDIACom 2017*, 1(8), pp.

5131–5136.

Singh, S., Jeong, Y.-S. and Park, J.H. (2016) ‘A survey on cloud computing security: Issues, threats, and solutions’, *Journal of Network and Computer Applications*, 75, pp. 200–222. Available at: https://doi.org/10.1016/j.jnca.2016.09.002.

Skafi, M., Yunis, M.M. and Zekri, A. (2020) ‘Factors influencing SMEs’ adoption of cloud computing services in Lebanon: An empirical analysis using TOE and contextual theory’, *IEEE Access* [Preprint]. Available at: https://doi.org/10.1109/ACCESS.2020.2987331.

Small Business Administration (2018) ‘Small Business Profiles for the States, Territories, and Nation’.

Sommer, T. and Subramanian, R. (2013) ‘Implementing Cloud Computing in Small and Mid-Market Life-Sciences: A Mixed-Method Study’, *Journal of International Technology and Information Management* [Preprint].

Srinivasan, S. (2013) ‘Is Security Realistic in Cloud Computing?’, *Journal of International Technology and Information Management* [Preprint]. Available at: https://doi.org/10.58729/1941-6679.1020.

Subramanian, N. and Jeyaraj, A. (2018) ‘Recent security challenges in cloud computing’, *Computers & Electrical Engineering*, 71, pp. 28–42. Available at: https://doi.org/10.1016/j.compeleceng.2018.06.006.

Sun, X. (2018) ‘Critical Security Issues in Cloud Computing: A Survey’, in *2018 IEEE 4th 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)*. IEEE, pp. 216–221. Available at: https://doi.org/10.1109/BDS/HPSC/IDS18.2018.00053.

Swire, P. *et al.* (2024) ‘Risks to cybersecurity from data localization, organized by techniques, tactics and procedures’, *Journal of Cyber Policy*, pp. 1–32. Available at: https://doi.org/10.1080/23738871.2024.2384724.

Takabi, H., Joshi, J.B.D. and Ahn, G.-J. (2010) 'Security and Privacy Challenges in Cloud Computing Environments', *IEEE Security & Privacy Magazine*, 8(6), pp. 24–31. Available at: https://doi.org/10.1109/MSP.2010.186.

Tang, M. *et al.* (2017) 'Towards a trust evaluation middleware for cloud service selection', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/10.1016/j.future.2016.01.009.

Thakurta, R., Urbach, N. and Basu, A. (2018) 'Understanding Technology Transition at the Individual Level', *Pacific Asia Journal of the Association for Information Systems*, pp. 25–60. Available at: https://doi.org/10.17705/1pais.10302.

Thong, J.Y.L. (1999) 'An Integrated Model of Information Systems Adoption in Small Businesses', *Journal of Management Information Systems*, 15(4), pp. 187–214. Available at: https://doi.org/10.1080/07421222.1999.11518227.

Thorgren S, W.T. (2020) 'Staying alive during an unfolding crisisHow SMEs ward off impending disaster'.

Tissir, N., El Kafhali, S. and Aboutabit, N. (2021) 'Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal', *Journal of Reliable Intelligent Environments* [Preprint]. Available at: https://doi.org/10.1007/s40860-020-00115-0.

Tu, S. *et al.* (2020) 'Mobile fog computing security: A user-oriented smart attack defense strategy based on DQL', *Computer Communications*, 160, pp. 790–798. Available at: https://doi.org/10.1016/j.comcom.2020.06.019.

Ullman, S. *et al.* (2024) 'Enhancing Vulnerability Prioritization in Cloud Computing Using Multi-View Representation Learning', *Journal of Management Information Systems*, 41(3), pp. 708–743. Available at: https://doi.org/10.1080/07421222.2024.2376384.

Vance, A., Siponen, M.T. and Straub, D.W. (2020) 'Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures', *Information & Management*, 57(4), p. 103212. Available at:

https://doi.org/10.1016/j.im.2019.103212.

Vandita, Jaiswal, A.K. and Srivastava, R. (2023) 'Role of Digitalization in the Growth of MSMEs in India: Opportunities and Challenges', *International Journal for Multidisciplinary Research (IJFMR)*, 05(05).

Varghese, B. and Buyya, R. (2018) 'Next generation cloud computing: New trends and research directions', *Future Generation Computer Systems* [Preprint]. Available at: https://doi.org/10.1016/j.future.2017.09.020.

Venters, W. and Whitley, E.A. (2012) 'A Critical Review of Cloud Computing: Researching Desires and Realities', *Journal of Information Technology*, 27(3), pp. 179–197. Available at: https://doi.org/10.1057/jit.2012.17.

Vos, A. *et al.* (2014) 'Risk Reduction Strategies in Online Shopping: E-trust Perspective', *Procedia - Social and Behavioral Sciences* [Preprint]. Available at: https://doi.org/10.1016/j.sbspro.2014.07.122.

Vu, K., Hartley, K. and Kankanhalli, A. (2020) 'Predictors of cloud computing adoption: A cross-country study', *Telematics and Informatics* [Preprint]. Available at: https://doi.org/10.1016/j.tele.2020.101426.

Wamuyu, P.K. (2022) 'Use of cloud computing services in micro and small enterprises: a fit perspective', *International Journal of Information Systems and Project Management*, 5(2), pp. 59–81. Available at: https://doi.org/10.12821/ijispm050204.

Wang, L.-Y.-K. *et al.* (2019) 'Usability factors predicting continuance of intention to use cloud e-learning application', *Heliyon*, 5(6), p. e01788. Available at: https://doi.org/10.1016/j.heliyon.2019.e01788.

Wang, Y. and Wei, J. (2015) 'Toward protecting control flow confidentiality in cloud-based computation', *Computers & Security*, 52, pp. 106–127. Available at: https://doi.org/10.1016/j.cose.2015.04.005.

Waqas, M. *et al.* (2020) 'A Comprehensive Survey on Mobility-Aware D2D Communications: Principles, Practice and Challenges', *IEEE Communications*

Surveys & Tutorials, 22(3), pp. 1863–1886. Available at: https://doi.org/10.1109/COMST.2019.2923708.

Weerd, I. van de, Mangula, I.S. and Brinkkemper, S. (2016) 'Adoption of software as a service in Indonesia: Examining the influence of organizational factors', *Information & Management*, 53(7), pp. 915–928. Available at: https://doi.org/10.1016/j.im.2016.05.008.

Werfs, M. *et al.* (2013) 'Migrating Software Products to the Cloud', *Journal of International Technology and Information Management* [Preprint]. Available at: https://doi.org/10.58729/1941-6679.1014.

Whitley, E. a, Willcocks, L.P. and Venters, W. (2013) 'Privacy and Security in the Cloud: A Review of Guidance and Responses.', *Journal of International Technology & Information Management* [Preprint].

Whittaker, B. (1999) 'What went wrong? Unsuccessful information technology projects', *Information Management & Computer Security*, 7(1), pp. 23–30. Available at: https://doi.org/10.1108/09685229910255160.

Xiao, Y. and Watson, M. (2019) 'Guidance on Conducting a Systematic Literature Review', *Journal of Planning Education and Research* [Preprint]. Available at: https://doi.org/10.1177/0739456X17723971.

Xie, X. *et al.* (2015) 'Research of job scheduling with cloud based on trust mechanism and SFLA', *International Journal of Grid and Distributed Computing* [Preprint]. Available at: https://doi.org/10.14257/ijgdc.2015.8.1.09.

Yang, C. *et al.* (2017) 'Utilizing Cloud Computing to address big geospatial data challenges', *Computers, Environment and Urban Systems* [Preprint]. Available at: https://doi.org/10.1016/j.compenvurbsys.2016.10.010.

Yang, H. and Tate, M. (2012) 'A descriptive literature review and classification of cloud computing research', *Communications of the Association for Information Systems* [Preprint]. Available at: https://doi.org/10.17705/1cais.03102.

Yoshino, N. (2016) 'Major Challenges Facing Small and Medium-Sized Enterprises in

Asia and Solutions for Mitigating Them', *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/ssrn.2766242.

Younus, M. *et al.* (2025) 'Analyzing the trend of government support for cloud computing usage in e-government architecture', *Journal of Cloud Computing*, 14(1), p. 14. Available at: https://doi.org/10.1186/s13677-025-00735-y.

Yu, Y. *et al.* (2018) 'Effects of entrepreneurship and IT fashion on SMEs' transformation toward cloud service through mediation of trust', *Information & Management*, 55(2), pp. 245–257. Available at: https://doi.org/10.1016/j.im.2017.07.001.

ZA, M. (2022) 'Cybersecurity and cloud computing: Risks and benefits'.

Zaman, S. (2024) 'A Systematic Review of ERP And CRM Integration For Sustainable Business And Data Management in Logistics And Supply Chain Industry', *Innovatech Engineering Journal*, 1(01), pp. 204–221. Available at: https://doi.org/10.70937/faet.v1i01.36.

Zhang, Q., Cheng, L. and Boutaba, R. (2010) 'Cloud computing: state-of-the-art and research challenges', *Journal of Internet Services and Applications*, 1(1), pp. 7–18. Available at: https://doi.org/10.1007/s13174-010-0007-6.

Zhang, Y. (2024) 'Research on the Application and Benefits of Financial Cloud in Small and Medium Sized Enterprises', *Highlights in Business, Economics and Management*, 37.

Zhao, J., Zhang, L. and Zhao, Y. (2022) 'Informatization of Accounting Systems in Small- and Medium-Sized Enterprises Based on Artificial Intelligence-Enabled Cloud Computing', *Computational Intelligence and Neuroscience*. Edited by S. Mumtaz, 2022, pp. 1–9. Available at: https://doi.org/10.1155/2022/6089195.

APPENDIX A:

DATASET

What is your age?	What is your gender?	What is your current employment status?	Which industry do you currently work in?	What is your highest level of education?	How many years of experience do you have in the field of AI or Machine Learning?	Which AI/Machine Learning techniques have you used in your work?	Which programming languages do you frequently use in your AI/ML projects?	I am concerned about the privacy of sensitive data stored on cloud platforms.	Cloud service providers adequately address data privacy issues.	I worry about unauthorized access to confidential data in the cloud.	Cloud systems ensure sufficient measures to protect data confidentiality.	Ensuring the integrity of data stored in the cloud is a major concern.	Cloud providers effectively maintain data integrity.
2	1	1	1	3	3	3	6	4	5	4	5	4	5
1	2	2	2	3	1	1	1	5	5	5	4	4	4
1	1	1	1	3	2	1	1	4	5	4	3	4	5
1	1	2	3	3	2	4	1	4	5	4	4	5	5
1	1	1	1	3	2	6	1	5	4	3	5	4	3
3	1	3	4	4	4	2	3	4	4	5	4	4	4
1	1	4	4	3	1	6	1	5	4	4	5	4	5
1	2	1	1	3	2	1	1	3	2	5	3	2	3
2	2	1	7	4	3	6	1	4	5	4	3	3	3
1	2	1	1	3	2	5	1	5	5	5	4	5	4
2	2	2	4	4	2	4	1	1	4	5	5	4	4
4	1	6	3	5	5	5	3	4	3	5	5	3	3
3	1	1	1	5	4	4	5	4	4	3	5	5	5
1	2	1	1	4	3	4	1	4	4	4	4	4	4
4	1	6	2	5	2	3	3	2	4	3	2	1	3
1	1	2	3	3	1	3	6	4	5	4	4	5	4
3	2	1	6	2	3	2	2	5	5	5	4	4	5
1	2	1	3	4	2	3	1	4	5	4	5	5	5
1	2	2	2	4	2	3	1	3	3	4	4	5	4
1	1	1	1	3	2	6	1	5	4	4	5	4	3
5	2	2	2	4	5	5	3	1	3	1	5	1	2
2	2	2	4	5	3	3	3	3	3	2	3	2	3
1	1	1	1	4	3	4	3	5	4	5	5	5	5
2	2	1	1	3	1	3	1	4	5	5	4	4	5
2	2	3	4	2	1	4	4	1	2	2	2	3	4
1	2	1	1	3	1	6	6	4	3	5	3	5	4
1	2	2	2	3	2	3	1	2	4	3	4	5	4
2	2	6	5	5	2	5	3	3	3	4	5	4	3
1	1	1	5	3	1	4	3	3	4	5	5	4	5
1	1	1	1	3	2	4	1	5	4	5	4	3	5
3	1	4	3	4	3	3	4	3	3	4	5	5	2
2	2	1	1	3	2	3	1	4	4	4	4	5	5
1	2	1	3	3	3	5	5	1	2	5	1	5	1
2	2	1	3	2	2	4	3	4	5	5	5	3	4
1	1	5	1	3	1	1	1	5	4	4	4	3	5
2	1	3	4	4	4	3	2	5	3	5	3	5	3
5	1	6	3	5	5	3	1	5	5	4	4	3	4
2	1	5	2	3	2	6	1	4	2	5	2	4	1
1	1	3	1	3	2	2	1	5	4	3	3	4	5
3	1	6	1	2	2	3	2	1	2	2	2	2	3

I am concerned about the availability of my data when needed.	Cloud providers have robust mechanisms to ensure continuous access to data.	I perceive a high risk of data breaches when using cloud services.	Cloud providers take adequate measures to mitigate the risk of data breaches.	Our organization is technologically prepared for cloud computing adoption.	We have the necessary IT infrastructure to support cloud adoption.	The organization has sufficient financial resources to invest in cloud solutions.	Budgetary constraints hinder our ability to adopt cloud computing.	Top management is actively involved in cloud adoption decisions.	Senior leadership supports the allocation of resources for cloud initiatives.	The organization is aware of the potential benefits of cloud computing.	Employees understand how cloud computing can enhance business processes.	Competitive pressure drives our organization to adopt cloud computing.	Competitors using cloud computing gain a significant competitive advantage.
4	5	4	5	4	5	4	5	4	5	4	5	4	5
5	3	4	4	5	4	3	4	2	4	1	4	5	4
4	3	4	5	4	3	4	5	4	5	3	4	5	4
4	4	4	5	5	4	4	5	4	4	5	5	4	4
5	4	5	4	5	4	5	4	4	5	4	5	4	5
5	3	5	4	3	4	4	4	5	4	4	4	4	3
4	4	5	4	4	4	5	4	4	5	4	4	4	4
1	5	1	5	3	5	3	3	2	5	3	5	3	2
4	4	5	4	4	5	4	4	4	3	4	4	4	4
5	4	5	5	4	5	4	5	4	5	4	4	5	4
5	4	5	4	5	5	4	4	4	4	4	4	4	3
3	2	4	2	4	2	2	2	4	3	3	2	1	4
4	4	4	3	3	3	4	4	5	5	4	4	4	5
4	4	4	4	4	4	4	4	4	4	4	4	4	4
5	4	3	2	1	3	4	2	5	4	3	2	2	4
5	3	4	5	5	4	5	5	4	5	5	3	4	4
4	4	5	5	4	4	5	4	4	5	4	4	2	2
4	4	5	4	4	4	5	5	5	5	4	5	5	5
3	5	5	4	5	4	5	4	5	5	5	5	5	4
5	3	4	4	5	3	3	5	4	5	3	4	5	4
3	2	3	1	5	4	2	3	3	3	3	2	4	3
3	2	3	3	2	3	3	2	3	2	3	2	2	2
5	4	4	4	5	5	5	4	4	5	4	5	4	4
4	5	4	5	4	5	4	5	4	5	4	5	5	4
3	1	4	5	4	2	3	3	3	3	4	5	2	3
2	5	4	2	5	3	1	5	2	4	2	4	2	5
3	4	5	4	3	4	5	4	3	4	5	3	4	5
5	4	3	5	4	5	3	4	4	3	4	5	4	5
4	3	4	5	5	5	5	4	3	3	3	4	4	4
4	3	4	5	3	4	5	5	3	4	4	5	3	5
5	5	4	3	5	5	4	3	5	2	4	5	5	4
5	5	5	5	5	5	5	5	5	5	5	5	5	5
4	2	3	2	3	4	5	5	5	4	2	3	4	5
4	5	4	4	3	4	5	4	4	3	4	5	4	4
4	3	4	5	5	5	5	3	4	5	4	3	4	5
3	5	3	4	5	5	3	4	5	4	3	5	5	5
4	3	3	5	5	5	5	5	5	4	3	4	3	4
2	4	2	3	4	1	2	5	3	2	3	4	2	5
2	4	5	4	4	3	4	5	3	3	5	4	5	3
3	3	3	1	3	4	4	4	4	4	3	3	3	2

Reliable internet connectivity is critical for adopting cloud computing.	Internet speed in our area is sufficient to support cloud computing adoption.	Our geographical location affects the availability of cloud service providers.	Location-specific challenges hinder our ability to adopt cloud technologies.	I am concerned about being locked into a specific cloud vendor's ecosystem.	Vendor lock-in limits our ability to switch providers without significant cost or effort.	Frequent downtime or outages are a major concern with cloud services.	The reliability of cloud services affects our willingness to adopt them.	I am concerned about losing control over data stored in the cloud.	Using cloud services compromises our ability to manage and secure our data effectively.	Cloud computing helps reduce overall IT costs for our organization.	Adopting cloud services leads to better cost management.	Cloud computing provides the flexibility to scale resources as needed.	The scalability of cloud services enhances operational efficiency.
4	5	4	5	4	5	4	5	4	5	4	5	4	5
3	4	3	3	4	3	4	3	3	3	4	3	3	4
3	4	3	4	5	4	5	4	4	5	4	3	4	4
5	4	5	5	5	5	4	5	5	4	5	4	5	5
5	4	5	4	5	4	5	4	5	4	5	5	4	5
4	3	3	4	4	4	3	3	5	4	5	1	4	4
4	4	4	1	4	5	5	5	1	5	4	4	4	3
3	3	5	2	3	2	5	2	3	3	3	5	2	1
4	3	4	4	4	3	5	5	4	3	4	5	4	3
5	4	5	4	5	4	5	4	4	5	5	4	4	5
4	4	4	4	4	4	4	4	4	4	5	4	4	5
3	3	2	3	3	3	5	1	3	2	3	2	5	3
4	3	3	4	5	4	4	5	4	5	5	5	3	3
4	4	4	4	4	4	4	4	4	4	4	4	4	4
3	1	5	4	3	2	2	3	3	4	4	3	2	1
4	5	3	4	5	4	5	4	5	4	4	3	4	4
3	3	2	2	2	3	2	2	2	2	3	2	2	2
5	5	5	5	5	5	5	5	5	5	5	5	5	5
5	3	4	4	2	4	4	3	5	4	5	4	5	5
3	4	5	4	5	4	3	4	4	5	3	2	4	4
2	2	4	3	2	5	4	3	4	2	5	3	3	2
2	3	2	2	2	2	4	2	2	3	3	2	3	2
4	5	4	5	4	5	4	5	4	4	5	5	4	5
4	5	4	5	4	5	4	5	4	4	5	4	5	4
3	3	4	4	3	3	3	3	3	3	3	3	3	3
2	5	2	4	1	5	1	3	4	2	5	2	5	2
4	3	3	4	5	5	4	4	4	5	4	3	4	5
3	4	4	4	5	4	3	5	5	3	4	5	4	2
5	5	4	5	5	4	4	4	4	4	5	4	5	4
4	3	5	3	4	5	4	3	2	4	5	3	4	2
3	5	4	5	3	4	5	5	4	4	3	5	5	3
5	5	5	5	5	5	5	5	5	5	5	5	5	5
4	3	4	4	4	4	4	4	3	3	3	3	4	4
5	4	4	5	5	5	4	4	4	4	4	3	4	5
5	4	3	4	4	5	5	4	4	4	5	4	4	4
2	5	5	5	3	5	3	5	4	3	4	4	1	5
3	4	3	4	5	4	5	4	5	4	5	4	5	4
2	5	2	5	1	5	2	5	3	5	1	5	2	3
5	3	4	5	3	5	4	3	5	4	3	5	3	2
3	4	2	3	3	4	4	1	2	4	4	4	4	3

Cloud computing is easy to adopt and integrate into existing business operations.	Employees find cloud-based tools and services user-friendly and efficient.	The reputation of cloud service providers influences our trust in their services.	Compliance with industry security standards enhances trust in cloud providers.	Cloud service providers are transparent about how they handle and protect data.	Providersâ€™ clear communication about security policies builds trust.	Our organization is actively considering adopting cloud computing.	Cloud computing offers significant advantages for our business operations.	The adoption of cloud computing will help us reduce IT infrastructure costs.	Cloud computing services are reliable and meet our business needs.	We are concerned about data security when using cloud computing services.	The flexibility and scalability of cloud computing are important for our business.	Our staff has the necessary skills and knowledge to adopt cloud computing.	Cloud computing helps improve collaboration and communication within our organization.
4	5	4	5	4	5	4	5	4	5	4	5	4	5
3	3	3	3	3	3	3	3	3	4	3	4	4	3
4	3	4	4	4	3	4	4	5	4	3	4	3	4
4	5	4	5	4	3	4	3	5	5	4	4	5	4
5	5	4	5	4	5	4	5	5	4	3	4	5	4
3	4	4	4	4	3	5	3	4	4	3	3	4	3
4	4	3	4	3	4	3	3	4	3	3	4	4	5
5	4	3	3	5	3	3	3	3	1	4	3	1	4
4	5	5	4	3	4	5	4	4	3	4	5	3	3
4	5	4	5	4	3	4	5	5	5	5	4	5	4
4	4	4	4	5	5	4	4	4	4	3	4	4	4
5	4	5	4	5	3	3	3	3	2	5	2	2	2
4	4	4	3	4	5	4	3	4	5	4	3	5	4
4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	2	2	2	2	2	2	2	2	2	3	4	4
5	5	4	4	4	5	4	4	5	3	5	4	4	5
2	2	3	5	2	2	3	2	2	2	2	2	2	2
5	5	5	5	5	5	5	5	5	5	5	5	5	5
4	1	5	4	5	5	3	4	4	2	5	4	5	5
5	4	5	3	4	4	3	3	4	4	3	4	3	4
3	4	2	3	4	4	3	3	3	5	1	5	3	5
3	3	2	3	2	4	2	3	2	3	3	3	2	2
3	4	5	5	5	4	5	4	4	4	5	4	5	5
5	4	4	4	5	4	5	5	5	4	4	5	4	5
3	2	4	5	4	3	4	5	4	3	4	3	3	5
4	3	5	2	5	2	5	3	1	5	2	4	3	4
3	4	5	4	3	4	5	4	3	3	4	5	4	3
5	5	5	3	5	4	5	4	4	5	5	2	5	5
4	4	5	5	5	4	5	4	5	4	4	5	4	4
5	4	3	4	5	5	3	4	5	4	5	3	4	5
5	4	5	3	5	4	5	5	2	5	4	5	3	5
5	5	5	5	5	5	5	5	5	5	5	5	5	5
3	3	4	4	4	3	4	4	4	4	3	4	3	4
3	4	4	4	4	4	4	4	4	5	4	4	4	4
4	3	4	4	4	4	4	4	5	5	4	4	4	5
4	5	2	2	2	3	2	3	2	4	2	2	2	2
5	4	5	4	5	4	5	4	5	4	5	4	5	4
4	2	5	2	5	2	5	3	4	4	2	2	5	3
4	5	2	5	4	3	4	5	5	3	5	5	3	4
4	4	5	4	3	4	5	5	4	5	4	4	4	5