CYBER SECURITY IN CLOUD COMPUTING ENVIRONMENTS: RISKS & SOLUTIONS

by

Ravindra Mugula

DISSERTATION

Presented to the Swiss School of Business and Management, Geneva

In Partial Fulfilment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

JANUARY, 2026

CYBER SECURITY IN CLOUD COMPUTING ENVIRONMENTS: RISKS & SOLUTIONS

by

Ravindra Mugula

Supervised by

Dr. Anna Provodnikova

APPROVED BY

Apostolos Dasilas

Dissertation chair

RECEIVED/APPROVED BY:

Renee Goldstein Osmic

Admissions Director

ABSTRACT

CYBER SECURITY IN CLOUD COMPUTING ENVIRONMENTS: RISKS & SOLUTIONS

Ravindra Mugula
2026

Dissertation Chair: Dr. Anna Provodnikova

This research project examines significant security threats to cloud computing services and tests various protective tools to determine which ones most effectively address these issues. Our primary objective is to analyse how combining data encryption (DE), access control (AC), and Intrusion Detection Systems (IDS) enhances cloud security compliance and performance.

The study employs structured questionnaires to gather responses from 300 experts, including IT professionals, cybersecurity specialists, and cloud service providers (CSPs). Participants were selected through convenience sampling due to their professional expertise in securing cloud systems (CS). Fixed response questions are used in the survey to collect precise data on security features, including encryption methods, access permission and IDA. Descriptive statistics and inferential analysis findings were generated by using the Statistical Package for the Social Sciences (SPSS) for the data analysis.

Our findings indicate that data encryption protects against unauthorised access and data loss, while IDA effectively prevent malware attacks and data theft. Access control in a fully integrated security system demonstrates its ability to shield organisations from insider

threats and credential theft. Overall, security solutions that work in tandem offer enhanced cloud protection and help organisations meet their security requirements.

Robust security systems protect data integrity, ensure regulatory compliance, and mitigate advanced internet threats, leading to increased trust and improved performance in cloud-based environments. These results are significant for security practitioners across multiple industries and for cloud security researchers, who will benefit from the detailed insights this study provides. Our research contributes new perspectives on cloud security by examining the interplay between cloud threats, security tools, and system performance.

Keywords: Cybersecurity, Data Encryption (DE), Access Control (AC), Intrusion Detection Systems (IDS), Cloud Security Compliance, Cloud Security Effectiveness.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviations	Full Form
SPSS	Statistical Package for The Social Sciences
DE	Data Encryption
AC	Access Control
IDS	Intrusion Detection Systems
CC	Cloud Computing
EC2	Elastic Compute Cloud
NIST	National Institute of Standards and Technology
M2FC	Multi-Dimensional Mean Failure Cost
AWS	Amazon Web Services
IT	Information Technology
ROI	Return on Investment
SaaS	Software as A Service
IaaS	Infrastructure as A Service
SOA	Service-Oriented Architecture
SLAs	Service Level Agreements
CSA	Cloud Security Alliance
OCC	Open Cloud Consortium
SNIA	Storage Networking Industry Association
ENISA	European Network and Information Security Agency
IAM	Identity and Access Management
AAA	Authentication, Authorization, And Access Control
CSPs	Centralized Service Providers
ACID	Atomicity, Consistency, Isolation, And Durability

BC	Business Continuity
DR	Disaster Recovery
APIs	Application Programming Interfaces
DLP	Data Loss Prevention
CSE	Cloud Security Effectiveness

CHAPTER I:

INTRODUCTION

1.1 Introduction to Cyber Security and Cloud Computing

The term "Internet of Things" (IoT)-based cloud architecture refers to a wide network that includes multiple applications and devices made possible by the IoT. Infrastructure consists of the underlying systems, servers, storage, real-time processing, and operations. A different Internet of Things (IoT) cloud architecture incorporates the essential and globally applicable standards and services for the administration, safety, and connection of different IoT applications and devices. Figure 1.2 provides a high-level view of the IoT-based cloud attack paradigm, while Figure 1.1 shows the traditional IoT architecture. Many different kinds of clouds have emerged in the past decade, and they first appeared during that time (Karam, Baker and Taleb-Bendiab, 2012; Mohiyuddin *et al.*, 2022; Abid *et al.*, 2023). Some, on the other hand, adhere to current trends; these include service architectures, management domains, data centre operations, and distributed cloud environments. According to a recent research released by Gartner Cearley *et al.* (2019) Cloud computing (CC) is predicted to boost the cloud service market by 17% in 2020, making it one of the top ten strategic technology trends for that year.

Figure 1.1: Typical IoT architecture (Source: Nasir *et al.*, 2022, p.8852-8866)

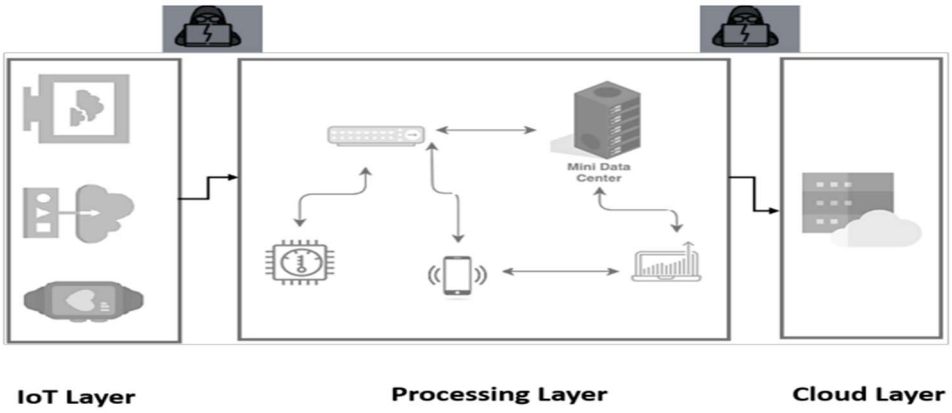

Figure 1.2: IoT-based cloud attack model (Source: Ahmad *et al.*, 2022, p.16)

It was in the 1990s when the phrase CC initially appeared in print, describing dispersed computing platforms. Take Amazon's 2006 "Elastic Compute Cloud" (EC2) as an example. The same holds for Google App Engine; in 2008, the company published the beta version. To facilitate the launch of private and hybrid clouds, NASA launched Open Nebula in 2008, the initial open-source program of its kind (Larsson, Henriksson and Elmroth, 2011). 2008 saw the launching of Microsoft Azure, while 2010 saw the introduction of the open-source CC project OpenStack. IBM created its smart cloud platform in 2011. 2012 was the first year Oracle Cloud began to provide PaaS, SaaS and IaaS (infrastructure as a service). Even now, this journey has much further to go as there are new developments in the digital realm imminent. The evolution of CC is shown in Figure 1.3.

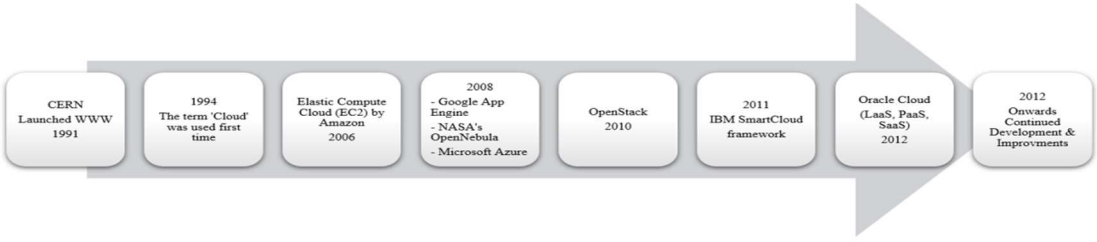

Figure 1.3: Cloud computing history (Source: Ahmad et al., 2022, p.16)

According to Mell and Grance (2011), "National Institute of Standards and Technology" (NIST) states that the CC model is defined by five features. It is necessary

to investigate the following: first, self-service that is available whenever needed; second, sharing resources; third, quick growth; fourth, access to networks; and fifth, measured service. In addition, four different deployment methodologies and three different service models are available for cloud service provisioning. Hosting, data storage, database administration, networking, software, analytics, and intelligence suppliers are CC's primary goals. Based on their special needs, users can modify the type and amount of services which they are offered. Due to its cost-effectiveness, convenience, and ability to store and retrieve data rapidly, CC has supplanted traditional IT services. Due to CC, businesses are no longer required to invest significant money in constructing expensive on-premises data centres. Using remote servers to store software systems and services makes CC possible, automating various businesses. Today, this approach is being followed by an expanding number of industries (Ghobaei-Arani *et al.*, 2019). The scalability and rapid software and hardware updates offered by CC make it ideal for many industrial applications (Baker *et al.*, 2013; Al-khafajiy *et al.*, 2020; Shabbir *et al.*, 2021). CC also gives users many security alternatives and lets them maximise their network resources. With these benefits, CC seems like it will be a fun ride. Industries are poised to reap substantial benefits from CC and underlying technologies due to the vast array of new applications, solutions, services, platforms, and more that they have the potential to bring. With the help of CC, deep learning utilises large datasets and various training methodologies. Its use can also assist deep learning models in attaining cost-effective scalability using GPU processing power. Everybody, from cloud administrators and developers to software and end-users, is counting on a flawless experience for any cloud-based solution to reach its full potential. Complexity, security, dependence, compliance, privacy, control, and expense are some hurdles to cloud adoption (Xia *et al.*, 2021). CC security is a major concern since, depending on the model chosen, data and apps can live on different cloud

layers. Researchers ranked security as their top concern when it came to CC due to this unpredictability. Distributing virtual environments and diverse data and resources is what the cloud is all about. CC allows users to have access to infinite storage space and additional server resources as needed, in contrast to restricted compute capabilities, storage space, and hardware accessible in traditional commercial software infrastructure. Current methods of user authentication, identity, and access management are not cloud-friendly. Some factors raise serious security concerns, including the usage of reduced user control, external data storage, and integrated models and architectures. Data protection is the top priority when it comes to privacy and security in the cloud. There will be a rise in cybercrimes impacting people, businesses, and governments if this is hacked, since it exposes users' personal information.

According to Khorshed, Ali and Wasimi (2012) security is the deciding element in whether CC is successful or not. Data location was recognised as a security risk in 2011. Issues related to data security were addressed (Ismail, 2011; King and Raja, 2012). Because it is associated with the credibility of CSP, trust was another area of interest for the researchers. Important issues were establishing the trust model and subsequently working on the trust management process. According to Ryan and Falvey (2012) Trust is crucial in any relationship that involves CC because of the inherent security difficulties and risks. Systems hosted in the cloud are just as vulnerable to data breaches as their on-premises counterparts. Data integrity and the safety of CC were brought up about the virtual machine's security, which was emphasised as crucial (G and S, 2013).

Chen *et al.* (2022) examined the literature on smart IoT CS over the last five years, focusing on studies that examined the use of consumer-oriented IoT clouds. The research analysed the IoT cloud system's security and showcased a new concept for the cloud. Contrarily, Rao and Saraswathi (2021) offer a methodology for examining cloud-

based social networks' privacy and security concerns. Considering both common and uncommon security risks to the cloud is essential when taking a technical look at different types of assaults on CS. In a triangular overview of issues with CC that was published by Puthal *et al.* (2015), this three-part study was directed at investigating contemporary CC security concerns. In addition, the report provided some suggestions as to how these challenges might influence the uptake of CC. Cloud platforms and different intrusion detection and prevention technologies were compared in a previous article by Khan (2016) who conducted yet another comprehensive evaluation of a security issue. In addition, Shahzad, Iqbal and Bokhari (2015) examined the practical implementation of algorithms for processing encrypted queries in a high-throughput cloud environment for a real-time platform. In 2016, after describing several security vulnerabilities, the researchers released "multi-dimensional mean failure cost" (M2FC), a quantitative method for evaluating security risks. To address the security issues that were noticed, they also suggested suitable solutions. While discussing CC and IoT, Rong, Nguyen and Jaatun (2013) addressed issues of CC accountability and security. Modi *et al.* (2013) investigated the causes of CC popularity, how it has been targeted, and how existing and potential solutions could improve security and privacy in the cloud. An exhaustive literature review on cloud security-related topics, including vulnerabilities, threats, attacks, and development on a system to categorise them. More robust data protection is provided by the described privacy strategies in cloud-based systems that are based on IoT (Ahmad *et al.*, 2022).

1.2 Common Risks in Cloud Computing

Although CC has helped with data processing and storage, it has also introduced new dangers. Location of infrastructure, data centres, data integrity, data segregation, and unfamiliarity with relevant rules are all potential sources of risk. Reduced maintenance costs and elastic scalability are anticipated outcomes of resource consumption in a CC

environment. For instance, to fulfil a user's request, the service provider determines which resources will be used for the specific task and when they must be released. The biggest concern of users when they outsource the process to the service provider is security and integrity of their data (Albakri *et al.*, 2014). CC, in which numerous external customers use Internet technologies to access scalable and elastic IT-enabled capabilities, has created marketing confusion as competing IT solution providers rebrand this simple term as "cloud washing," further confusing business executives. Thanks to CC, companies of any size can easily access, on an as-needed basis, a broad variety of enterprise-level IT systems through a pay-as-you-go model (Mell and Grance, 2011). The availability of platform and infrastructure as a service was a crucial premise for building CC-based apps. As a result, new technological developments occurred, which might support other applications. Since IBM Corporation adopted the CC paradigm at the tail end of 2007, a few prominent tech businesses have gradually accepted it. A few examples of these are Google App Engine, Amazon Web Services (AWS), Apple iCloud, Microsoft Azure Services Platform, and AWS (EC2, S3) (Xue and Zhang, 2010). However, the cloud is a threat to data security in various aspects such as authenticity, confidentiality and integrity (Gaikwad, 2007).

The utilisation of CC has skyrocketed in recent years, with major companies like Microsoft and Google making the switch. "CC" does not refer to virtualisation but rather to operating systems, the separation of software, and hardware. The program can now autonomously revert to alternative solutions in the event of a failure, as it can now function independently of the OS and hardware. "Cloud" means "remote data centre" according to Kim *et al.* (2009). The word could mean more than one thing. The ability to access data and information kept on the Internet by means of a web browser is the initial capability. The second is a system that charges for the use of computer resources. The concept of CC is described by the National Institute of Standards and Technology (NIST) as a model for

a shared pool of configurable computing resources that can be accessed by consumers on demand through a network. These resources include servers, networks, applications, storage, and services. The model also includes little to no manual intervention or provider interaction. Furthermore, CC is described by Gartner as an approach to computing that allows for highly scalable information technology (IT) to be made available as services to external clients through the Internet. To paraphrase Kepes's succinct definition, CC is the infrastructural paradigm shift that enables SaaS to flourish. Dillon, Wu and Chang (2010) proposed that customers can acquire functional capabilities on an as-you-go basis through a diverse array of web-based services. Previously, these capabilities were prohibitively expensive and necessitated professional expertise to execute. In addition, CC is defined by Kumar et al. as an online storage system that, instead of using local computers, stores data on remote servers, making it accessible from any Internet-connected device, regardless of location. Virtualisation strategies and automated decision-making are utilised by CC when it comes to virtualising servers and hardware. Virtualisation allows CC users to store and run multiple programs on a shared virtual infrastructure instead of relying on a single program running on a traditional server. Hypervisors enable the use of virtualisation, which in turn enables several applications to operate on a single server. Google Apps, YouTube, Docs, Facebook, Gmail, and Outlook are all examples of cloud services. Internet-based service providing is what CC is all about. The five defining features of CC are self-service on demand, extensive network access, pooling of resources, rapid elasticity, and measurable service. Improving the effectiveness and efficiency of computer systems while simultaneously lowering their associated costs is the goal. 91% of European and American organisations and businesses made the decision to transition to the cloud due to the cost reductions that CC makes feasible (Modi *et al.*, 2013; Ahmed *et al.*, 2017).

To achieve confidence in a security model or architecture and to mitigate risks within it, risk management is one of the supporting processes that must be carried out.

The following are the most essential components of risk management while discussing software development through SDLC:

- Risk Analysis
- Risk Identification
- Risk Abatement

It is possible to break this task down into smaller ones when discussing CC risk management.

Mather, Kumaraswamy, and Latif state that when it comes to cloud architecture, risk management primarily entails two tasks:

- Risk Management
- Risk Monitoring

Afterwards, they resorted to a different method. The following sub-activities can be derived from these two main activities:

There are primarily three things to do when it comes to risk management:

- **Identify** - Consumers has to figure out for themself how much risk he can afford. In the cloud, this is highly dependent on the specific needs of each customer and the kind of data they deal with.
- **Planning** - After evaluating the type of architecture and the significance of the data, a strategy can be formulated, accompanied by the provision of suitable tools and measures to mitigate security risks.
- **Design and Implement** - This is the stage where the strategies and resources proposed during the planning phase are implemented. After they are created,

these security technologies are integrated into the overall architecture. There are primarily two functions that make up risk monitoring, and they are:

- **Testing and Auditing** - Determine whether the tool put into place in the previous phase was successful and reliable by putting it through its paces on the actual platform. To ensure the tool is reliable, audits are conducted thereafter.
- **Maintenance** - This is where the consumer's and CSP's respective roles are laid out. Here are the duties that both consumers and CSPs must fulfil to strengthen cloud security (Security, 2014).

1.3 An Overview of Cyber Crime and Cyber Security

Cybercrime is an unlawful act that utilises technological tools on computers and the Internet to perpetrate an offence such as hacking, identity theft, phishing, ransomware, and data theft affecting individuals, business entities or even a state (Al-Khater *et al.*, 2020). Because the Internet is used more and more, the sophistication and frequency of cyber threats increase and cause significant financial losses, breaches of data and service disruptions (Li and Liu, 2021). Cybersecurity measures such as firewalls, multi-factor authentication, encryption, and so on help to protect systems, networks, and data against intrusion. In addition to preventing cyber threats, cybersecurity also guarantees the secrecy, integrity, and accessibility of digital resources, which are vital for safeguarding our current world's reliance on these resources from emerging cyber dangers (Abrahams *et al.*, 2024).

Similarly, thieves use ICT to carry out many of their activities. Despite the fact that humans employ numerous sophisticated devices, including laptops and cell phones, that operate similarly to machines and alleviate mental tension, this does not imply that they are exclusively advantageous; they also have numerous adverse consequences, including

cybercrime and insecurity (Giri, 2018). Email transmissions, financial transactions utilising automated financial systems, and ensuring communication reliability are examples of significant human activities (Harknett and Stever, 2009). Similarly, Indian chat rooms are experiencing a significant increase in participation, particularly among women and children, with a 50% growth compared to the previous year. There has been an increase in cybercrime in India using social media; for instance, the number of incidents rose from 155 in 2016 to 328 in 2017 (Chang and Xu, 2008). The Internet's pervasiveness has made it an essential component of most people's lives.

Cybercrime refers to any illegal activity that involves a computer, network device, or network itself. Many illegal acts make use of some form of information and communication technology (Grispos, Hanvey and Nuseibeh, 2017). Criminals primarily focus on exploiting security vulnerabilities, causing service unavailability, violating privacy, and initiating harmful physical actions (Parto, 2005). Only those who commit cybercrimes are aware of this occurrence. The sophistication of terrorists, cybercriminals, and hackers is also on the rise.

Techniques are employed under the pretence of security, which are seldom addressed or analysed within the broader security community (Kumar and Panchanatham, 2015). The current generation demands a high level of privacy from contemporary services like e-commerce, CC, mobile computing, and net banking. Positive limits are what people desire to protect their data and their lives. Security and privacy are outcomes of effective data security procedures; with the preservation of data in digital formats in the modern era, the scope of security must be broadened to address cybercrimes.

Reducing these kinds of crimes is a responsibility shared by all. To stop the kinds of incidents that are committed in various nations, particularly India, governments also impose several limitations and enact legislation (Cerezo, Lopez and Patel, 2007). There are

a few open-ended enquiries about online safety: (a) what to do if you have been duped; (b) if you have downloaded dangerous software; (c) if you have sent money to a scammer; (d) if your credit or debit card details have been taken; (e) if your complete identity has been stolen (Mulligan and Schneider, 2011).

Network invasions, virus transmission, and criminals committing crimes like stalking, identity theft, and breaches into private networks are all examples of cybercrimes that have recently increased in frequency and severity, posing a greater threat to people than ever before (Jasim Mohammed, Abdulmohsin AL-dahneem and Hamadi, 2016).

Types of Cyber Crimes

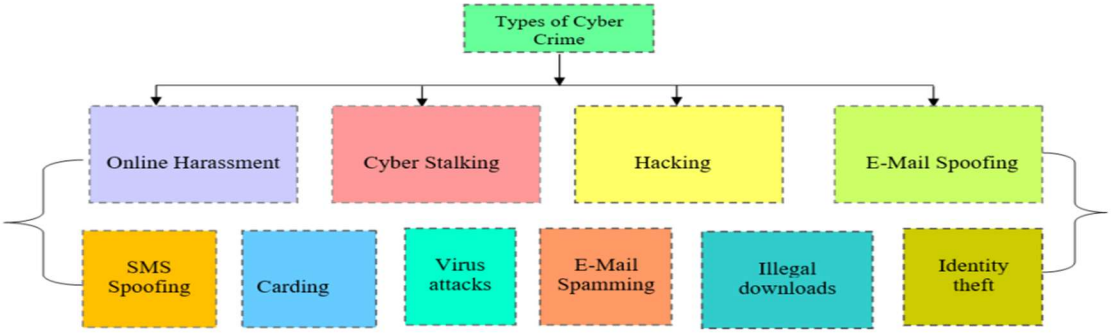

Figure 1.4: Types of Cyber Crime (Source: Tuli, Kumar and Gautam, 2022, p.36-45)

1. **Online Trolling:** Email is used to exchange badgering symbols, marks, typefaces, characters, etc. (R.Sharma, 2012). Social media is used for all of these. A troll in this context is someone who publishes stuff that is offensive on an Internet forum. It also refers to trolling someone online and insulting them directly.
2. **Hacking:** A hacker is someone who gains unauthorised access to a system and steals information from it. Because of a security hole in the computer system, hackers were able to steal users' personal information from social networking sites (Ahlstrom and Bruton, 2001). Fake operator instructions are an example of fraudulent emails frequently circulated among users on social media

platforms. In less than a minute, hundreds of these emails are distributed to hundreds of recipients.

3. **Entails Blocking Unwanted Messages:** Deceptive SMS messages often result in stolen financial information. These calls are designed to exploit individuals by targeting sensitive data such as passwords, bank account details, and OTPs for fraudulent gains (Sreehari *et al.*, 2018).
4. **Carding:** Criminals exploit fees on debit cards and ATMs to take out cash. First, hackers utilise unlawful calls to obtain personal information, creating phoney cards to threaten users using their information (Lubitz, Battle and Eichler, 2025).
5. **Virus Attacks:** To destroy and corrupt personal data, criminals produce malicious viruses and then distribute them to computers. Hackers can do anything they want to other people's accounts. A movie, picture, etc., can be added (Baron *et al.*, 2014).
6. **Email Spamming:** Sending thousands of emails to various users under fictitious circumstances, which might be exploited to steal user information (Cormack, 2006).
7. **Illegal Downloads:** Cybercrime is another term for downloading the newest video games and movies. For instance, hackers create certain programs, like PUBG and Blue Whale Game, with the express purpose of stealing data or making money. Because participants in these games must pay money to buy certain cards, hackers profit from this (Oh *et al.*, 2010).
8. **Identity Theft:** The practice of criminals conducting online transactions utilising victims is known as this crime. Additional victims include schemes that have been taken advantage of by hackers or criminals (Batar, 2021).

1.4 Cloud Security: Theory and Practice

Several technologies we are already familiar with have given rise to CC. These technologies fall under the category of kinds of technologies, such as virtualisation, web services, utility computing, grid computing, www, the Internet, and service-oriented architecture. A new technology called CC has revolutionised the way computers work. The advent of CC has effectively moved all operations online. Because of this, we can build, release, and maintain a cloud-based application without shelling out six figures for software licensing; moreover, we can lower the "total cost of ownership" (TCO) for companies of any size and expedite their "return on investment" (ROI).

NIST's definition of CC will now be the subject of discussion, as they say:

1. **Cloud service models:**

The word ‘CC’ stands for a model which provides on-demand, easy access to a shared pool of configurable compute resources to customers and service providers alike. The resources could be servers, networks, apps, storage, and services. It offers five main components, three different kinds of services, and four different deployment strategies in our availability-focused cloud strategy.

Cloud model features, service models, and deployment models have all been characterised by NIST in the following ways:

- **Software as a Service:** In the cloud, implementations of the "software as a service" (SaaS) give consumers the ability to run programs and applications. The end user usually is not required to understand or care about the underlying infrastructure when utilising an application. Everything administrative is handled invisibly as a service, running in the background of that app.
- **Platform as a Service:** Cloud hosting is typically offered by PaaS providers, who typically bundle software and infrastructure into a programmable

container. Users may then utilise this container to host their applications or services. PaaS is comparable to SaaS, but it encompasses the whole application environment rather than just the software. PaaS providers often bundle infrastructure and software in a programmable container and offer users a cloud to host their applications or services. In contrast to SaaS, PaaS often encompasses the whole application environment, including the development and solution stack, in addition to the computing platform.

- **Infrastructure as a Service:** IaaS clouds provide "storage, database, and guest virtual machines" (OS-ready) as well as other virtualised resources. In a similar vein, tenants engage with "infrastructure as a service" (IaaS) clouds by providing IT with blueprints for their systems. Virtualisation is the same as setting up storage, databases, or servers at a physical location.

2. **Cloud Deployment Model**

- **Public Clouds -NIST defines a public cloud as** A company offering cloud services that owns and makes accessible the underlying infrastructure to users in the public or major industrial groups.
- **Private Clouds - NIST defines it as this:** Organisations are the only ones that run the cloud infrastructure. Operating either on- or off-site, it could be overseen by the company or an outside entity.
- **Community Clouds - NIST defines it as:** "Multiple organisations share the cloud infrastructure and serve a particular community with common problems. This could be hosted either on-premises by the organisations themselves or by an outside company. All of these installations are detailed in the SLAs so that everyone can agree on the conditions of service use. Such a cloud deployment

methodology can greatly assist these organisations in achieving cost reductions and improving their growth.

- **Hybrid Clouds - NIST defines a hybrid cloud as:** The cloud architecture is done by combining two or more separate clouds connected with standardised or proprietary technology so that the data and applications are portable. When we examine what makes CC unique, we find features like resource pooling, on-demand access, user-defined resources, metered pricing, scalability, flexibility, agility, and utility (Security, 2014).

1.5 Overview of Cloud Computing

CC's capacity to offer comprehensive computing capabilities—including data preservation and access to complex programs—on demand and without the requirement for additional hardware or software has propelled it to the status of a major paradigm (Rasheed, 2014). This provides a robust and versatile computing environment; it leverages virtualisation technologies to establish cloud data centres. Several companies are interested in the developed and marketed notion due to the possibility of saving money by not investing as much in software and hardware (Youseff, Butrico and Da Silva, 2008; Armbrust, A. Fox, and R. Griffith, 2009) presented the core concepts of CC, including grid computing, distributed computing, microservice architecture, parallel computing, virtualization, containerization, and "service-oriented architecture" (SOA). They range from relatively recent developments like SOA and Microservice Architecture to more established ones like grid computing and containerization. Some of these technologies have been around for a while, like virtualisation, distributed computing, and parallel computing. CC systems are extremely fluid. They are experiencing constant improvement in both hardware and software aspects. If one believes Heininger (2012), CC's new ICT provisioning approach is characterised by the following terms: self-service, scalable,

service-centric, pervasive, and consumption-based. The concept's qualities serve as its primary definition. According to NIST, CC makes rapid provisioning and releasing Cybersecurity measures such as firewalls, multi-factor authentication, encryption, and so on help to protect systems, networks, and data against intrusion. In addition to preventing cyber threats, cybersecurity also guarantees the secrecy, integrity, and accessibility of digital resources, which are vital for safeguarding our current world's reliance on these resources from emerging cyber dangers (Buyya *et al.*, 2009). In a cloud computing model, users have access to a shared pool of resources that can be expanded or contracted as needed according to the agreements made between service providers and their clients. CC utilises new ideas and technology to maximise the use of both logical and physical resources. The materials are accessible to users as needed because they are services. In contrast to SaaS, which focuses on end users, IaaS and PaaS provide services to third-party providers and independent software developers. Classification schemes for CC should categorise them as either private, hybrid, public, or community, depending on the accessibility they offer (Figure 1.5).

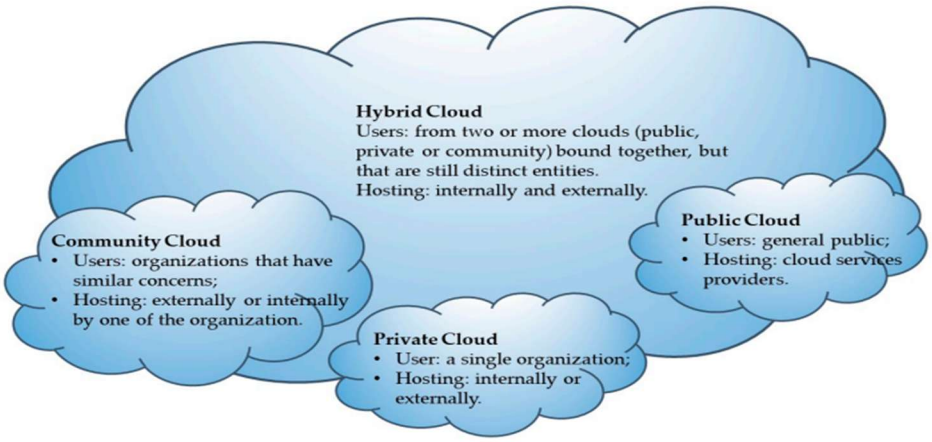

Figure 1.5: Types of Cloud Computing (Source: Radu, 2017, p.295)

A cloud computing data centre is described by Kliazovich, Bouvry and Khan (2012) as a collection of communication and computing resources arranged so that the received

power can be converted into processing or data transfer activities to meet customer requests. This definition relates to the IaaS model's energy efficiency. Additionally, SaaS helps conserve the environment by consolidating data centre operations to utilise less equipment through service sharing and processing centralisation. Companies offering SaaS have a couple of options when it comes to improving software energy efficiency. One option is to use green data centres to host software services with fewer copies. The development of algorithms that adhere to "Service Level Agreements" (SLAs) is an additional objective. In terms of environmental protection investments, cloud providers are better positioned than individual users, both in terms of motivation and resources. Green compilers and scheduling are two things that PaaS providers may offer. When it comes to green CC, SaaS and PaaS providers both have plans and tools to optimise energy use at the software level. Cloud technology's growing popularity was aided by the benefits it provided to both individual users and enterprises. Among these advantages are disaster recovery, flexibility, lower ICT resource costs, improved teamwork within a company, and automated software upgrades. Business owners are drawn to CC because it allows them to easily adjust the amount of resources their organisation has access to in real-time. Reduced equipment requirements, increased energy efficiency, and CO2 emissions all contribute to less electrical waste, which is only one of the many environmental benefits of CC (Liu *et al.*, 2009; Kliazovich, Bouvry and Khan, 2012). Businesses may also have to deal with interoperability issues, data transfer barriers, and a software/hardware design shift when they move to CC (Gai and Li, 2012). Most of the dangers associated with this technology are in the realm of security. Regardless, CC technologies continue to expand due to the numerous advantages they provide to businesses. These advantages include cheap costs, quicker access to HPC resources, and enormous storage capacity. Concerning the impact

on the environment, the following sections outline the primary issues found in both scholarly and non-scholarly research (Radu, 2017).

1.6 Future Trends in Cloud Computing and Cyber Security

Over time, technology has evolved significantly. The Internet now allows people to share and receive data at unprecedented speeds. But there are still worries about data transfer security and the possibility of information breaches. At the moment, the Internet is expanding at a faster rate than most infrastructures. In today's modern environment, many new technologies are changing the way people live (Olomu, Binuyo and Oyebisi, 2023). One thing is certain when looking ahead: technologies will not appear the same as they do now. These new technologies are unable to effectively protect our private information, despite its importance. Despite the implementation of technical safeguards by organisations and individuals, cybercrimes persist on a daily basis. Since the majority of business transactions are now conducted online, this industry demands a high level of security. Because of this, cybersecurity has grown in importance. In order for society to continue to benefit from IT, cybersecurity must be implemented to mitigate risks, hazards, and vulnerabilities. The protection of critical information infrastructures and the bolstering of cybersecurity are essential to the economic security of every nation. Ensuring the security of the Internet has become essential to both government policy and the creation of new services. Fighting cybercrime requires a more thorough and secure strategy. The law must be enforced to investigate and prosecute cybercrime because technical safeguards by themselves are insufficient to prevent any crime. Many countries and governments are currently enforcing stringent cybersecurity regulations (Computing, 2014).

For decades, companies have been preserving and protecting data in an effort to keep their customers' personal information secret. Commercial organisations created CC to meet the needs of individuals and businesses for secure data processing and storage.

According to Mei, Li and Li (2017), CC, or simply computing, is used by numerous businesses across various industries and leverages Internet technologies for cloud storage. The five key elements of CC are quick elasticity, extensive network connectivity, on demand self-service, measurable service and resource pooling (Armbrust *et al.*, 2010) Components of CC primarily include SaaS, Infrastructure as a Service, and Platform as a Service according to Mell and Grance (2011). Community, private, public, and hybrid usage are the four other CC applications. Benefits of CC include reduced IT infrastructure overhead expenses, increased processing power and storage, flexibility and scalability, and less storage space utilisation. Since moving to the cloud has allowed start-ups to reinvest in operations rather than capital expenditures, CC is attractive for cutting IT budgets. The smallest businesses are the ones that use CC the most, whereas medium-sized businesses and businesses with 100 or fewer employees have the lowest rates. Bigger companies have adequate internal processing capabilities. However, there are several disadvantages to CC, such as the requirement for speed, direct resource access, and Internet access (Ashari and Setiawan, 2011). Therefore, it could be very dangerous for organisations to rely solely on CC service providers. Organisations could suffer severe consequences from any interruption in cloud services (Grigoriou, Retana and Rothaermel, 2012).

The service providers get paid by the corporations that utilise CC services. Customised proprietary cloud networks are being developed by large multinational organisations to meet their specific needs. Some very large corporations have found that it is more profitable to construct their own cloud networks rather than use the ones offered by common service providers (Varghese and Buyya, 2018). For example, the wealth of data that Coca-Cola has access to can be used to create a very secure private network that is specifically tailored to its needs. The world's leading computer company, IBM, is working on storage solutions for private clouds. CS will probably be developed by other

global corporations as well. An IT department is present in the vast majority of big businesses. As CSPs develop increasingly complex solutions that can be customised to meet the demands of individual businesses, businesses will be able to outsource their IT departments (Baldini *et al.*, 2017). For example, the wealth of data that Coca-Cola has access to can be used to create a very secure private network that is specifically tailored to its needs. As CC gains popularity and ease of use, private citizens and smaller businesses will follow large corporations in adopting CC. Many companies study data every year. To do analytics, firms need highly advanced computers. CC, however, will soon incorporate that analysis, enabling companies to access analytical data whenever they need it. To address that sporadic requirement, businesses will not need their pricey computers (Baldini *et al.*, 2017). Businesses can use these services only when required, as their costs fall. Consequently, using cloud-based analytics will save costs and risks, which will boost businesses' profitability. (Baldini *et al.*, 2017).

1. **Mobile Cloud-Computing Trend:** The widespread use and rapid development of smartphones necessitate solutions that cater to mobile CC to provide the necessary computational power and apps. Therefore, mobile CC is merely a combination of CC and mobile computing. Mobile computing is made possible by the integration of CC with mobile devices. This enables mobile devices to access cloud storage, memory, and computational power. Mobile CC raises three primary concerns: security, apps, and standard operating procedures. While on the road, the cloud can be used to extend the phone's hardware and the life of the battery. Mobile CC's main issues and challenges are methods, resources, and performance (Akherfi, Gerndt and Harroud, 2018). state that a common architecture is one option to improve the cloud processing and storage-power capacities of mobile devices. Mobile CC is increasingly

being used for social network services, image and video processing, online gaming, and e-commerce in general. Many general polls included mobile CC as a significant topic.

2. **Quantum Computing Trend:** Recently, quantum computing has been one of the most talked-about advancements in CC, which both threatens and has the potential to revolutionise the current model.
3. **Hybrid Cloud Solutions Trend:** It is widely believed that Hybrid Cloud Solutions will soon become the norm in the CC industry, joining other predicted developments. Hybrid cloud solutions are also known to be flexible, inexpensive and meet the market's always-changing needs. Due to heightened rivalry from big businesses, Hybrid Cloud Solutions make it feasible to meet these needs in the market.
4. **Automation Trend:** Increases in cloud adoption force businesses to cope with additional computing, increasing the amount of data and application resources they need to manage. Process Automation will bring a decrease in repetitive tasks, an increase in productivity, and a decrease in errors. So, it is important for businesses of all sizes to try to automate diverse tasks. To make things easier for cloud managers, automation can cut down on expenses and free up time (Taleb and Mohamed, 2020).

1.7 Security Threats in Cloud Computing

CC service dissemination criteria, such as availability, compatibility, and dependability, are a topic of lively community discussion. The security issues associated with CC are distinct from those associated with other models because of the variety of system architectural and service models used. Assuming accountability even when operational duty is shifted to one or more third parties is an essential component of CC,

which is all about gracefully relinquishing control. While there are certainly advantages to using clouds, there are also security issues that must be resolved.

According to Brodkin (2008), Gartner identified seven key security risks linked to CC. Similarly, Catteddu (2010) explored these concerns, providing additional insights into the challenges posed by cloud-based systems. ENISA also identified ten security risk assessments.

Gartner lists seven possible security problems with CC:

1. **Privileged user access:** The "physical, logical and personnel controls" that IT departments implement on internal systems are not applied to outsourced services. There is an inherent risk when sensitive data is processed outside the company. Find out everything you can about the individuals handling your data. It is the customers' right to know how their data is being processed and handled, so that unprivileged users cannot be given access to sensitive information. The providers should be very open about the information, such as details about the process of hiring, oversight of privileged administrators, and controls over their access.
2. **Regulatory compliance:** Data held by a service provider does not absolve the customer of responsibility for its safety and integrity. Traditional service providers have to go through external audits and security certifications. Companies in the cloud unwilling to undergo audits are informing their clients that they may only utilise their services for the most basic duties. It is important for consumers to carefully review the terms and conditions that service providers provide for customer compliance services by their policies.
3. **Data location:** While the consumer or client may not know processes running or data storage locations, the service provider is liable for them and the entire

process. On behalf of their clients, CSP may promise to comply with local privacy regulations if they store and process data in a particular jurisdiction. Clients should follow the rules set out by the service provider and enquire about the company's dedication to protecting client-sensitive information.

4. **Data segregation:** Cloud storage usually stores the data in a shared environment with data of other customers. Encryption works, but it is no magic bullet. The cloud service provider must prove that skilled professionals developed and tested the encryption algorithms. Data can become useless due to encryption mishaps, and even regular encryption can make accessibility more difficult.
5. **Recovery in the case of disaster:** A cloud provider has a responsibility to inform its customers what is in their disaster recovery plan, even if the customers themselves do not know exactly where their data is located. There is a high risk of complete failure for any service that does not use multi-site replication of data and application architecture. If a customer wants to know how long it will take for a provider to restore completely, they should ask.
6. **Investigative support:** Investigating illicit or unethical behaviour should be impossible if it violates CC policy or user service. Cloud services can be studied as especially difficult since host and data centre locations are dynamic and co-location may occur. Unless customers can have a contractual promise from vendors to support specific types of investigations and evidence that these operations have been successful in the past, they may think that examination and discovery requirements will be impossible to complete.
7. **Long-term viability:** In an ideal world, companies that offer CC services would never go bankrupt or be bought up by huge corporations. Nevertheless,

clients need assurance that their data will be accessible even after this happens. Without a doubt, data retrieval is important because it is an important factor for the long-term viability of cloud services. It is essential to find out from prospective suppliers how and in what format clients can retrieve their data. An overview of the ENISA security risk evaluations is provided below: Cloud infrastructures give clients up some of their security for the trust of being able to use the cloud provider's infrastructures. Currently, no standards are in place, making it difficult for clients to switch providers or even bring their data back in-house for IT. This type of risk pertains to the potential breakdown of processes that divide storage, memory, and routing among several tenants. Security flaws in resource isolation schemes make attacks considerably more difficult than in conventional operating systems. Moving to the cloud could jeopardise investments made in compliance or certification efforts, and using a public cloud infrastructure might sometimes make it impossible to achieve certain types of compliance. The client management interfaces of public cloud providers are available over the Internet and are, by nature, public, increasing the security risk associated with them. As a result, the consumer may have difficulty knowing whether the data processing is legal. The lack of transparency on data deletion practices across cloud providers poses a security risk to clients, who may not know how their data is removed.

1.8 Improving Cloud Computing Security:

Businesses and academic institutions established some groups and partnerships to tackle security concerns around CC. Those groups and alliances endeavour to enhance and enhance CC security by promoting best practices for CC security and providing education. Here is a rundown of the many CC security groups.

a) **Cloud Security Alliance (CSA):** This non-profit group works to spread awareness about cloud security best practices. To promote the proper utilisation of CC security solutions, this alliance also provides funding for educational initiatives and awareness campaigns. Furthermore, vigorous research endeavours are strongly encouraged (Csa, 2019).

b) **Open Cloud Consortium (OCC):** CC standards and frameworks to handle interoperability across clouds are both supported by this group. In addition, both the reference implementations and the CC benchmarks are supported. Finally, the consortium supports CC-related events. (Cloud, 2012).

c) **Storage Networking Industry Association (SNIA):** A non-profit organization assists its members in managing and storing substantial amounts of data. This is essential for CC to address storage-related issues, including security challenges (Yoshida, 2017).

d) **The Agency for Network and Information Security in Europe (ENISA):** They are a place to get information security advice and suggestions and a channel for information on what is the best practice for the EU and its Member States. ENISA has some guidelines towards improving the cloud security, and the users of these services should have some assurances that their service providers are following those guidelines (Catteddu and Hogben, 2009). Therefore, we verify the following action items to guarantee the safety of the clients' and vendors' financial transactions.

- Evaluate the potential dangers of using cloud services.
- Various cloud provider offerings should be compared.
- Get guarantees from chosen CSP.
- Cloud providers should have less assurance work to do.

e) **National Institute for Standards and Technology (NIST):** A key part of NIST's mandate is the development of technical standards and guidelines for safe and effective operation of CC. To that end, NIST has proposed cloud security standard roadmaps and catalysts to assist the industry in developing its standards. According to the National Institute of Standards and Technology (2022). NIST also suggests that both public and private sectors use CC. Fungible clouds with the following characteristics are the target of NIST cloud standards:

- Substitution of services amongst each other
- Data and consumer applications can be moved easily.
- Language models, semantics, and common interfaces
- Federated security agencies

Contests among vendors are based on how well their products are put into action. Additionally, vendors compete based on their innovative skills, and sophisticated technology can be enhanced through the development and promotion of value-added services (Oh *et al.*, 2010).

1.9 Cyber Security: Between Challenges and Prospects

Organizations can better prepare for cyber threats to their data and systems if they have a firm grasp of the fundamentals of cybersecurity (Li and Liu, 2021). The primary goal of cyber defence is to prevent data breaches, stealing, or other forms of harm to computer systems. The ability to withstand and recover from harm, whether from natural disasters or hostile forces, is symbolized by this. The interplay of online users, applications, and services, backed by geographically dispersed physical ICT devices and interconnected networks, creates the complex environment known as cyberspace. As previously stated by Kemmerer (2003), the term "cyber security" refers to the measures used to prevent

unauthorized access to computer systems, applications, data, networks, and programs. Information, Internet, network, and information and communication technology security concerns exist; however, they are not fully addressed by present safeguards. It is now critical to manage common cybersecurity risks by bridging gaps between many security domains in Cyberspace and improving communication between organizations and providers (Varadharajan and Suri, 2024). Because different organizations and service providers in Cyberspace concentrate on distinct but equally important security domains, with little to no input from one another, the state of Cyberspace security is disjointed. It seems like every day brings new reports of fraudsters stealing data from other people's devices or launching targeted attacks on websites, databases, or mobile apps. For this reason, cyber defences are receiving more funding and focus in many nations. These days, digitalization and information security permeate every sector of society, from governments to businesses to universities to individuals (Abu-Alhaija, 2020). Consequently, the IT sector now includes the pursuit of cyber security measures and the development of suitable technology.

1.10 Problems Facing Cyber Security

According to recent findings published in official publications, The Australian Cyber Security Centre (2015), attacks on power grids and other critical infrastructure systems are becoming increasingly sophisticated and frequent, both in terms of their physical and cyber components. An appropriate cyber defence system is now essential to protect the important information kept on the system, which is a major obstacle brought about by the expansion of Internet technology. Tech advancements and user demand have led to the expansion of Internet technology, which now provides a plethora of new features and services. Both new service development and government policy now centre on protecting the Internet and its users (Ten, Manimaran and Liu, 2010). Any cyber defence

plan will have holes in it unless all aspects of cybersecurity are well understood. Given the breadth of cybersecurity, all of these factors must be considered in any effective cybersecurity implementation. The main points are illustrated in Figure 1.6.

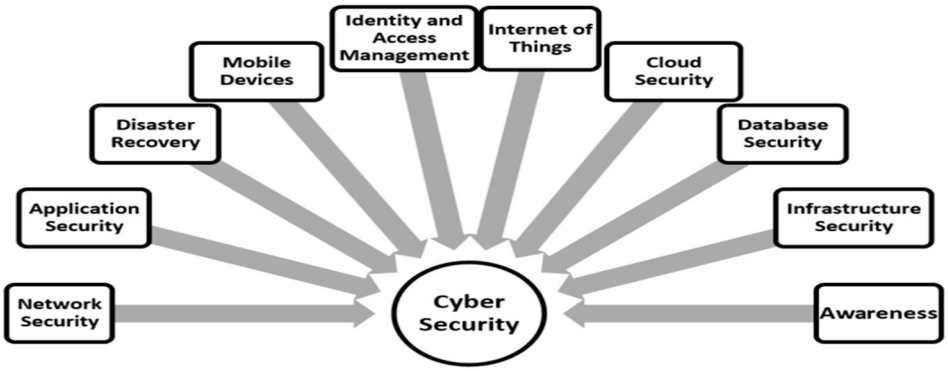

Figure 1.6: The Domain Areas of Cyber Security (Source: Ahmadi, 2021, p.213-230)

Cybersecurity is becoming more accepted as a worldwide issue instead of a technical or computer security problem. The unlawful employment of cyberspace has extensive implications on the economic stability, the security of the people, their health, and the security of a nation. As pointed out by Tariq et al. (2023)Cybersecurity has emerged as a major national policy issue, to which the highest levels of government must be held accountable and responsible. Cyber threats require coordinated action of the community, state and international efforts to respond to such threats backed by holistic policies on cybersecurity. Although technological solutions are relevant in reducing cyber risks, they cannot be relied upon singly. Strong legislative frameworks will be necessary to enable law enforcement agencies to research, charge, and prevent cybercrimes, which will strengthen the overall cybersecurity ecosystem.

Another significant concern in the cybersecurity environment is the security of critical infrastructure. Some of the infrastructure sectors, including healthcare, water supply, transportation, energy, communications, finance, and emergency services, are also pillaring of societal operations, but there are various definitions of critical infrastructure

depending on a particular country (Tyagi and Sreenath, 2021). Although advanced information and communication technologies allow them to achieve operational efficiencies, these infrastructures are becoming vulnerable to natural and manmade threats, especially the sophisticated cyberattacks (Arvidsson, Johansson and Guldåker, 2021). The increased reliance on cyberspace and ICT systems has exacerbated vulnerabilities, particularly in industrial control systems including Supervisory Control and Data Acquisition systems (SCADA) systems, which are part of the configuration of the large-scale industrial networks, including those of electricity and gas distribution (Elhady, El-Bakry and Abou Elfetouh, 2019). Moreover, systemic risk is enhanced by the interdependencies that exist between power, communication and computing systems that intensifies the effect of cyber intrusions (Massoud Amin and Wollenberg, 2005). Although technological developments are expected to resolve available shortcomings, they tend to increase the complexity and thus increase the attack surface and probability of cyber abuse.

The use of mobile devices has also made the cybersecurity efforts in an organisation even more challenging. The act of using unsecured smartphones and laptops to connect to organisational networks by employees subjects them to great risks because even the strongest security controls are compromised by weak endpoints. Also, the fact that public or semi-public Wi-Fi networks are available to clients and vendors exposes the system to threats of unauthorised access. Mobile technologies have become one of the main sources of cybercrime, and a significant percentage of cybercrimes is accomplished via mobile technology, especially in mobile apps and not through standard web browsers (Symantec, 2019). The threats experienced by the users include malware infection, hijacking the device, and theft, particularly where awareness of security is minimal. It is also complicated by the fact that most organisations are not prepared to handle this challenge, with most of them indicating lower levels of confidence regarding the security of mobile

properties than other networked devices (Bishop et al., 2017), which is an essential gap in modern cybersecurity policies.

Identity and Access Management (IAM) is a core component of ensuring the confidentiality, integrity, and availability of the organisational systems and data. The key to reducing internal and external threats is to have effective control over the access of physical space, digital resources, and sensitive information (Teoh et al., 2018). In spite of its significance, IAM projects are often unsuccessful in getting sufficient funding because they are commonly viewed as not directly impactful on functionality or profitability. Yet, in the ever more sophisticated and heterogeneous technological landscape, IAM solutions are necessary to implement access policies and minimize security risks. Identity as a service, physical and logical control of assets, authentication of devices and users, as well as proactive approaches to threats should be included in the list of comprehensive identity management (Bishop et al., 2017). Devoid of solid IAM systems, organisations are susceptible to unauthorised access, compromise of credentials and insider dangers.

Another essential aspect of cybersecurity is application security because the security of systems and data they process in general is highly dependent on the integrity of software applications. Application security deals with the design, development, deployment, testing, and maintenance of software in a manner that maintains security properties of the software lifecycle (Bishop et al., 2017). All applications are not equally vulnerable; vulnerabilities can be as a result of poor requirements analysis, unsafe design decisions, bad configuration, or even patch management. Ethics is involved in all the software lifecycle stages and therefore extensive documentation and open development procedures are highly required. Principles like the least privilege, open design, secure-by-design are important in avoiding vulnerabilities at the design stage (Arce et al., 2014). Additionally, to reveal the implementation deficiencies, both the static and dynamic testing

approaches are required, whereas ethical accountability is related to the vulnerability disclosure and continuous maintenance (Abu-Alhaija, 2020).

1.11 Cloud Computing: Challenges and Opportunities

Early computing infrastructures were both capital and human-labour-intensive, and therefore only large organisations could afford to acquire, maintain, and operate these systems (Narayan, 2022). In the 1980s, personal computers were widely available and inexpensive. This opened up a world of possibilities for businesses and individuals all over the globe. Another change was the rise of PC-based applications developed and distributed by a large pool of talent. As the organisational size grew, mainframe computing gave way to local area networks (LANs) that connected servers and terminal computers within an organisation. Finally, the Internet, which is ubiquitous, transformed the world's personal computers into an extensive network of terminals, software, services, data sharing, and malware of all types (Ahi *et al.*, 2022).

Personal computers are, generally, quite reliable and are fairly easy to use and maintain, yet the users are still expected to run a complex device of which they have little knowledge (Yousefpour *et al.*, 2019). It uses each computer for a small part of the time and deploys its entire computer and software, and hardware capabilities for even less (Gill *et al.*, 2024). Also, sometimes users are solely responsible for the data that is typically stored in the vulnerable media, such as hard drives, compact discs, and flash memory, which all have a high possibility of being stolen, damaged, or lost.

It is in this light that the attractiveness of a public utility model of computing can be seen wherein, it allows users to access computing services and resources without necessarily creating and operating privately run, small scale infrastructures (Nwobodo, 2016). In this model, computing services are provided in a similar way as traditional utility services like electricity, water, and telecommunications services here people use the

services whenever they need them and do not invest in and maintain their own generators, wells, or communication towers. This strategy enables individuals and organisations to enjoy the benefits of scalable and flexible computing capabilities and minimise complexity and capital spending in their operations (Chinazor Prisca Amajuoyi, Luther Kington Nwobodo and Mayokun Daniel Adegbola, 2024).

In a model of a public utility computing, clients usually sign legally binding contracts with service providers, which state service terms, duties, and expectations clearly (A. Ali, 2018). The service provider takes control of such critical functions as payment processing, data access, and data storage thus removing the technical complexity underlying these functions. Also, service providers usually provide service-level guarantees, which describe performance standards, availability, and reliability, which strengthen trust and accountability in the service relationship. Additional cost effectiveness is realized in the form of a pay-as-you-use pricing model, where subscribers pay to use services, depending on their actual usage (Arani *et al.*, 2023). This model not only optimises the utilisation of the resources but also aligns the computing costs with the organisational needs, thereby making it especially desirable in the dynamic and large-scale computing environment like cloud computing.

This mode of operation provides all the typical benefits of public utilities, such as increased server utilisation, economies of scale, capacity, reliability, ease of use, and protection from data loss and damage. Users do not need to be tech-savvy, and there's no need for tech support. The provider staff is highly trained, and the services are unlimited in storage capacity. CC describes this new paradigm (Vaquero *et al.*, 2009; Armbrust *et al.*, 2010; Wang *et al.*, 2010; Rittinghouse and Ransome, 2017).

As with every paradigm shift, there are pros and cons to moving computers to the cloud. Pros include many benefits, but cons include less control and less security (Zhang

et al., 2010; Wooley, 2011; Rittinghouse and Ransome, 2017). The truth is that, when a user (whether it's a man or an organisation) decides to let a service provider take his data, he doesn't do so without risking the availability, secrecy and integrity of his data: A denial-of-service attack or even a simple loss may render the subscriber's data unavailable when it's needed. Junket of subscriber data confidentiality may result if subscriber data confidentiality is accidentally or intentionally revealed to be or accessed by an unauthorised person. Finally, damage or destruction of the subscriber's data can also damage or destroy the integrity of the subscriber's data. There is a greater need for security measures in CC compared to other shared utility models because of the two-way nature of the relationship between providers and subscribers. CC offers two-way communication, which includes transmitting information from subscribers to providers, in contrast to the water and electric infrastructures, which only permit one-way transfers. This arrangement may result in safety concerns. Keep in mind that, albeit on a smaller scale, transferring (vocal) information from subscribers to providers also involves a telephone service, which presents security problems (the possibility of wiretapping).

1.12 A Framework for Secure Clouds

Below is Figure 1.7, which displays the safe CC framework. It has three main parts that make up security, and each of those parts has its own set of troubles with cloud privacy and security. These parts are Requirements for security and privacy: determine the needs for privacy and security in the cloud, including authentication, authorisation, etc., and assaults and threats: issue warnings about various forms of assaults and threats that clouds are susceptible to. Observe the potential dangers and issues with CC. What follows is an in-depth analysis of each rule.

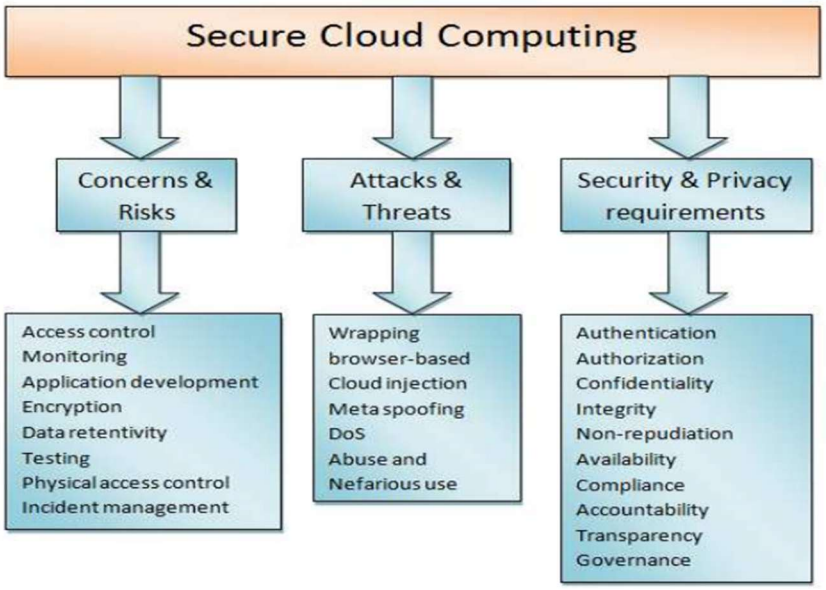

Figure 1.7: Framework for Secure Cloud Computing (Source: Harfoushi and Obiedat, 2018, p.234*)*

1. **Security and privacy requirements**

Information security involves protection of data and records in terms of confidentiality, integrity and availability and it also includes such mechanisms as authentication, authorisation and access control (Kar Yee and Zolkipli, 2021). Besides such technical protection, privacy is the close relationship with information security and implies adherence to various legal, regulatory, and ethical norms. In the context of cloud computing, the privacy frameworks were used to ensure that the cloud deployments comply with the legal standards by implementing the principles of consent, purpose limitation, and legitimacy in processing data. Wider scopes of effective information security management include such aspects as governance, regulatory compliance, and transparency. Based on ISO 7498-2, “International Organization of Standardization” (ISO) has established a list of main information security requirements that were used to offer a systematic basis of ensuring the safety of information system (Ramgovind, Eloff and Smith, 2010).

It is also challenging to control identification and authentication in cloud computing environments, and the primary reason behind such difficulties is that there is a multitenant nature of the cloud architecture. Multitenancy allows multiple users to share the underlying infrastructure and this greatly increases the possibility of rogue users taking advantage of the shared resources and also makes it difficult to identify and verify the users (Wang, 2011). In order to curb these risks, cloud service providers (CSPs) need to apply powerful mechanisms that can authenticate and verify individual users when they access accounts. The conventional authentication procedures like usernames and passwords are still highly applicable in accessing cloud-based browsing services, but they are not sufficient in dealing with contemporary threats to security. Despite the fact that more secure options, like two-factor authentication (2FA) or external authentication factors play an important role in increasing security (Abraham, 2009), they might also cause difficulties in terms of usability and scalability in a large cloud environment. However, the successful authentication is one of the basic conditions of securing the user profiles and avoiding the case of unauthorised access to the cloud resources.

Very similar to authentication, there is the issue of authorisation and access control on the cloud environment. Public and hybrid clouds frequently have many users with different access privileges, and CSPs need to establish and administer access privileges by the account role and service agreements. Governing these privileges such as who is the owner of what and embedding least-privileged access is not that simple, especially in dynamic cloud environments where the identity of the user and workload are meticulously changed on a regular basis (Teneyuca, 2011). Another issue would be in the process of monitoring and controlling the actions of the privileged user like the administrators whose access would be of significant risks in case they abuse it. Some of the actions taken against these challenges by high-profile technology companies include separation of duties,

increased monitoring of privileged accounts and tightening of access to customer data by an administrator to the companies (Teneyuca, 2011). Building trust between customers and CSPs is thus of great essence since the customers have to trust the providers that they will handle access responsibly as well as protecting sensitive information (Mathisen, 2011).

Another fundamental security need in cloud computing is confidentiality as more users and access points are expected to keep increasing. Confidentiality makes sure that the sensitive information can only be received by the authorised individuals, and the aspect is enhanced in public cloud environments by the fact that they are open and shared. Among other factors that endanger the privacy of data in the cloud, there are poor user authentication, multitenancy, data remnancy, and unsafe hosted software applications (Zissis and Lekkas, 2012). Although multitenancy can be effective in enabling efficient use of resources, there is a risk of one tenant to access the data of another tenant in case of an insufficient isolation mechanism. Data remanence also adds to the risks of confidentiality whereby even after a data is deleted, it might still be present in a form that it might leak sensitive information. The probability of data breach is also high due to weak authentication habits and compromised credentials and the collaboration between users and providers in ensuring access credentials is a shared responsibility. Moreover, the internet service providers should make sure that third-party programs that process customer information are of high quality in terms of security measures. The most common methods of ensuring confidentiality would involve encryption algorithms that meet Federal Information Processing Standards (2001) and sophisticated methods of authentication like two-factor authentication.

The integrity plays a vital role in ensuring that the cloud data and software are accurate, consistent, and not distorted within their lifecycle. Protecting integrity is the prevention of unauthorised data and application modification or deletion, falsification, or

misuse of data and applications. Integrity in cloud computing is also defined to include compliance to such concepts as atomicity, consistency, isolation and durability (ACID) and data quality and completeness in all the cloud service models (Robinson *et al.*, 2010); (Youssef and Alageel, 2011). CSPs are in charge of maintaining the integrity of data through control mechanisms that inhibit unauthorised access and check maliciousness. The cryptographic hash functions are greatly applied in order to test the integrity of the data and track the modifications. In addition to data, CSPs also need to deal with underlying hardware and network infrastructure integrity, as frauds at those levels can call the credibility of cloud services in general.

Another essential security requirement in cloud environments is non-repudiation, which ascertains that neither the sender nor the recipient of a transaction can be in a position to refuse having been involved in a given transaction. The ability is critical in accountability, dispute resolution and compliance with the law. Digital signature, timestamps, and confirmation receipt services are among the techniques that are usually used to create non-repudiation in cloud-based transactions and communications (Youssef and Alageel, 2011). Non-repudiation reinforces trust between the users of the cloud and the service provider by providing verifiable evidence of the activities and transactions.

One of the inherent features of cloud computing is availability which is the possibility of authorised users to have access to the software, data and hardware resources whenever necessary. CSPs should also make sure that their services are not affected by cyberattacks, security breach, or even failure of the system. Availability is one of the primary considerations that can determine the service provider of the customers because a long period of downtime may lead to devastating operational and financial effects. There are various strategies of availing high availability including minimisation of service outage and organisational data protection and sound business continuity and disaster recovery

mechanisms (Subashini and Kavitha, 2011). The methods like fault tolerance, data replication, redundancy, and recovery plans which are well defined are very important in ensuring the availability of services. Other security and privacy requirements are availability that have been further elaborated in literature (Robinson *et al.*, 2010; Tripathi and Mishra, 2011).

Auditability and compliance is a major issue of cloud computing as it entails the need to comply with extensive legal, regulatory and contractual demands. Depending on the type of business, people may be obliged to adhere to regulations and standards including SAS 70, ISO 27001, HIPAA and PCI DSS to conduct business and retain the confidence of customers (Teneyuca, 2011). Since cloud information is often shared over internet systems, customers are also obliged to adhere to the encryption provisions and software licensing policies. Nonetheless, CSPs find it especially hard to comply since they might not be in-depth aware of the nature of the information, ownership, or physical location of the data present in their infrastructure. This invisibility renders the delivery of concrete compliance evidence hard to customers. On the same note, customers can hardly understand cloud operations and it is difficult to confirm services are compliant with relevant legal and regulatory requirements (Tripathi and Mishra, 2011). The solution to these problems is to ensure regular internal and external audits and give clear audit reports to resolve them. However, this large amount of cloud data is a reason why the process of auditing and locating audit-relevant data have become more challenging (Wang, 2011).

The trust between the cloud users and the service providers is mainly achieved through transparency. The cloud operations, data handling practices, and security responsibilities should be well communicated to customers so that they can learn how their data is handled, stored and secured. The CSPs should be properly identified, and their roles and responsibilities stated (Robinson *et al.*, 2010). Service Level Agreements (SLAs) are

of primary importance in ensuring transparency as they are the main legally binding documents that are used to describe the service expectations, monitoring and reporting processes, regulatory compliance and security duties. Since cloud data is processed and stored somewhere far off, the customers are usually concerned with the usage of data, its privacy, and the possibility of its misuse. These concerns are further increased by risks that are involved with sharing and virtualisation of resources (Sarathy, Narayan and Mikkilineni, 2010). Therefore, effective governance structures, with clear policies and procedures, would be needed to safeguard cloud environments against security threats, loss, and abuse of data, and responsibly carry out the cloud operations.

1.13 Attacks and Threats

It is important to determine the nature of the attackers and the level of damage that they can cause on the security of the cloud systems before classifying the attacks in the cloud computing environments. The threat actors that commit cloud attacks are diverse and may be motivated by different reasons, expertise, and organisational capacity (Oluremi *et al.*, 2025). On the simplest level, random attackers are the ones who are typical forms of cybercriminals that use simple and easy to obtain tools to scan the internet and possibly find vulnerable systems at random. Such attackers are usually not well skilled and apply methods that are more familiar and which are fairly easy to identify.

Weak attackers are more sophisticated than random attackers, as they are more technically skilled, and will modify tools that are publicly available to attack a particular cloud service provider (Dawood *et al.*, 2023). They are much more targeted in their attacks and are more threatening to cloud environments than opportunistic threats. Powerful attackers, on the other hand, are well-coordinated and highly experienced teams that intentionally attack particular cloud applications or end users (Alani, 2014). These criminals are usually driven by the money motive and work in organised groups of

cybercriminals networks, which allow them to carry out the attacks in an organised and enduring manner. At the top are the substantial attackers, who are highly techno savvy and have concealed interests. These attackers can go undetected by the targeted organisations as well as the law enforcement agencies, and thus they are some of the most dangerous to the cloud infrastructures (Zaid and Garai, 2024).

Another type of classification of cloud attacks is through the models of cloud services and methods used. Wrapping attacks are one of the outstanding categories that use the vulnerabilities of Simple Object Access Protocol (SOAP) messaging. In this kind of attack, predators intercept SOAP messages in between the client browser and the server usually to attack XML signatures that are deployed to authenticate or verify the integrity of transmitted messages. XML Signature Element attack is considered to be one of the most popular examples of such vulnerability (McIntosh and Austel, 2005). Tightly connected to them are browser-based attacks where attackers modify the encryption and signatures of SOAP messages using compromised browsers. These attacks can be done through browser cache, SSL certificate spoofing, and phishing, which compromises browser-level security (Shital and R., 2017).

There are other attack vectors that are prone to Platform as a Service (PaaS) environment. Attacks such as SQL injection, provide attackers with the capability of injecting malicious SQL queries or OS commands, or cross-site scripting into an application (Paul, Sharma and Olukoya, 2024). In others, the attackers seek to install malicious virtual machines or service modules that are falsely considered as legitimate occurrences thus having permission to be executed. These risks are usually addressed using hashing and input validation mechanisms. Metadata spoofing is another PaaS-related threat whereby the web service metadata descriptions are altered to deceive systems or the users.

Such attacks should be checked by verification and validation mechanisms (Thompson and Reynolds, 2022).

Denial of service (DoS) attacks pose a major threat to the availability of the cloud. Such attacks are achieved when an attacker overloads a server by sending excessive requests that overload the CPU and memory resources of the server. Redundancy of the servers to other servers when they are overloaded may occur in cloud environments but distributed denial of service (DDoS) attacks are not easy to deal with in multitenancy where lots of users share the same infrastructure (Sabahi, 2011). The effect is increased in case cloud services are denied to the genuine users. Although a cloud elasticity enables the providers to increase resources to counter such attacks, systematic DDoS attacks are an acute issue (Singh and Gupta, 2022). Other typical attacks are the buffer overflow attacks, where the attackers override legitimate code and execute malicious programs and privilege escalation attacks, which take advantage of the weaknesses in the software to hack into the secured resources without authorisation.

In addition to attack methods, there are also inborn vulnerabilities in the cloud environments. Grobauer, Walloschek and Stöcker (2011) suggest breaking down cloud-specific vulnerabilities into a number of important areas. The vulnerabilities in the basic cloud technologies are the weaknesses in the encryption systems, web applications, and virtualisation platforms including the unsafe cryptographic techniques, web session hijacking, and VME escape. There are other weaknesses due to the nature of core clouds known by the National Institute of Standards and Technology (NIST). Indicatively, elasticity can impose data recovery and it can compromise the network protocol, and self-service on demand can result in unauthorised access to the management interfaces. On the same note, the measured service models can provide a chance of billing evasion (Allioui and Mourdi, 2023).

Other weak points are caused by the domain of poor implementation of the traditional security measures to cloud structures. These are bad key management practices, security metrics that do not consider virtualised environments as well as low network level controls in the virtual networks (Fernandes *et al.*, 2014). Moreover, recent cloud products are usually vulnerable to weak authentication protocols, injection attacks and the absence or improper authorisation checks which make them more susceptible to cyber-attacks.

To address these rising issues, the Cloud Security Alliance (CSA) has launched the first certification programme on secure cloud computing in 2010 at the Black Hat USA Conference. The main aim of this plan was to enhance standardised security practices on the cloud environment (Yogamangal and Sriram, 2012). The provision of cloud computing services through abuse and malicious use is among the key cloud security risks as proposed by the CSA. This is because the cloud registration process is easy, coupled with the low prices and the relative anonymity, such that attackers can use cloud platforms to perform tasks like password cracking, host malicious material, use as points of attack, launch distributed denial of service attacks, and to coordinate botnet command- and-control infrastructure. To counteract these effects, the CSA suggests a better credit card fraud detection, tougher registration and validation as well as a better monitoring of the network traffic.

The other important risk detected by the CSA is associated with insecure interfaces and application programming interfaces (APIs) (Belal and Sundaram, 2022). Cloud APIs and cloud user interfaces are used by cloud users to communicate with cloud resources through cloud service providers. When these interfaces are not designed well or they are not well secured, they can leave cloud environments vulnerable to data manipulations, weak authentication, unauthorised access among other malicious activities. Users must be provided with transparency about the security threats of APIs. Some of the mitigating

measures that have been proposed by CSA include assessing API security models, using strong authentication and encryption controls and familiarity with the dependency structures in API frameworks to minimise the exposure to these threats (ARAVINDA A KUMAR and Divya TL, 2024).

1.14 Research Problem

The adoption of CC comes with a series of advantages, including scalability, flexibility, and cheapness. Nevertheless, it entails various risks to data security, which include leakage, modification and unavailability. The major threats are privacy violations and data leakage, which are the consequences of structured data shared in the cloud being a tempting prey for both internal and external threat actors. Large-scale breaches arise from these risks, which are compounded by insider threats and credential theft; that is, proper access control mechanisms and identity management systems are required. As much as data encryption methods are innately important for data protection, these methods are sometimes rather challenging to implement, and their efficacy is highly reliant on key management. Furthermore, IDSs are used in most organisations to detect malware and prevent data leakage, but various impediments exist when it comes to the timely identification of threats.

When organisations target compliance with the ISO 27001 or NIST framework, as well as the GDPR, additional layers of complexity are introduced as organisations have to adhere to legal obligations when selecting and implementing cloud security practices. However, using different security solutions in an organisation's multi-cloud environment causes interoperability, configuration problems and higher operational costs. This question arises out of the knowledge of how well these solutions integrate to give proper and holistic protection against emerging cyber threats. However, considering the constantly evolving threat landscape, further research should be devoted to investigating the effects of

identified integrated security measures on the security of cloud environments. Issues and challenges involve an analysis of how security objectives of a CC model can be achieved while degrading its performances and economic benefits at the same time. To overcome such challenges, the following objectives are outlined in this study: The study seeks to explore and classify major risks; assess the applicability of particular security measures; and provide an optimal framework for cloud security sustainability.

1.15 Purpose of Research

The objective of this study is to identify and categorise the major cybersecurity risks in CC, assess the efficiency of the data encryption, access control, as well as IDS in minimising these risks, and investigate how integrating security solutions affects cloud security compliance and its overall effectiveness in safeguarding the cloud environments. Particularly, the study has the following sub-objectives:

1. To identify and categorise the primary cybersecurity risks related to cloud computing.
2. To analyse the influence of data encryption on mitigating the risks of unauthorized access and data loss in cloud computing environments.
3. To examine the effectiveness of access control mechanisms in preventing insider threats and credential theft in cloud computing systems.
4. To analyse the role of IDS in detecting and mitigating the risks of malware infections and data exfiltration in cloud environments.
5. To analyse the influence of various security solutions on cloud security compliance.
6. To examine the impact of integrated security solutions on the overall effectiveness of cloud security.

1.16 Significance of the Study

This study has considerable implications for the academic and practical literature as it tackles some pivotal concerns regarding cybersecurity in CC contexts. Since cloud technology is now a regular element in business processes across industries, it is crucial to learn more about the risks connected to it to avoid data leakage, loss of funds, or reputation. Dissecting and categorising these risks will give an understanding of the latest threats and give the organisations specific approaches for mitigation that will protect the cloud-based data from unauthorised access and maintain the three main tenets of data security: confidentiality, integrity, and availability.

The work also adds to the literature by identifying and analysing the effectiveness of data encryption, access control systems, and IDS against unauthorised access, internal threats, lost passwords, viruses and Trojan horses, and data leakage. In addition, it covers issues related to compliance with different types of security frameworks and legislative acts. It provides tips for companies that are challenged with the task of adapting to current legislation and preserving cloud security.

This research will evaluate how such solutions affect cloud security performance and help identify the major trends in developing coherent security strategies. The outcomes of the research will be valuable for IT managers, CSPs, and cybersecurity specialists to understand how to implement security features and prevent risks using CC's unique solutions, versatility, and cost-efficiency. Moreover, the investigation of sustainable cloud security frameworks that the work will pursue will continue to strengthen long-term resistance to these threats to promote the unhampered use of the cloud in the growing context of a highly connected world.

1.17 Research Purpose and Questions

Research Purpose

Thus, the purpose of this study is to synthesise the extant knowledge to understand the security risks in the CC context and review the security measures to eliminate these risks. Several threats have been acknowledged and classified in this research, including: Unauthorised access, Data loss, Data leaks, insider threats, Credential theft, Malware attacks and Data exfiltration.

Specifically, the study aims to assess the operation of data encryption, access control mechanisms and IDS as tools that are instrumental to managing specific risks in protecting data and preventing breaches. In addition, it seeks to evaluate the effectiveness of security solutions in compliance with regulations and standards that govern industries, meaning that compliance is crucial as it fosters trust and prevents organisations from incurring penalties.

Measuring the effects of blending various security tools in a single framework and the consequent effects on the efficiency of cloud security are one of the key purposes of this study. In this way, the study can provide a specific guide for organisations to achieve efficient, deployable and compliant cloud security strategies, enabling them to utilise the benefits of the cloud without sacrificing the security of data or operations.

Research Question

The purpose of this research is to go into depth about these aspects to strengthen the security of CC environments. Specifically, the following questions must be answered:

- **RQ1:** What are the primary cybersecurity risks related to cloud computing, and how can they be categorized?
- **RQ2:** How does data encryption mitigate the risks of unauthorised access and data loss in cloud computing environments?

- **RQ3:** How effective are access control mechanisms in preventing insider threats and credential theft in cloud computing systems?
- **RQ4:** What is the role of Intrusion Detection Systems (IDS) in detecting and mitigating the risks of malware infections and data exfiltration in cloud environments?
- **RQ5:** How do various security solutions influence cloud security compliance?
- **RQ6:** What is the impact of integrated security solutions on the overall effectiveness of cloud security?

CHAPTER II:

REVIEW OF LITERATURE

2.1 Introduction

El Kafhali, El Mir, and Hanini (2022) CC security challenges were explored with a view to the architectural design, threat classification and mitigation strategies to address the growing needs of newly emerging technologies. Several emerging technologies, including smart cities, IoT and 5G Internet, require the ability to handle and store more data. Ultimately, the wide variety of new companies embracing these technologies poses several security concerns for the cloud paradigm. All parts, including users, networks, access control, and infrastructures, are now part of CC. When security teams don't have a clear picture of the cloud's architecture, slow threat detection, they run into data duplication, regulatory compliance challenges, and a lack of control over data access and protection. They expect CC paradigms to lead to quick innovations in meeting computational demands as they become more integrated into digital computer environments and daily life. As the first of its kind, this research serves as an architectural guide to CC, including topics such as core features, service models, deployment strategies, and virtualisation of cloud data centres. The second part is that they give security concerns and frameworks for CC. Their thorough literature review identifies and summarises the many attempts to address these security concerns. Moreover, lastly, they classify all the many kinds of cloud assaults and privacy issues. They conclude by reviewing the security assessment mitigation strategies and protection methods literature. They conclude by outlining some potential future routes and discussing open concerns in cloud security.

Muhammad *et al.* (2021) Security challenges in CC are analyzed and a proposed quantitative risk assessment framework (called "Multi-dimensional Mean Failure Cost" or M^2FC) is proposed to evaluate and mitigate these risks. The idea of delivering virtualised,

scalable resources, software, and hardware to users on demand is a novel one, and it is known as CC. This study introduces a novel approach to the CC model. While it does have some good features, such as provisioning and services on demand, it also has some bad ones. The inadequacy of security measures addressed by CC is a major concern. In this study, researchers will discuss CC security challenges and show how to fix them using a quantitative method for assessing security risks called “Multi-dimensional Mean Failure Cost” (M2FC). They begin by outlining the general concerns with CC security. They offer a basic framework to analyse and assess cloud security issues and suggest solutions to these problems.

Ahmad *et al.* (2022) explored the transformative impact of CC on the industrial sector and the IoT while addressing associated security challenges. With CC, data and resources are spread out over several places and can be accessed from any industrial setting, thanks to its adaptable design. The advent of CC has revolutionised how data, services, and applications are stored, accessed, and used in the industrial sector. Many businesses have moved to CC in the past ten years due to its many advantages, including lower costs, better performance, and wider availability. On top of that, the use of CC has led to notable advancements in IoT. Some security risks were, however, brought to light by the hasty move to the cloud. For cloud-based systems, traditional security methods may not work at all or may not work at all. In the past three years, problems and security issues relating to the development and sequential use of multidimensional cyber weapons have been resolved within the cloud platform. The swift expansion of "deep learning" AI technology brings multiple advantages for industrial cloud security applications. The following are some of the research findings: investigation into the design, setup, services, and security models of IoT systems hosted on the cloud; a comprehensive breakdown of the four key areas of cloud security in the context of the Internet of Things (IoT): data, networks and services,

applications, and security pertaining to individuals; They begin with an overview of the latest developments in cloud-based IoT attacks, then move on to present the limitations from a general, AI, and DL perspective. They then survey the literature for technological challenges, and finally, they highlight the need for future work by identifying significant research gaps in IoT-based cloud infrastructure.

Tabrizchi (2020) investigated the effects and difficulties of CC in contemporary corporate settings, with an emphasis on privacy and security issues. Credit card companies have been in the limelight due to the exponential increase in demand over the past few decades. Businesses can reap many benefits by storing their data in the cloud. Benefits of CC include streamlined IT management and infrastructure, easier data access from nearly anywhere with an Internet connection, and reduced overhead expenses. Further investigation is necessary to fully understand the complexities of cloud security and privacy. Possible answers to these problems have been offered in earlier publications by researchers from academic institutions, businesses, and standards organisations. This survey presents information on cloud security concerns, needs, threats, and vulnerabilities. Furthermore, this work will examine the existing security and privacy problems with the CC systems in particular. In addition, this study presents a new taxonomy for many of the recent security solutions. Furthermore, this study addressed outstanding concerns and suggested future paths while introducing a variety of security risks that endanger CC services. Organisations in the cloud, data owners, including service providers, and end users confront unique security risks, which this research sought to illuminate.

2.2 Identifying and Categorising Cybersecurity Risks in CC

Jagadale *et al.* (2024) comprehensively examined the operational model of CC, focusing on its efficiency, scalability, and transformative impact across multiple industries, such as banking, healthcare, retail, education, and manufacturing. CC lets its users access

company resources from the Internet through private clouds or third-party servers. CC can be described as a self-service, pay-as-you-go, and scalable operational model. Multiple industries, including banking and healthcare, retail services, education and manufacturing, and business operations, are migrating toward the pay-as-you-go model due to its efficient. Through this, users can gain access to storage, servers, networks, apps, and services without really physically being there (Imran, 2014). CC security risks can arise from a lack of control over data, leading to data failures, malicious use of CC, unsecured APIs, rogue insiders, account services, shared technology difficulties/multi-threaded nature, and traffic hijacking. The development of security and the provision of assurance for consumers is an ongoing process that is made possible via several innovative methods, enhancements, and research activities that take place daily. CC is defined, the most pressing security concern in the industry at the moment, research obstacles, CC's significance in key sectors, and the author's predictions for future developments in cloud security are all part of this paper's overview.

Zadeh *et al.* (2023) addressed the growing problem of data breaches by developing and implementing a structured system to evaluate their severity. Data breaches have been a growing problem for a long time, and their frequency is only going up. Therefore, we need a better way to gauge how serious they are. To fill a notable void in the literature on evaluating the severity of breaches, this study offers a method for calculating and categorising cybersecurity threats. The research targets two primary objectives: developing a structured benchmark system to measure breach gravity and implementing it for practical breach investigations. To accomplish these goals, they measure the seriousness of data breaches using a content analysis approach. After that, a powerful decision analytics method called a likelihood impact matrix analysis is used to calculate the risks accurately. A more thorough and nuanced evaluation of the severity of data breaches is produced by

combining these methods. The suggested paradigm is applied to data breaches from organisations included in the Standard & Poor's 500 index. The results show that the most impactful and likely breaches are those involving hacking and the loss or theft of portable media. In light of these findings, the research recommends measures that businesses may take to decrease the likelihood of a data breach. Research findings have important implications for both theoretical and applied cybersecurity risk management.

Kanwal *et al.* (2021) delve into the difficulties associated with CC's security. It delves into the current security strategies, initiatives, and downsides of cloud infrastructure. Among the first companies to leverage CC, Amazon and Alibaba were established in the mid-1990s. Computer science is expanding at a rapid pace. These days, CC is being used by a lot of people. The most advanced computer architecture is seen in CC, which is mostly reliant on the Internet. Concerns about the safety of one's cloud-based platform often arise after its deployment. Since all clouds are web-based, it is not inconceivable to retrieve data from a specific cloud. Security concerns are rising in tandem with CC's popularity. The ability to breach various clouds and get needed data is becoming more common as more people learn about the technology that allows it. Security has become an important focus for many organisations as they provide cloud-based products to their clients. Nevertheless, many security researchers are trying to figure out how to make things safer. Cloud security is always evolving, but hackers will always find a way to breach it. Security in the cloud is becoming an increasingly intricate issue as more and more industries get on the bandwagon of CC.

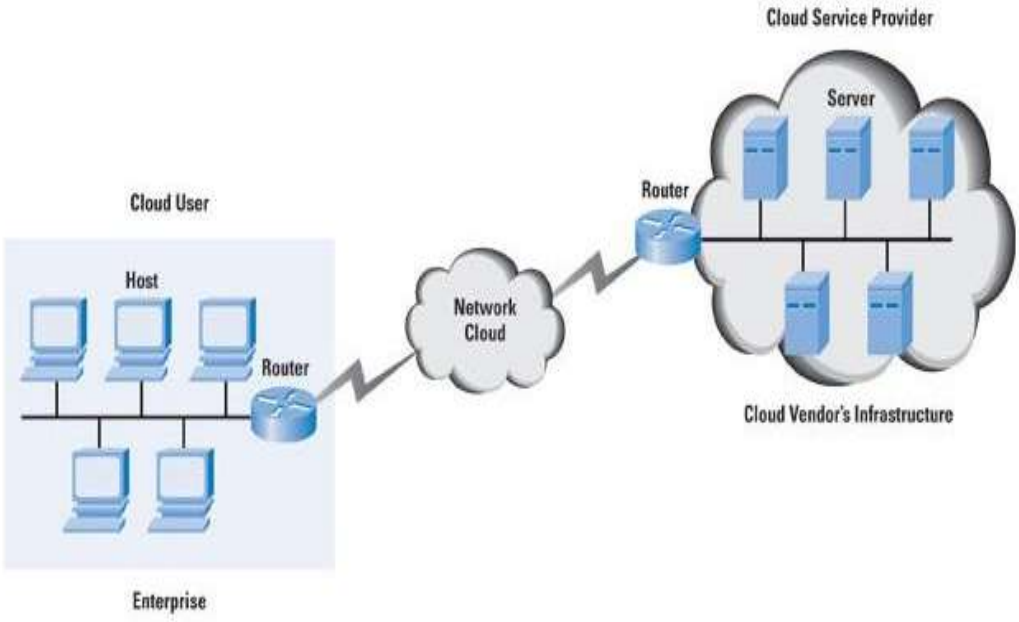

Figure 2.1: Cloud Network Infrastructure Market (Source: Rasal, 2021, p.680-683)

Subramanian and Jeyaraj (2018). An architecture known as CC allows users to use a shared pool of computer resources on demand or pay-per-use. CC provides consumers and organisations with some advantages, including lower operating costs and capital expenditures. Even though CC offers many advantages, several barriers limit its use. Security is an important factor that is constantly taken into account. The computer archetype suffers from the absence of this crucial component, which leads to ethical, economic, and personal suffering. The security issues that cloud organisations encounter were the main topic and investigation of this study. CSPs, data owners, and cloud users are a few examples of these entities. Focusing on CC, which comprises several computational, communication, and service-level agreements. Researching the origins and consequences of different cyberattacks led to the required improvements.

Jathanna and Jagli (2017) explored the evolution and impact of CC (CC) as a transformative resource in the IT landscape. The concept of CC as a resource has transformed the computing environment by drawing in consumers and organisations with

its promises of vast scalability, reduced prices, and enhanced dependability. It enhances the powers of IT. CC has expanded very much in IT over the past few years. With many more corporate and personal data being stored on cloud servers, information security is becoming a rising concern. Many companies, such as Microsoft, considered industry leaders in the software sector, are collaborating to offer cloud services (Mosbah, Soliman and El-Nasr, 2013). Despite the cloud's popularity, clients hesitate to move their operations online. Security concerns are among the main difficulties impeding CC's expansion. It makes data privacy and protection more difficult, which nonetheless has an impact on the market. The danger of data breaches in the cloud environment must be understood by users. The study draws attention to problems with CC.

Rao and Selvamani (2015) analysed the increasing adoption of CC and its technological links to Grid, Utility, and Distributed Computing. CSP like Microsoft Azure, IBM, Amazon, Google's Application and others helps users create apps on the cloud and access them from anywhere. There are services of third parties that offer to store and access data in the cloud. As the data is sent over the internet to a remote server, it must be secure. Security issues should be dealt with first before the CC is implemented. It is about cloud-based system data security problems and how to solve them.

Almaiah *et al.* (2024) conducted an in-depth analysis of cyber risks impacting database management systems, which serve as the backbone of information systems and applications. Database management systems are becoming more important, yet this industry is still vulnerable to cyberattacks. Any information system or application must have a database management system as its foundation. Data loss and extensive damage to the database system are possible outcomes of any cyberattack. As a result, risk management relies heavily on cyber risk classifications and assessments, which set the groundwork for recognizing and countering cyber dangers. By doing a risk assessment, one may better

comprehend the gravity of cyber threats and design effective security measures to lessen their impact. The purpose of this study's cyber risk analysis of database management systems is to classify threats, vulnerabilities, effects, and responses. This aids in the discovery of suitable security controls to decrease the cyber risks linked to each threat category. Furthermore, it aims to discover possible technological solutions to protect database systems from cyber-attacks. To gather, evaluate, and categorize data according to sorts of dangers, weaknesses, and mitigation strategies, this research makes use of the content analysis approach. The biggest technological threat to database systems, as they comprised 9 percent of total incidents, was SQL injection attacks and 'Denial of Service' (DoS) assaults. Other than intrusive attempts and insecure audit trails, assaults against infrastructure and ransomware attacks are second-level technical threats to database systems. Seven percent and five percent of instances, respectively, are caused by these events. In addition, out of all the non-technical dangers to database systems, insider threats accounted for 5% of events, making them the most prevalent. In addition, out of all the technical vulnerabilities in database systems, the most prevalent ones, accounting for 9% of the total, weak audit trails, and unpatched databases, were weak authentication and multiple account usage. Furthermore, 4% of database system vulnerabilities were categorized as second-level security issues, including software defects, poor coding techniques, weak security controls, inadequate encryption procedures, unsecured networks, password abuse, and weak data masking. Organisations can benefit from this work's results by learning about the many cyber risks and creating effective defences against them.

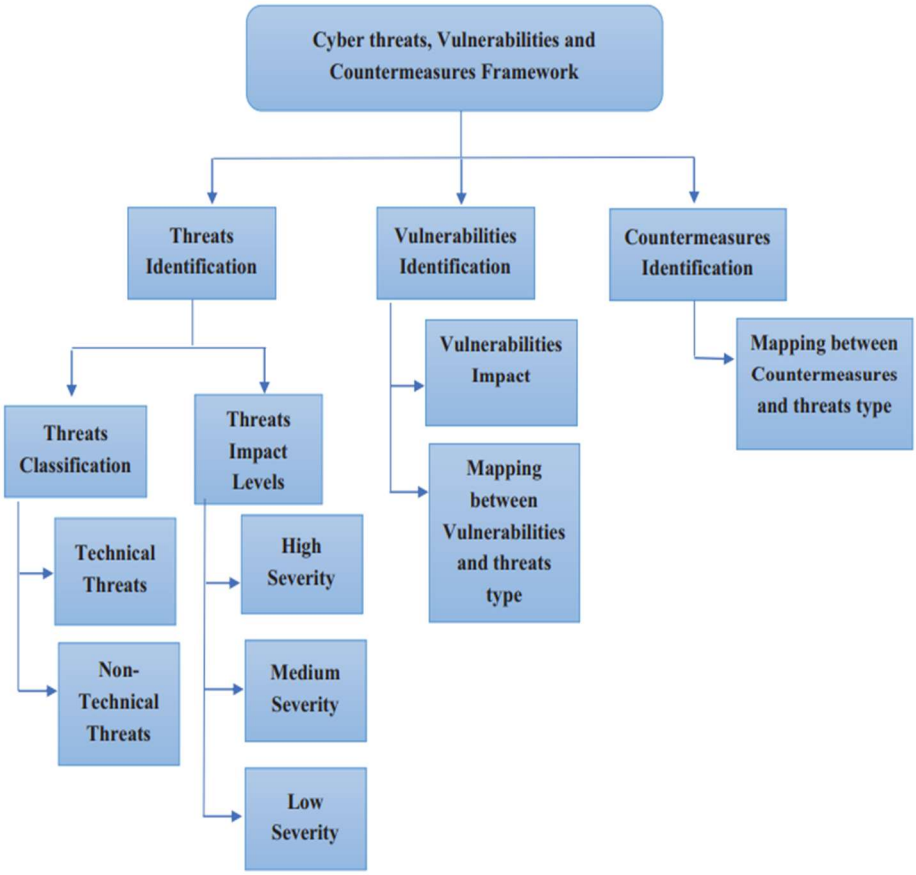

Figure 2.2: Cyber threats, vulnerabilities and countermeasures framework (Source: Almaiah *et al.*, 2024, p.3189–3220*)*

Wilson and Kiy (2014) analyzed the outcomes of successful hacking attempts against commercially marketed cybersecurity protection systems and derived actionable insights for improving security planning practices. The outcomes of successful hacking attempts against cybersecurity protection systems sold commercially and marketed as secure are condensed into ideas that can be used in various guard planning situations. The concepts provide a framework for investigating existing vulnerabilities and evaluating proposed countermeasures to foresee potential security holes; they also explain why trust in such systems was incorrect. The following are some of the proposed concepts: 1) a categorization of security risks; 2) a model of computer systems with five layers; 3) a

paradigm contrasting payloads and defences; and 4) the nine Ds of cybersecurity, a set of comprehensible defensive methods. Motivating improved practices and demonstrating real-world application of principles to forecast future vulnerabilities, an eavesdropping danger is outlined that is inherent in many cell phones and notebook PCs. Furthermore, it is shown that the nine Ds can be used as an analytical tool to rank the anticipated efficacy of some possible countermeasures.

Bhadra (2020) critically examined the transformative role of CC (CC), IoT, and big data in the Fourth Industrial Revolution while addressing the inherent challenges and risks posed by these technologies. CC, IoT, and big data are rapidly transforming the computer domain as the Fourth Industrial Revolution era advances at a continuous pace. Consequently, the scale and complexity of computer jobs and processes are reaching new heights. Even while it provides its stakeholders, including individuals and organizations, with great benefits in today's informational environment of networked society, CC (henceforth referred to as CC) is becoming a maze. With the advent of reliable hardware virtualisation, affordable computers and scalable storage tools, high-capacity network systems, and essential service-oriented architectural frameworks, CC has become a globally recognized and promising domain of technological paradigm. These components are prepared to provide a wide range of services instantly upon demand. However, CC is inherently dialectical, and this study's overarching aim is to make a pitiful effort to construct a critical discourse primarily around the dangers, vulnerabilities, and risks that CC services face from an interdisciplinary cyber-behavioural viewpoint. As a result of these CC difficulties, end-to-end security cannot be achieved, and the transition from a late modern civilization to a risk society is being further reinforced.

Dawood *et al.* (2023) explored CC as an innovative approach for resource sharing, server management, and cost efficiency while addressing its associated security risks. CC

is an innovative approach that allows users to share resources like stock cache and server management. CC transforms large-scale system technical solutions into frameworks for server-to-service communication, which reduces time and money for any organization that uses it. However, CC, like any other technology, introduces new security risks. This study aims to do two main things: (1) define various cloud models and (2) analyse cloud services. New advances in cloud security will be discussed in the section that follows. The next sections will cover security trends, cloud-assisted IoT apps, data breaches, authentication, phishing, key exposure, audits, and inadequate vigilance. Make recommendations for attacks and responses specific to each cloud model based on current security trends and issues. Finally, the study identifies some prospects and consequences regarding cloud model security. As for the future, it was meant to assist academic and business researchers in pursuing CC security.

Dawood *et al.* (2023) comprehensively examined the challenges and opportunities associated with CC, focusing on its growing usage, security flaws, and potential remedies. Among the many useful answers to technological issues, CC stands out. With data security being a top concern, this study seeks to examine CC's security flaws and potential remedies. Scopus, PubMed, Web of Science, and Science Direct were the databases utilised in a systematic review. Following a review of the research's abstracts and titles, the author used inclusion and exclusion criteria to determine whether studies met their high standards for relevance. The next step was to pull out the relevant data by reading the complete texts of the chosen research. Cloud security poses significant difficulties in data availability, integrity, and security, as well as confidentiality of information and network safety. Additional security measures for cloud infrastructure include authentication, data classification, encryption, and APIs. Cloud storage and retrieval could benefit from data encryption to offer secure communication. Furthermore, this research has taken into

account some key difficulties that contribute to the problematic nature of the cloud security engineering paradigm.

Abayomi (2022) analysed the multidomain nature of CC environments and addressed the security, privacy, and trust challenges inherent in such systems. CC environments are multidomain. Each domain utilises unique processes while interacting through different interfaces and semantics and possesses distinct security, privacy, and trust standards. A domain in these systems can represent its standalone service and infrastructure blocks or applications. Service composition and orchestration through service-oriented architectures present a technologically applicable means to build multidomain structures. A comprehensive policy-based management framework for CC environments must use recent studies on secure service composition and integration of policies across domains. The security issues discussed in this study are pertinent to CC and are being recognised and investigated by academic institutions, security organisations, CSPs, and cloud users.

Coppolino *et al.* (2016) analysed the challenges hindering the widespread adoption of CC, particularly focusing on enterprise-sensitive data security concerns, and proposed solutions that can unlock its full potential. Many businesses are caught in cloudy and not-to-cloud limbo, primarily because of worries about enterprise-sensitive data security. Eliminating this obstacle is a crucial prerequisite for maximising CC's amazing potential. This report offers a thorough examination of the primary risks obstructing the widespread adoption of CC and a concise summary of the solutions currently offered by the leading suppliers. The study also outlines cloud security research's (near) prospects by highlighting the most recognised methodologies and major research trends. A selection of the finest proprietary and open-source cloud solutions is used for the study. Thus, the research is a useful resource for IT professionals who want to quickly weigh the pros and cons of innovative technology and better understand the security risks connected with CC.

Reece *et al.* (2023) analysed the security challenges organisations face when utilising multi-cloud environments and provided insights into prioritising mitigations and countermeasures. Integrating data across various cloud-hosted services and systems is becoming more important as more and more organisations move their IT infrastructure to the cloud. Most IT companies are expanding their multi-cloud setups by distributing their workloads among various CSP. The more cloud services and technologies an organisation uses, the more danger vectors and vulnerabilities there are. The biggest issue in protecting a multi-cloud environment from attacks is determining which mitigations and countermeasures to prioritise, especially as the number of attack routes keeps growing. By combining various widely-used risk analysis techniques, they determined which mitigations and countermeasures were most critical by analysing potential threats across multiple clouds. Analysis priorities revealed that authentication and architecture pose the most threat vector risk. With this information at their disposal, IT administrators may allocate funds for cybersecurity in a way that prioritises the most effective defences and mitigations.

2.3 Impact of Data Encryption on Cloud Security

A *et al.* (2023) Encrypted was explored as a key to CC security, especially for protecting sensitive information from unauthorised access. CC security measures that protect sensitive information rely on encryption. The necessity to safeguard private information from unwanted access is growing in importance as more and more businesses move their data and apps to the cloud. Cloud data encryption methods, including symmetric, asymmetric, and homomorphic encryption, are thoroughly examined in this study. The research also examines important management techniques for keeping encryption keys safe and data access secure. Organisations may enhance their cloud data

protection efforts by learning about encryption methods and using strong key management practices. This will help reduce the chances of data breaches and unauthorised access.

Gudimetla (2024) explored CC as a transformative solution to data storage and management challenges driven by the exponential increase in data generated by individuals and organisations. Computing on the cloud is one of the most important factors directly related to technological advancement. The exponential growth in the amount of data generated by individuals and organisations has led to data storage and management challenges. For some time, businesses and IT experts have been searching for a way to store and manage data that is safe, reliable, trustworthy and easy to use and CC has come up as a serious contender. Cloud storage of data helps provide on-demand services and powerful applications, depending on a flexible and secure computing infrastructure of computing resources. Nevertheless, users should ensure their sensitive data is securely encrypted before entrusting it to the cloud. If users want to keep sensitive information safe when storing it in the cloud, they must encrypt it first. Symmetric and asymmetric systems are the two most used forms of data encryption.

Ahmad *et al.* (2022) addressed the challenges associated with auditing shared data in cloud environments, particularly focusing on improving access control and ensuring data integrity. The significance of auditing shared data is rising with the number of people using the cloud. Nevertheless, the handling of certificates is a problem with these methods. The certificate-shared auditing approach falls short regarding handling dynamic data and safeguarding data privacy. Due to security considerations, the verifier cannot view the data content to certify data integrity. An innovative method for strengthening access control and guaranteeing integrity is suggested in this study. To do this, the cloud's storage and retrieval algorithms are augmented using a new mechanism that improves performance. The exponential growth in the amount of data generated by individuals and organisations has

led to data storage and management challenges. For some time, businesses and IT experts have been searching for a way to store and manage data that is safe, reliable, trustworthy and easy to use and CC has come up as a serious contender. Cloud storage of data helps provide on-demand services and powerful applications, depending on a flexible and secure computing infrastructure of computing resources.

Ghosh *et al.* (2023) proposed and evaluated an advanced end-to-end data security solution for CC, addressing the risks of remote data transfer and reception. One of the most exciting new developments in computing, CC is revolutionising computing by bringing it into the service-oriented era. Its pay-as-you-go service model solves the problem of computing infrastructure ownership and management. Security breaches, however, pose a significant risk, particularly in cases when data is transferred from or received by a server that is accessible remotely. Although it employs various encryption methods to guarantee data security, this strategy is somewhat broad and may fail to uphold the security criteria. This work suggests an end-to-end data security solution by implementing hashing, extra padding sequences, randomised salting and encryption techniques used by the sender side to the receiver side. They used a simulated system and mathematical formulations to prove that the suggested strategy works, including various performance measures. In addition, its efficiency was evaluated against state-of-the-art algorithms, revealing that the suggested method generates a thicker ciphertext that is almost uncrackable because of randomisation modules. Encryption and decryption take much longer, but ensuring everything is secure is more important than saving time.

Man *et al.* (2023) developed and evaluated an advanced neural network–based encryption system to address data and information security challenges in cloud storage. Data and information security for users is a relatively new area of study, and recent findings indicate that cloud storage still has security issues. This develops a neural network–based

picture encryption system and investigates the dangers cloud data poses. The original key to the cloud encryption system is hidden using an improved "bidirectional activation" (BA) neural network built from an existing model. The key system's security and randomness are amplified, and a many-to-one mapping association is established between the key and the chaotic initial value. Following this, they present an algorithm for encrypting medical images that uses M-semi tensor product dispersal and dynamic index scrambling. Compared to a conventional method, dynamic index scrambling offers greater adaptability and enhanced efficiency and security. The diffusion approach employs the semi-tensor product operation to resist a selective plaintext attack. Upon decomposing a plaintext image, Schur produces a product matrix that includes a unitary matrix. According to the results of the performance investigation, the encryption algorithm is quite secure.

Qureshi *et al.* (2022) present a graphical overview of workflows of many existing data security and encryption strategies, and critically analyse these methods based on common factors. In the ever-changing realm of technology, CC concepts are quickly gaining traction. Providing consumers with storage and processing resources on demand through a pay-as-you-go model is the primary goal of CC. As a result, even the smallest companies can take advantage of affordable, high-quality infrastructure. However, smart systems face major worries about data privacy and security when transferring data generated to the CC resources managed by a third party. This is because of the cloud resource-sharing attribute. To address data security concerns, numerous encryption methods have been suggested.

Yalla (2021) enhanced financial data security in CC environments by exploring the integration of Attribute-Based Encryption (ABE) with big data analytics. Specifically, it investigates how this combined approach can help banks and financial institutions combat sophisticated cyber threats while ensuring scalability, access control, and regulatory

compliance. Advent of CC, “attribute-based encryption” (ABE), and big data analytics, there is a chance to make financial data more secure today. As the banking industry faces more sophisticated cyber-attacks, proactive measures to safeguard sensitive data are crucial. The study researches how CC systems can integrate ABE with big data analytics to improve financial data security. First, ABE is overviewed, including 'ciphertext policy ABE' (CP-ABE) and 'key policy ABE' (KP-ABE). The second half of the paper describes how ABE allows granular control over who is capable of accessing encrypted data. The study then investigates ABE’s role in CC with regards to scalability and secrecy of data. The discussion also includes how financial institutions can benefit by integrating big data analytics, especially in anomaly detection, predictive analytics, real-time transaction monitoring and security enhancement. Big data analytics is found to be a crucial tool in detecting fraud, managing risks and meeting the need for regulatory requirements, as the study underlines. Case examples showing real-world financial firms' usage of ABE and big data analytics complement the technical descriptions of these tools. Through continuous development and verification of compliance, financial institutions can enhance data security while adhering to legal and ethical constraints. In conclusion, this study provides helpful insights into the potential of ABE, CC, and big data analytics to safeguard bank customers' financial data and lessen the impact of cybercrime in the modern financial markets.

Pureti (2023) provides a comprehensive understanding of encryption as a critical element in modern cybersecurity systems, empowering individuals and organisations to effectively protect sensitive data. Encryption is an essential component of contemporary cybersecurity systems, providing a strong defence against the disclosure or alteration of sensitive data. Intending to equip individuals and organisations to effectively safeguard their data, this study offers a thorough overview of encryption principles, methodologies,

and best practices. Readers will be able to apply encryption solutions that are specific to their security needs after reading this research, which clarifies the key management strategies, basics of encryption algorithms, and protocols. This study simplifies encryption by providing real-world examples and practical insights. It helps stakeholders understand cryptographic protection and improve their cybersecurity.

Blessing (2024) examined with special focus on their importance in CC, with regard to contemporary encryption techniques and key management practices. In CC's ever-changing world, data needs to be protected through a strong encryption protocol and key management. This research is done to know the most recent ways of cloud encryption and important management practices in order to protect sensitive information stored in the cloud. They take a look at symmetric and asymmetric encryption techniques, among others, and talk about how well each one works with various data kinds and cloud applications. More specifically, they examine the effects of critical management issues on security as a whole, including key creation, distribution, storage, and lifecycle management. Insights into attaining a balanced strategy that meets both performance and security issues are provided through current standards, technology, and best practices. The study concludes with recommendations for enhancing cloud encryption and key-management strategies to protect sensitive information against evolving threats while maintaining compliance with regulatory requirements.

Daalen (2023) examined the relationship between encryption technologies and human rights, particularly the rights to privacy and free speech, within the framework of European laws. There are always new proposals to limit encryption technologies, even though they constitute an essential component of today's digital infrastructure. Even in the EU, where their use is already codified in law, legislators demand changes that will affect these technologies. The right to privacy and the right to free speech are two of the most

fundamental human rights at issue here. Despite prior work on the topic, an examination of human rights case law in Europe has not yet provided a solid foundation for the claim that encryption technologies bolster human rights. The present study fills that need by providing a framework for assessing limitations on encryption technology about the rights to privacy and free speech protected by the European Convention on Human Rights and the European Charter of Fundamental Rights. The first part of the study covers the important purpose of encryption technology, which is to limit who can access certain information (also known as secrecy). The second part of the study is a synopsis of various government policies and practices that affect these technologies. Secondly, in this post, we'll take some time to talk about case law surrounding data protection and freedom of expression, privacy, which all encompass the right that governments are allowed or not allowed to have access to protected information and that it also should prevent other people from accessing protected information. Encryption technologies are a key technology to cut the risk of unauthorised access, and therefore, this risk should be at the heart of the evaluation of governance measures in the field of encryption technologies. The study concludes with the recommendation that states thoroughly evaluate this matter before introducing new laws and that courts take unauthorised access of danger as among the central factors that they consider in proportionality and interference determinations.

Ali (2018) analysed and enhanced cloud storage security by exploring key strategies and mechanisms that organisations can use to safeguard their data. Organisations are placing a premium on data security as they move more and more of their storage needs to the cloud. The primary tenets of cloud storage security, including encryption, access controls, and methods to avoid data loss, are examined in this research. Several methods of data encryption, including those employed while data is in transit and at rest, are covered in the paper. The study looks at methods for managing access, including role-based access

controls, which are crucial for preventing unauthorised users from accessing data stored in the cloud. They also look at data loss prevention tactics like recovery plans and backups to make sure that neither malicious nor accidental data loss occurs. By learning and applying these security procedures, businesses can build a solid foundation for their cloud storage, shielding private information from prying eyes and guaranteeing that their data will always be accessible and uncompromised.

Gai *et al.* (2016) addressed privacy concerns in the context of big data usage on the cloud by introducing and evaluating an innovative data encryption method. Privacy issues have arisen as a significant roadblock, even if the use of big data on the cloud is growing at a dizzying rate. Adopting these new technologies has improved application performance and changed service models from numerous angles. But there are also many practical difficulties caused by the exponentially increasing volume of data. Among the major concerns that arise throughout data processing and transmission is the timing of encryption execution. In pursuit of adaptable efficiency, many modern apps forego data encryption, which raises privacy concerns. They present a new method of data encryption called "Dynamic Data Encryption Strategy" (D2ES) and focus on privacy concerns in this article. The goal of the suggested solution is to encrypt data selectively, utilising privacy categorisation techniques while keeping to strict time limits. By employing a selective encryption technique while keeping execution time needs in mind, this approach aims to maximise the extent of privacy protection. Experiments have assessed D2ES's performance, proving the privacy benefit.

Kumar, Chaisiri and Ko (2017) reviewed the data protection measures used worldwide to ensure the utmost data security by reducing risks. Data protection is the focus of this study as it pertains to CC. Cloud data and the safeguards put in place to secure it are the subjects of the investigation. Data availability in the cloud is useful for many apps, but

it also opens data up to apps that could have security issues to begin with. Likewise, data could be in danger when using virtualisation for CC and running an untrusted guest “operating system" (OS) on a hypervisor; this is because the hypervisor has no way of knowing how reliable the guest OS is. The research also uncovered information about DAR and DIT security. The research takes as its starting point the various levels of SaaS, PaaS, and IaaS paradigms.

Lee, Dewi and Wajdi (2018) explored and evaluated data security measures in CC environments, using the Heroku platform as an example of a Platform-as-a-Service (PaaS). A rapidly developing subfield of broader computer and network security concerns the protection of data stored in the cloud. The models of data centres used by third parties are employed by cloud platforms. The cloud platform Heroku is an example of a PaaS. Multiple languages used for web application deployment models are supported. The controlled container system, integrated data services, and strong ecosystem on Heroku make it easy to develop and run state-of-the-art apps. CC addresses data security, an important issue, through the use of cryptographic technologies. Data encryption using the AES is one option. This study details the steps necessary to set up Heroku as a cloud platform, and then how to secure data on Heroku using AES in particular. Evidence from the performance evaluation supports the usage of AES cryptography for data security. Further, the data delay time for encrypting data is proportional to the data size, as shown by the delay calculation of data encryption.

Adee and Mouratidis (2022) address privacy and security challenges in CC by developing an advanced cryptographic and steganographic data security model. Computing in the cloud is a fast-growing industry. With the help of this system, users can have access to data storage and computational power without directly managing them. In this research, the need for a cryptographic and steganographic data security model is to alleviate present

issues of privacy and security of CC data. They reviewed much material on current CC security models to root out the issue and find out what was causing it. Methods from the field of design science are employed in this enquiry. Each step of the design science research process—from defining the problem to gathering requirements to creating the artefact and testing it—is critically evaluated. This artefact was built using Python and design thinking principles. Its functionality is described using tables, algorithms, and histograms. This study's end product is a four-pronged strategy for data security that uses AES, Least Significant Bit steganography, Rivest-Shamir-Adleman, and identity-based encryption. Data protection and security may be achieved through four processes: encryption technologies, steganography, data backup and recovery, and data sharing. Increased data redundancy, efficiency, and security in the cloud benefit the suggested method, which also safeguards data privacy, integrity, and confidentiality from hackers.

Abroshan (2021) the cloud services industry has an important problem in guaranteeing the safety of CC. When dealing with data stored in the cloud—which provides reliable and secure services via shared resources—it is essential to employ a robust encryption solution that does not negatively impact performance. To strengthen CC security while keeping speed to a minimum, this study suggests a cryptographic approach. Due to the critical nature of computing speed in the cloud, a sophisticated cryptography technique is counterproductive. Thus, this method consists of the use of an improved Blowfish algorithm and one based on elliptic curves. They will encrypt the data using Blowfish and the key using elliptic curve approach to provide better security as well as better efficiency. Additionally, data integrity is guaranteed by utilising a digital signature approach. Throughput, execution time, and memory consumption characteristics all see improvements after evaluating the approach.

2.4 Access Control Mechanisms and Insider Threats

Babu and Bhanu (2015) solved and reduced insider attacks that are one of the most critical threats to organisations, especially in CS where vectors and areas of attack are expansive. The greatest threat to organisations is through insider attacks. Insider attacks are not very encouraging to deal with because insiders understand both the system and its inside out. The number of insider attacks is much larger in the cloud because the attacker can execute the attack more easily due to the greater attack vector and scope. An insider attack may be very devastating to the credibility, output of a company and bottom line. Insiders may create accidental or intentional damage. Privilege control is one of the measures that can be used to mitigate insider attacks. Thus, effective privilege management may be used to mitigate the insider risks. To develop a nimbler and scalable defence against insider attacks, this paper suggests a privilege management system, which would combine risk and trust as a part of an access control system to track individuals.

According to Saxena *et al.* (2020) The insider threat poses a significant issue both to the private companies and the government. A better understanding of the insider threat environment and the features of the latter would be beneficial to create mitigation strategies, including non-technical ones. According to this study, public and commercial organisations, especially those that constitute the infrastructure of the necessary infrastructure of a country, have specific challenges in productively detecting and thwarting insider threats. In understanding insider threats and underpinnings of human behaviour and psychological variables, they explore the feasibility of cyber kill chain. The paper will conclude with the identification of research areas in the future, as well as with the unresolved issues related to the insider threat.

Yaseen *et al.* (2017) The request-response paradigm employs policy enforcement point (PEP) and policy decision point (PDP) to control access to cloud services. PEP-side

caching in the model improves the availability of PEP and reduces the overhead in processing PDP. As per this study, insiders are more dangerous to CC since they are able to bypass cloud access restriction mechanisms by utilizing PEP-side caching. The research suggests a workable strategy that can identify and stop insider threats on the PEP side while putting little strain on PEP and PDP performance to address this issue. Extensive testing has shown that the model effectively reduces the risk of insider threats. Finally, the results also show that there is little model overhead in PEP and PDP. It has also shown algorithms, theorems, lemmas for the efficacy and validity of the proposed method.

Duncan, Creese and Goldsmith (2015) Customers may enjoy more agility and deeper savings with CC. Nevertheless, doubts about the safety of private, community, and public clouds are still voiced as possible obstacles to adoption. An evaluation of research goals for present and future network technologies by the European Network and Information Security Agency highlighted trustworthy cloud models as a significant subject for further investigation. More recently, in September 2012, the Carnegie Mellon University computer emergency response team published an article outlining the internal threats to CC and proposing avenues for future research. Not only that, but a 2010 study out of the University of Warwick looked into CC security, namely the possibility of cascading effects. The research included a thorough modelling of the vulnerability and threat landscape, as well as the potential incentives and motivations that could drive attackers. According to one of the findings, the biggest danger may come from inside. This study showcases the advancements achieved in this area of study by exploring the many insider attacks, their consequences, and the harm they can cause.

Hou *et al.* (2020) Intelligent transportation, smart cities, and real-time big data analysis are just a few of the many application areas that have taken advantage of mobile edge computing, which is characterised by position awareness, low latency, mobile

support, decentralisation, and delivery. Researchers and companies alike are very interested in this technology. On the other hand, it introduces new security risks, particularly data security risks during data access, which can cause unauthorised access, modification, or publication of data, jeopardising its confidentiality and integrity. Since access control is a crucial tool for protecting user data when it is accessed, Its use in mobile edge computing became apparent very quickly. However, data security in real-world mobile edge computing applications is lacking in the present access control system owing to issues such as its coarse-grained nature, inflexibility, inability to account for internal threats, etc. This research's data-security-enhanced "Fine-Grained Access Control mechanism" (FGAC) ensures data security in mobile edge computing. The original idea behind FGAC was to have a theory-based, attribute-based, fine-grained trusted user grouping system. Second, a reliable role-based access control mechanism was incorporated into the system to assign users tasks depending on the reliability of their user groups. To accomplish granular data protection, the authentication process evaluates the user's permission to undertake access activities based on matching attributes. According to the experimental results, FGAC successfully detects malevolent users, achieves fine-grained access control, adjusts groups accordingly, and guarantees data security during data access in mobile edge computing.

Aljumah and Ahanger (2020) CC has been recognised as a significant component of computer technology that has emerged alongside the emergence and widespread usage of computers. Although CC has improved users' commercial and personal operations through the use of shared, Internet-connected computer resources, it has also introduced serious security and privacy risks that must be addressed by CC systems. So, this research delves into the many dangers CC faces and lays out ways to protect yourself from them. Because upper-level management is clueless about CC and its security features, a serious

risk of data breaches has been identified. In addition, improper usage of CC services might compromise not only the organisation's sensitive data but also the user's identity and personal details.

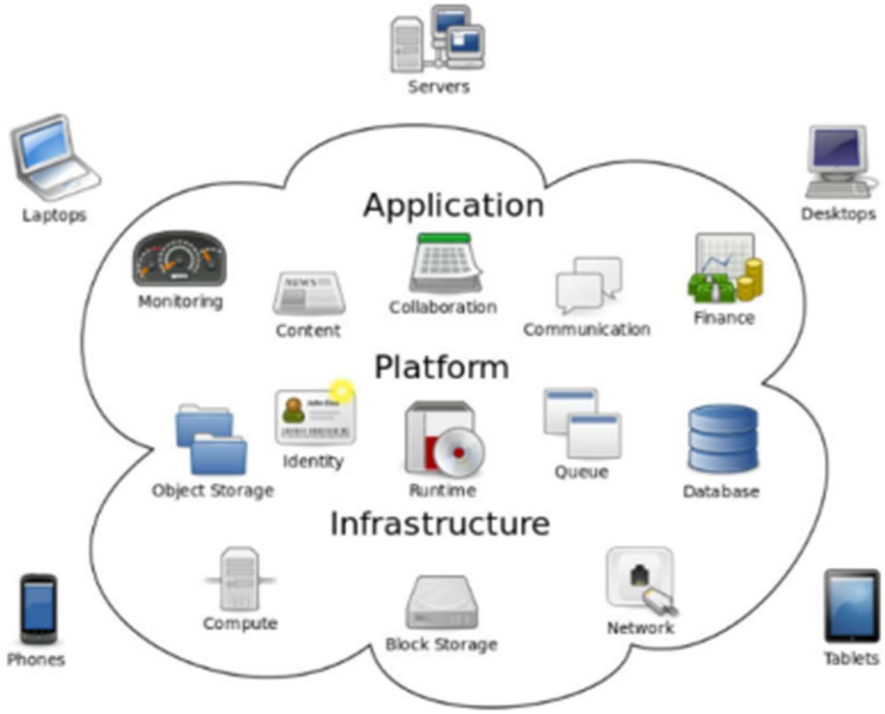

Figure 2.3: Basic cloud structure (Source: Muhammad et al., 2018, p.1-11)

Alhenaki *et al.* (2019) Significant technological advancements have surfaced in the last 10 years, which could make daily activities more convenient for both individuals and businesses. Both the commercial and governmental sectors have come to embrace and make extensive use of CC technology. A growing number of businesses and organizations are moving their operations to the cloud, according to new findings. Nevertheless, CC services are susceptible to various forms of attacks because they depend on an Internet connection, which poses a considerable security risk. Every year, CC improves its security processes, yet security is still an issue. They carried out a survey study on CC for this

report. They discussed various forms of attacks, defence strategies, potential dangers to this new technology, and countermeasures already in place.

Mehraj and Banday (2020), The trust management at CC is complicated and multidimensional. This is inevitable though with the spread of concerns with regard to data breaches, identity theft, data integrity, and secrecy with regards to cloud services. Knowing what "cloud trust" is and how it is established between customers and CSP is crucial, especially in light of the rising profile of CC. Meeting the ever-changing demands of cloud services is a challenge for conventional trust management systems, which are based on static relationships of trust. This research presents a theoretical zero-trust approach for CC. The model provides a theoretical taxonomy of perspectives and tenets for building confidence in cloud services. In addition, the study looked into the difficulties of trust in CC and the significance of trust establishment.

Abdullayeva (2023) Cybersecurity for CC must be guaranteed by its building blocks. The first step in making this technology more secure online is to pinpoint all of the risks it poses. This study recommends creating a new cybersecurity reference model for CS, with different components making up different CC levels. Currently available CC security reference models omit social media considerations and provide insufficient depth regarding the virtualisation and service layers, and the critical components necessary to provide cybersecurity for CC. Cybercriminals' assaults on cloud infrastructure and the general cyber flexibility issues with CC are documented by a layer of IoT sensors. In addition, the essay delves into the cyber dangers offered by different CC service types. To protect CS, the software creates an attack model. This section examines the rules and regulations that pertain to CC's cyber defences. Regarding the safety of CS, they explained the ideas of cyber resilience and cybersecurity in more detail. Building cyber resilience into intelligent CS is an ongoing process. A constructed cyber resilience model

incorporates the information security and cybersecurity aspects of CC to construct an all-encompassing model of cyber resilience in CS, which is an advantage over the existing model.

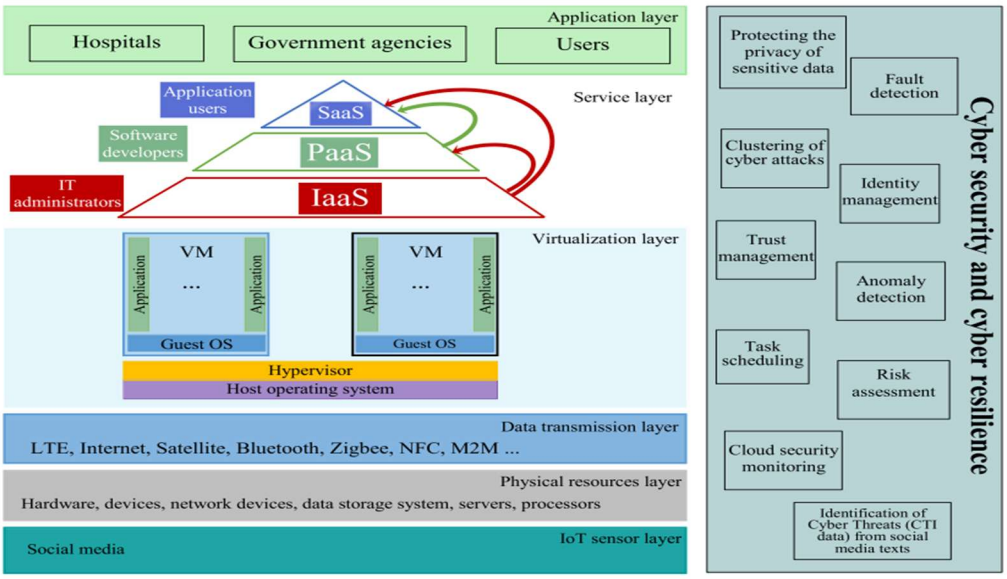

Figure 2.4: The proposed cybersecurity reference model for the Cloud Computing system (Source: Abdullayeva, 2023, p.1-16)

Tissir, El Kafhali and Aboutabit (2021). Emerging on the foundation of distributed computing, CC is a paradigm shift in IT. The term is defined as the utilisation of shared computing resources. CC is vulnerable to assaults, security breaches, and vulnerabilities like any other new technology. Cybersecurity, often known as cyberspace security, is an emerging academic discipline that studies how safeguards influence software, users, and services in their online interactions. Despite extensive study, the criteria for cybersecurity management in CC remain unknown. Examining all aspects of CC, such as security, cybersecurity variations, ISO, and NIST standards, was the primary goal of this study. The purpose of this document is to provide a comprehensive framework for the management and prevention of cyber risks in CC by outlining the standards and procedures provided in the NIST Cybersecurity Framework CSF, ISO 27,032, ISO 27,001, and ISO 27,017.

Furthermore, the study identifies the criteria for evaluating the level of maturity of the organisations that use the framework. The objective is to provide companies with the information they need to either enhance their existing cybersecurity measures or establish new ones for managing cloud-based cybersecurity risks.

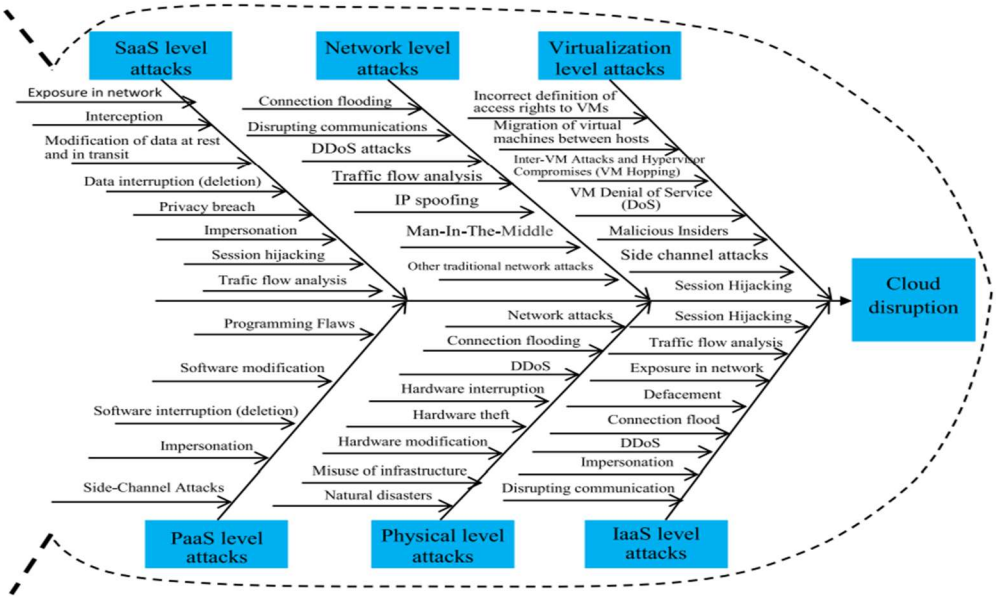

Figure 2.5: Cyber-attack model for cloud system (Source: Abdullayeva, 2023, p.1-16)

El Sibai *et al.* (2020). CC refers to a kind of Internet-based computing in which users request and receive various forms of IT resources. Through the Internet and services provided by CSPs, this technology allows individuals and organizations to gain access to software, data storage, and platforms for creating applications. Concerns about the safety of sensitive information pose a significant challenge to CC. Numerous serious threats to users' data security result from unfettered access to these services and data. Controlling who can access what data and resources and keeping those resources safe is a major problem for CSPs. Cloud reliability and user confidence in this setting depend on this. In this document, we provide a comprehensive list of all the access control mechanisms currently used in CC. The advantages and disadvantages of each of these models are

provided with their respective analyses. On top of that, we evaluate the present control mechanisms considering the cloud requirements that these models have investigated.

2.5 Security Solutions and Cloud Compliance

Priya and Sangeetha (2024)As CC further revolutionises how companies handle data storage, processing, and access, robust security measures must be established. The study analyses the numerous security issues that arise in CC settings and suggests workable ways to reduce these dangers. Key themes covered include network security, compliance and legal concerns, incident response, data privacy and confidentiality, data integrity and encryption, authentication and access control, and new threats. Enterprises can enhance the security posture of their cloud environments using best practices and leading-edge technology and safeguard confidential data. These solutions are useful as evidenced by case studies and real-world experience. Knowing what trends to expect in the future might help you keep ahead of changing security risks. Ultimately, to safeguard private data and preserve confidence in cloud services, a proactive approach to cloud security is necessary. Both industry and academics are concerned about privacy and security problems, which have gained prominence as CC has developed. Several CC privacy security protection solutions are used to further the study on privacy security challenges.

Yimam and Fernandez (2016), CC's adaptability, scalability, low entry cost, universal access, and flexible billing are some of the reasons why customers are migrating their primary activities to the cloud. That being said, there are concerns around privacy, security, and compliance that arise from this. Legal requirements can be heavy on firms, depending on the nature of the services they offer. For example, in the US, public retail firms are obligated to adhere to SOX and PCI, healthcare organisations to HIPAA, and government entities to FISMA. Their assessment of work on compliance concerns is that compliance becomes more difficult than it needs to be as there is no reference design and

relevant patterns. Secondly, they also pay attention to the latest industry trends in terms of compliance approach. After that, they present a summary of compliance concerns and suggestions about the contents of this architecture and related patterns.

Kalaiprasath *et al.* (2017), Cloud services are becoming popular to many businesses. This is done to ensure that user data is secure and safe in the cloud. However, no matter how much you may try to explain to people, cloud security standards are still being developed, and most cloud companies are using a patchwork of privacy and security measures. This leaves cloud customers wondering what kind of security measures the services will use and whether they will be sufficient to address their specific security and compliance requirements. After carefully examining the potential risks that cloud users could face, they have determined the necessary compliance frameworks and security procedures to mitigate such risks. This study provided the basis of their cloud security ontology that presents the controls, threats and compliance related to cloud security. Moreover, they developed an application to categorise security threats faced by the cloud clients into several groups and then identify the top-level security and compliance policy controls to be enabled for each threat. However, the application also indicates which cloud providers conform to certain security rules. Regardless of the technical expertise of the person, the system can be used to create the security standards for themselves and identify providers who follow them.

Odeh *et al.* (2024) investigate into multifaceted domain of data privacy and regulatory compliance within cloud-based IoT systems. It adopts an exploratory method, with stringent analysis, practical studies, and comments of users, in a bid to reveal the complexities and difficulties of ensuring the safety of sensitive data without breaching regulatory frameworks. They give the critical comparison with industry standards and practical implications are addressed to different IoT applications. As noted by the Cyber

Security Market Report Summary, the cyber security market is projected to experience a sharp growth between 2022 and 2027 with a significant Compound Annual Growth Rate (CAGR) of 13.57%. Several key factors are propelling this growth among them being the growing use of mobile technologies, advent of disruptive capabilities of firewall-based deception and greater IT security budgets. It brings out how important it is to do things ethically and legally, and how it is a landscape that is always changing and needs to continue to evolve.

Alrehaili and Mutaha (2020). Among the most hotly contested subjects in today's academic area are CC, its associated security concerns, and solutions. There is still a gap in the accurate mapping of these problems to their corresponding remedies, even though several surveys on cloud security are now common. While some surveys focus on access control techniques and others on virtualisation concerns and solutions, there is a lack of a uniform framework that would broadly define the idea of cloud security and thoroughly examine its unique needs. Additionally, the countermeasures offered in a survey must accurately represent the problem it is addressing. All of these considerations have been taken into account while designing this survey research, which covers the essential topics and appropriately connects them before discussing some unresolved issues in the field.

Barrow and Kumari (2016) CC is unquestionably a way to add significant capabilities or push the boundaries on demand with virtually no investment in new software, new staff training, or new frameworks. Even though the cloud is all the rage these days, businesses are still debating whether it's safe to migrate their operations to the cloud. Security is the only factor causing it. Businesses are reluctant to embrace the cloud and all of its many advantages since no cloud service provider guarantees 100% security to its clients. The advantages of the cloud are limited in the absence of appropriate security measures. This study presents several cloud service models and an assessment of the many

security problems and challenges arising when cloud services are provided. Security concerns unique to the cloud environment's service delivery models (SaaS, IaaS, and PaaS) are the main emphasis of the study. This study also looks at the different security measures being used to guard the cloud from different types of hackers.

Kim and Kim (2017) illustrate how businesses use IT for compliance management and explain the mechanisms behind different types of voluntary compliance practices. It does this at a time when privacy and security concerns are becoming increasingly pressing as a result of the advancements in big data and AI. This study presents a theoretical framework that draws from theories of planned behaviour and IT relatedness. The researchers propose that one's knowledge of compliance and inclination to comply are impacted by their behavioural views about social pressure and compliance. Along with that, they imply that the connection between the two independent variables and compliance intention is moderated by compliance knowledge. A large Korean oil firm, S-OIL, uses a compliance support system, and the authors polled 975 of its workers using a standardised questionnaire. There are two categories of respondents: those who actively use IT and those who do not. Both the active and passive groups of IT users had their compliance intentions influenced by beliefs about and exposure to social pressure, and compliance knowledge mediated the relationship between compliance intentions and compliance action. However, Model 2 (active IT utilisation group) outperforms Model 1 (passive IT utilisation group) in terms of mediation effect, R-squared and importance of each route coefficient. Furthermore, the degree of IT use also moderates the paths between behavioural belief and compliance knowledge and between social pressure and compliance knowledge. Thus, the purpose of this study is to investigate the difference between the aforementioned components and their relationship to knowledge management practice in order to explain

more effective voluntary compliance behaviour. It will focus on knowledge and its supporting systems, such as the compliance support system.

Onumo *et al.* (2021) With the proliferation of cyber threats and the challenges that businesses encounter in securing their IT assets, it is critical to tackle the problem of compliance with organisational security control policies and procedures. Based on organisational theory literature, they develop a multi-theory model, which considers organisational mechanisms, professed cultural values and employee cognitive beliefs, to investigate how organisational mechanisms influence cybersecurity control procedures. This model incorporates the competitive value framework, the technology-organisational theory, as well as the environmental theory. It also draws from the theory of planned behaviour. Researchers in Nigeria analysed survey data gathered from structured questionnaires administered to public sector IT firms using "structural equation modelling" (SEM). They wanted to find out if there was a connection between the various elements that affect security behaviour among employees, such as techno-cultural aspects, socio-organisational mechanisms, and others. The findings indicate that employees' knowledge and perceptions of cybersecurity have an important influence on their intention to follow the organisation's cybersecurity control measures. Moreover, the study also reveals that security technologies moderate the effect of employees' cognitive beliefs and that stated cultural norms mediate the effect of organisational components (leadership) on employees' security behaviour. Consequently, in order to achieve successful cybersecurity compliance, leadership and lawmakers should encourage organisational security steps that incorporate cybersecurity into the daily work of everyone.

Vitunskaite *et al.* (2019) Some advantages meant to transform people's lives have been brought about by smart cities. Among these are, but not limited to, lessening environmental impact, cutting costs, and improving economic efficiency. But the concept

of a "smart city" is far from mature. It leaves itself vulnerable to cybercriminals and attackers, which can do substantial damage, because it is technologically dependent. High degrees of interconnection, social and political complexity, and competing interests of many stakeholders make smart city security a challenging social and organisational issue. Their existence demonstrates that the functions and duties of many stakeholders remain vaguely defined in the existing standards and guidelines. Nobody is on the same page when it comes to the most important security standards. This study examined the cybersecurity measures of smart cities, paying special attention to the legislative framework and technological requirements. Within its pages are ninety-three pieces of security advice and guidelines. Next, it compared the smart cities of Barcelona, Singapore, and London in terms of their technological standards, third-party administration, security measures, and governance frameworks. This study used the case study to provide a framework that would guarantee security at every level of smart cities. The framework would include technological standards, input from governance, regulations, and compliance assurance.

Ngozi Samuel Uzougbo and Adewusi (2024) As cyberattacks grow in both frequency and sophistication, cybersecurity becomes an increasingly pressing issue for financial institutions throughout the globe. This research is intended to compare and contrast different international regulations and rules that financial institutions ought to observe for cybersecurity compliance. This research finds similar regulatory frameworks in the cybersecurity compliance of essential jurisdictions such as the US, the EU, and the Asia-Pacific countries to identify similarities, variances, and best practices. The paper begins by giving an overview of the current situation of cybersecurity laws on financial institutions with a focus on highlighting the main objectives and the guiding principles of the laws. Then, it discusses data protection, incident response, and risk management and legislative structures of different places. The paper will examine the current legislation of

cybersecurity that exists and give recommendations on how compliance and resilience can be enhanced through the examination of the specific rules and regulations that each jurisdiction has implemented. The primary conclusion made in the study is that, with the integration of the financial sector and the need to have coherent regulatory response, global standards of cybersecurity are getting perched nearer to each other. This is due to a growing realization that worldwide cooperation and information sharing is required to effectively counter cyber threats even when dissimilarity in legal frameworks, particularly in data security and data breach reporting still exist. The report lists financial institutions that are faced with a number of challenges, including a resource shortage, burdensome regulatory standards, and dynamic cyber threats. To address these difficulties, it is crucial to employ strong cybersecurity solutions, including encryption, multi-factor authentication, and frequent security audits. Last but not least, the worldwide scene of cybersecurity compliance in banks is better understood after reading this comparison study. This study aims to help financial institutions, regulators, and lawmakers improve cybersecurity and deal with the ever-changing cyber threat landscape by identifying common patterns and best practices.

Djebbar and Nordström (2023) Cybersecurity standards offer a methodical framework for handling and evaluating cybersecurity threats. There is no better resource for security standards and controls than these for organisations looking to lessen the chances and consequences of cyberattacks. However, picking the correct security standards for a given system is difficult due to the abundance of cybersecurity frameworks and standards available. The selection procedure is already challenging without having to account for the lack of total comparative overlap across various criteria. When new security standards are required by business demands, there is a chance that existing security requirements and controls may be duplicated, leading to more effort and expensive

compliance fees. Optimising the effectiveness and financial benefits of standard compliance efforts requires a thorough analysis of cybersecurity standards and the identification of any overlapping security controls and criteria. This study compared three security standards: ISO/IEC 27001:2022 for management systems protecting sensitive data, ISA/IEC 62443-3-3:2019 for industrial control and automation systems, and ETSI EN 303 645 v2.1.1 for consumer devices connected to the Internet. The standards were laboriously selected because of their potential for widespread use and approval across the world. They purposefully chose standards with diverse foci to show that standards may have substantial similarities while being developed for distinct contexts. The goal is to improve the clarity and simplicity of the compliance process while assisting organisations in choosing the best security measures for their unique requirements. A close examination of the results reveals that the chosen three criteria overlap considerably. By getting a thorough grasp of common security needs and controls, companies may simplify their compliance efforts and eliminate redundant labour, which is particularly helpful when fulfilling the criteria of various standards.

2.6 Integrated Security Solutions and Cloud Security Effectiveness

Ali, Khan and Vasilakos (2015) It is possible to provide powerful, elastic, easily managed, and inexpensive resources over the Internet with CC. CC's ability to maximise the utilisation of the hardware resources by allowing the hardware resources to be used optimally and in a shared manner. The characteristics mentioned before are enticing companies and individuals to move apps and services to the cloud. Power plants and distribution centres are also being moved to the cloud. This also comes with a couple more security risks when utilising services offered by third-party cloud providers. Security issues arise when moving user assets (data, programs, etc.) out of the control of the administrative area in a shared environment where there are many users working around the user. This

analysis delves into the many security concerns that stem from CC's fundamental functionality. In addition, the study highlights the most up-to-date approaches to addressing security concerns in the book. The study also provides a high-level overview of the security holes in mobile CC. The concluding section also covers open questions and potential avenues for further study.

Segun-Falade *et al.* (2024) With the introduction of CC, desktop and mobile operating systems have changed the sea level, allowing unprecedented efficiency, functionality, and user experience to be reached. This gets into the importance of cloud mixing in various OSes and its implications on developers and final users. The incorporation of CC enables mobile and desktop operating systems to have more computational power, scalability of storage capabilities, and easy to synchronise data. Mobile system is highly compatible with cloud services because the customers can use the data and applications they have anywhere and, on any platform, hence making it a reliable experience. Besides simplifying personal data management, this synchronisation option will allow developers to create more active and vibrant applications, relying on the cloud infrastructure to provide real-time updates and performance improvements. Through cloud integration user desktop systems can store large volumes of data and execute programs with high resource demands without overloading their local hardware. Cloud-based virtual machines and application delivery services have enabled users to execute high-performance applications on less powerful machines. This increases the number of opportunities regarding advanced desktop applications being available and usable. The integration into the cloud also facilitates the use of shared workspaces and collaborative tools, which increase productivity and make users collaborate and work in real time. The considerations of cloud integration are security, data privacy, and system performance. There are other security provisions necessary to protect the sensitive information when

using cloud-based systems like strong encryption of information and secure authentication procedures. Also, consumers with spotty or non-existent network coverage may have trouble using cloud services due to their dependence on Internet connectivity. Finally, modernising desktop and mobile OSes through cloud connectivity is essential for better data accessibility, application speed, and user experience. There will be more chances for creativity and solutions to new security and connectivity problems as cloud technologies develop more, and their impact on operating systems will grow. More adaptable, efficient, and networked computer systems are the result of this continuous integration.

Sarker *et al.* (2023) The IoT is a highly popular technology that influences people's daily lives, from social to commercial to economic. The current and future IoT technologies show enormous potential for enhancing the standard of living for all people by automating processes, increasing productivity, and making consumers' lives easier in many different domains, from smart cities to education. Nevertheless, smart applications in the IoT context are significantly impacted by cyber-attacks and threats. Compared to the new security risks and assaults, the old methods of protecting IoT are woefully inadequate. Applying AI abilities, especially ML and DL solutions, is crucial to developing a secure infrastructure for the future generation of the IoT. With the use of ML and DL, this study describes in-depth IoT security intelligence, a system that can autonomously protect IoT devices from cyberattacks by analysing raw data. Lastly, they review the study's findings and point out related research questions and potential avenues for further investigation. From a purely technical standpoint, this study intends to serve as a reference and road map for cybersecurity experts and academics working on projects involving the IoT.

Suwandi (2022) Data security in the cloud is the subject of this research. This research looks at cloud data and how it relates to security. To guarantee optimal data

protection by lowering risks and dangers, the research looked in-depth into depth on data protection methods and approaches utilised worldwide. Data availability on the cloud is great for many apps, but it also exposes data to apps that could have security flaws. In a similar vein, data might be in danger while using virtualisation for CC and running an untrusted guest “operating system” (OS) on a hypervisor. The research also sheds light on DAR and DIT security considerations. A comprehensive understanding of SaaS, PaaS, and IaaS forms the basis of the research.

Recently, Bagherzadeh *et al.* (2020) There has been much focus on the widespread use of smart grids and power markets as part of the effort to update the electrical infrastructure in industrialised nations. As a result of the meteoric rise in the development of communications technology and, more specifically, AI, power systems are undergoing a period of rapid transformation as they join the digital age. In recent times, the unique characteristics of the IoT have supported the widespread implementation of this innovative idea in the frameworks of several technological domains. For many reasons, including energy, several researchers have detailed the hierarchical paradigms and architectural details of implementing this novel idea. Using this technology can improve conventional energy management methods in power markets and smart grids. The IoT will make old ways of managing energy inefficient. Instead, grids that have been upgraded with IoT will show off a decentralised, peer-to-peer structure with much autonomy. It is suggested that to accomplish the desired goal, CC and IoT should be combined. In addition to presenting new obstacles, this connection, known as Cloud IoT, displays great benefits that align with smart grids' goals. Before anything else, the existing study presents an extensive explanation of Cloud IoT. The next step is thoroughly examining the possibilities, current obstacles, and potential remedies.

Zarichuk (2024) The usage of CC is rapidly expanding and is already an integral part of many data storage and processing infrastructures. Because there are threats to the security and integrity of user data, it is imperative to identify the best practices for cloud data protection. Finding ways to ensure that cloud environments and current apps are secure and private was the main goal of the research. Other papers on the subject employed the analytical technique, but actual implementation relied on the experimental method. Creating a security monitoring program is one of the primary outcomes of the research. The number of unsuccessful login attempts is one indicator of the presence or absence of suspicious behaviour, which is determined by analysing event logs. The console displays all the essential information after checking access to resources. To better understand the pros and downsides of various cloud platforms about data privacy and security, the author has put up a comparison chart. It details the requirements for providing services to the chosen services. The author builds a block diagram of potential approaches to better understand the interdependencies among the many facets of cloud security. It includes data encryption parameters and tactics, and information on how to defend against assaults and safeguard sensitive data. Some security and privacy-related procedures reviewed regarding CC include intrusion detection, authorisation, legal requirements, interaction with modern apps, user identification and authentication, monitoring and logging, and more. The research has real-world relevance because it may inspire new approaches to bolstering CC privacy and security. Developers and administrators in the cloud were able to employ them to successfully safeguard user data and guarantee privacy in contemporary apps.

Gill *et al.* (2022) The field of autonomous computing studies how machines may autonomously accomplish "control" actions defined by users without the need for direct human input. The principles of autonomic computing for both closed- and open-loop systems have been greatly impacted by those of control theory. Complex systems often

have multiple control loops that operate simultaneously and are dependent on each other. One fundamental problem with computer resource management is the paucity of research into integrating AI and ML to enhance resource autonomy and performance on a large scale. This is always the case from a single web server to numerous resources in a data centre. By combining AI with ML, it is possible to achieve varying levels of granularity in automating systems, from fully autonomous to human-in-the-loop.

Ullah *et al.* (2023) A relatively new technology, CC is a system that runs the network's software and hardware applications over the Internet. Using the principle "you pay as you go on," CC makes these services available. One emerging technology that is making waves in the telecom industry is IoT. We should expect better cities, smarter homes, and more convenient lives as a result of IoT gadgets' mission to link everything in our environment to the web. Rapid advancements in both CC and IoT are made possible by their combination. This researcher provides an overview of IoT and CC, concentrating on their respective security concerns. This exemplifies how IoT benefits from CC. Finally, it discusses the problems with CC and IoT in terms of security.

CHAPTER III:

METHODOLOGY

3.1 Overview of the Research Problem

CC is extolled for such advantages as scalability, flexibility, and cost advantages, but it has also been seen to bring in risks to cybersecurity. It would be impossible to devise strategies for controlling these risks without first categorising them. Security breaches and data leakage are some of the most critical challenges identified; thus, the possibility of using data encryption as a solution is discussed. Moreover, there is a diverse threat from insiders and credential theft. Hence, it is pertinent to assess access control solutions. The performance of IDS in preventing and finding malware and information leakage also deserves analysis. Adherence to conformity relating to security is another significant factor, which depends on different security measures. In addition, recognising the influence of integrated security solutions on the total effectiveness of cloud security is crucial for complex protection.

3.2 Operationalisation of Theoretical Constructs

The manoeuvre of variable operationalisation was done by employing emerging operational definitions and concrete research instruments for initial theoretical constructs of cybersecurity available in the literature. Specific survey questions were mapped to measures like Data Encryption, Data Loss, Unauthorised Access, Insider Threats, Credential Theft, IDS, compliance and effectiveness of cloud security, which were then rated on a Likert scale from 1 (SD) to 5 (SA).

For example, the construct of Data Loss was measured by items as the presence of effective prevention measures, awareness of data backup procedures, frequency of testing those systems, and participation in any data loss situations. Likewise, Credential Theft was measured using questions on measures put in place on security, user awareness on how to

protect credentials, more complex forms of authentication used and guidelines on handling credential theft.

Concerns like Cloud Security Compliance were then realised based on an assimilation of cloud security compliance to benchmarks, permitted user appropriateness, reformation security review, vulnerability review and data encryption policies. Further, organisational cloud security effectiveness translates to Cloud Security Effectiveness as another translation to measures such as conformity with best practice guidelines, anticipatory posture of cloud security, responsibility and management of data confidentiality and data integrity.

This approach ensured that all the abstract concepts were counted for statistical analyses, demonstrating the connection and efficiency of different security measures, as recommended in operationalization frameworks. They are the measurable variables on which the study was founded, allowing for an association of the patterns and the possibility of drawing more conclusions.

3.3 Research Purpose and Questions

In order to strengthen the security of CC environments, our research will analyse these topics in depth. To be more precise, the study requires answers to the following study questions:

- **RQ1:** What are the primary cybersecurity risks related to cloud computing, and how can they be categorized?
- **RQ2:** How does data encryption mitigate the risks of unauthorized access and data loss in cloud computing environments?
- **RQ3:** How effective are access control mechanisms in preventing insider threats and credential theft in cloud computing systems?

- **RQ4:** What is the role of Intrusion Detection Systems (IDS) in detecting and mitigating the risks of malware infections and data exfiltration in cloud environments?
- **RQ5:** How do various security solutions influence cloud security compliance?
- **RQ6:** What is the impact of integrated security solutions on the overall effectiveness of cloud security?

3.4 Research Design

In this study, a quantitative research design was used. The researcher used Pearson's Correlation to look at survey findings to identify statistically significant relationships or differences between employee risk level and the efficacy of an AI-based security awareness training program (Ansari, 2022). Qualitative research was used for the study; whereby structured questionnaires were administered among IT specialists and organizations engaged in CC. The instrument used had Likert scale questions about perceived risks, the frequency of attacks and the level of security measures taken. In analysing correlations between the types of risks identified and the applied solutions, basic descriptive statistics were applied in combination with a regression test. The study complied with ethical standards of anonymity and data confidentiality as postulated (Eungoo and Hwang, 2023).

3.5 Population and Sample

The report investigated CC's biggest cybersecurity threats and how to mitigate them. The poll targeted cybersecurity, cloud, and IT professionals. Convenience sampling, a typical nonprobability method for gathering data from available and interested participants, made the study more practicable. This method has been utilised for research in organisations that lack time for random sampling (Etikan, 2016) and other reasons. Convenience sampling may lack generality, but cloud security managers were recruited.

The statistical equation recommended 300 respondents, which is why this figure was used as the assumption of having a large enough sample to help the researcher to obtain sufficient power to identify significant trends and relationships (Algarni *et al.*, 2021). This was chosen to provide sufficient depth and coverage of a subject area without making collection and analysis so cumbersome. Similar sample sizes have been used in related studies on security in CC to reason regarding the risks and measures to eliminate them (Algarni *et al.*, 2021). It would be relevant to mention that participants provided valuable information on compliance, breach of data, and threats prevention and prevention in a cloud setting.

3.6 Participant Selection

Category	Inclusion Criteria	Exclusion Criteria
Profession	IT professionals, CSP, and cybersecurity experts are actively working in the field.	Individuals without direct experience or expertise in CC or cybersecurity.
Experience	Minimum of two years of experience in managing or securing cloud environments.	Participants with less than two years of relevant professional experience.
Access to Cloud	Currently involved in projects or roles requiring CC security measures.	Not working in roles related to CC or cybersecurity.
Availability	Willing and available to participate in the survey within the designated timeframe.	Unable or unwilling to complete the survey within the given period.
Geographic Location	Open to participants from diverse geographic regions.	Participants without reliable access to the Internet for completing online surveys.
Language	Proficiency in English to ensure understanding of survey content.	Participants are unable to comprehend or respond to the survey in English.

3.7 Instrumentation

- **Data Encryption**

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Data Loss					
Effective measures are in place to prevent data loss.	1	2	3	4	5
There is a high level of awareness about data backup procedures.	1	2	3	4	5
Regular data backup and recovery tests are conducted to ensure data integrity.	1	2	3	4	5
Data loss incidents are promptly reported and effectively addressed.	1	2	3	4	5
Unauthorised Access					
Strict access control policies are implemented to prevent unauthorized access.	1	2	3	4	5
Strong passwords are used and changed regularly to enhance security.	1	2	3	4	5
Multi-factor authentication is employed to provide an additional layer of security.	1	2	3	4	5
Clear procedures are established for reporting and handling unauthorized access incidents.	1	2	3	4	5

- **Access Control**

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Insider Threats					
Measures are in place to detect and prevent insider threats.	1	2	3	4	5
There is a high level of awareness about the potential risks posed by insider threats.	1	2	3	4	5
Regular training sessions are conducted on recognising and reporting suspicious behaviour.	1	2	3	4	5
Clear procedures are established for investigating and responding to insider threat incidents.	1	2	3	4	5
Credential Theft					
Strong measures are in place to prevent credential theft.	1	2	3	4	5
The importance of safeguarding login credentials is emphasized to all users.	1	2	3	4	5
Advanced authentication methods, such as biometrics or token-based authentication, are employed.	1	2	3	4	5
Protocols for quickly responding to and mitigating credential theft incidents are well-established.	1	2	3	4	5

- **Intrusion Detection Systems (IDS)**

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Malware Infections					
Measures are in place to prevent malware infections across our systems and devices.	1	2	3	4	5
Anti-malware software is regularly updated and maintained to defend against new threats.	1	2	3	4	5
Incidents of malware infections are promptly detected, reported, and resolved.	1	2	3	4	5
Data Exfiltration					
Measures are in place to detect and prevent unauthorized data exfiltration attempts	1	2	3	4	5
There is a protocol for monitoring and analysing network traffic to identify potential data exfiltration.	1	2	3	4	5
Employees are educated on the risks and methods of data exfiltration.	1	2	3	4	5
Immediate actions are taken upon detecting data exfiltration attempts to prevent data loss.	1	2	3	4	5

- **Cloud Security Compliance.**

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The cloud service provider (CSP) we use complies with industry standards for security.	1	2	3	4	5
Access to sensitive data in the cloud is restricted based on defined roles and permissions.	1	2	3	4	5
Our organization regularly audits the security measures implemented by our CSP.	1	2	3	4	5
Our organisation conducts regular vulnerability assessments of our cloud infrastructure.	1	2	3	4	5
Our organisation ensures that data stored in the cloud is encrypted at rest.	1	2	3	4	5

- **Cloud Security Effectiveness**

Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Cloud security controls are consistently monitored and updated to address new vulnerabilities.	1	2	3	4	5
Our cloud security measures align with industry best practices and standards.	1	2	3	4	5
There is clear accountability for cloud security within our organization.	1	2	3	4	5

Our organisation has a proactive approach to identifying and mitigating cloud security risks.	1	2	3	4	5
Data integrity and confidentiality are well-maintained in our cloud environment.	1	2	3	4	5

3.8 Data Collection Procedures

The primary data were obtained from three survey questionnaires completed online, which provided quantitative data on cybersecurity threats and safeguards relating to CC. Writing the survey, the survey tool employed was a set of closed survey questions designed to assess the frequency and consequence of threats detected, including hacking, loss of data, and compliance violations, and the efficacy of implemented controls. This method made the response data both consistent and comparable, which complies with the recommended practices of cybersecurity research (Sen and Tiwari, 2017).

Accessing powerful, yet inexpensive, computational resources on demand is a key component of CC. It reduces the need to set aside funds for IT infrastructure and to buy and maintain pricey software and hardware. Prasad *et al.* (2018) and CSP completed the survey with 300 participants. The participants in the industry had the opportunity to give their opinions irrespective of their location and experiences because everything was done online. The questionnaires had to go through a pilot study to increase the validity of the data collected from the survey. This made the questions asked clear and aligned with the goals of the research. In the second part, current risks and Cloud Security Solutions were identified out of the data and statistic tools by doing a descriptive analysis of the data.

3.9 Data Analysis

Data analysis was done using “Statistical Package for the Social Sciences” (SPSS), which is a strong instrument used to analyse research data most often in quantitative

research (Habes, Ali and Pasha, 2021). This study used three main statistical methods, i.e, The research tools of this study are descriptive analysis, regression analysis and correlation analysis. Data was analysed descriptively to gain an idea of the general thoughts of the participants on cybersecurity concerns and possible solutions. The qualitative results revealed that data and compliance were the greatest risks to organisations when it came to risk mitigation. To illustrate these threats, statistics such as frequency, percentage, mean scores, and standard deviations were employed.

Regression analysis was conducted using multiple regression, where the intent was to establish a relationship between the level of independent factors, such as compliance with cybersecurity policies and controls and the levels of security incidences.

It also provided more information about the increase/decrease in risk that should guide the selection of measures with greater influence over the risk reduction (George and Mallery, 2024). Additionally, correlation analysis quantified the nature and degree of the relationships: compliance practice and minimised risk exposures, or training for specific employees and the rate of incidents. This approach gave a further understanding of how factors in a system either improve or reduce security stances (Algarni et al., 2021).

Scatter plots and histograms were also utilised in the analysis of data trends as figures to enhance the interpretation of the results. This enabled a comprehensive analysis, and the findings formed a basis for recommendations on the necessary changes for CC security frameworks for professional environments.

3.10 Research Design Limitations

The research design, while robust, had several limitations that must be acknowledged:

- **Sampling Bias:** It is also realised that the samples obtained from convenience sampling might have always been easily accessible and willing to participate.

This approach may not have curated the views of all the stakeholders in the study, especially the minority group composed of small organisations or in secluded sectors (Etikan, 2016)

- **Generalizability:** The convenience sample is based on the purposive choice of the participants, so the results cannot be considered generalizable to the population of CSP and IT specialists. Only the selected hosts are relevant and can be impacted by the regional factors, which restrict the generalization of the research findings to the world of global CC.
- **Self-Reported Data:** Surveys questionnaire could easily be affected by response biases where the respondents make approximations about what is practiced in their organisations rather than providing actual figures. Responses made by themselves can also confound the data with some respondents potentially providing more desirable answer (Podsakoff *et al.*, 2003).
- **Cross-sectional Design**: Since the study's data were only gathered once, it employed a cross-sectional research design. This hampers the consideration of time series data on the trend or changes in cybersecurity practices over time, eliminating any possibilities of establishing causal relations between such variables.
- **Limited Depth of Responses:** While the survey contains many closed-ended questions, this approach limited the extent of participants' answers. Other research questions could have offered a deeper and more detailed understanding of cloud security from the participants' perspective.
- **Survey Distribution:** Despite the convenience of using an online survey, respondents with less access to computers, especially on the Internet, or those who are not familiar with other similar survey instruments, may have been left

out. This could also mean that there would be biased sampling, and some demographic variables would be understated (Pallant, 2020).

3.11 Conclusion

Altogether, this research contributed to understanding cybersecurity threats and executive controls in CC contexts using a quantitative research approach. With developed and standardised questionnaires and data analysis tool SPSS, the major risks, including data leakage, compliance risk and governance risk, and their efficient handling, were identified. Despite the convenience sampling, which allowed the study to capture a specific population of IT professionals and cybersecurity experts, some limitations arise from the method used and their relation to the validity and reliability of the results. Nevertheless, the research contributes to a body of knowledge of cybersecurity in cloud infrastructure and provides practical insights on how to improve organisations' security posture. Future work can overcome the limitations by utilising longitudinal data and diverse sampling techniques and, therefore, gaining more holistic information on the dynamic nature of threats and protections in the cloud environment.

CHAPTER IV:

RESULTS

4.1 Reliability Statistics

Table 4.1: Reliability Statistics

Cronbach's Alpha	N of Items
.612	33

According to Table 4.1, there is a moderate degree of correlation between the 33 items of the scale and a Cronbach's Alpha score of 0.612, which suggests a reasonable level of internal consistency. Although this value can be considered adequate in the exploratory research or in the first stage of scale development, it is lower than the generally recognised level of 0.7 in strong reliability. It means that the scale should be improved and the review of the items in terms of their clarity, relevance, and redundancy may contribute to the reliability of the instrument.

4.2 Analysis of Demographic Details of Respondents

Table 4.2: Demographic Details of Respondents

		Frequency	Percent
Age	18-29 Years	54	18
	30-39 Years	56	18.7
	40-49 Years	65	21.7
	50-59 Years	54	18
	60 and above Years	71	23.7
Gender	Male	189	63
	Female	111	37
Educational Background	Bachelor's degree	82	27.3
	Master's degree	76	25.3
	Doctorate	97	32.3
	Other	45	15

Field of Study	Computer Science/IT	48	16
	Engineering	40	13.3
	Business	36	12
	Humanities	49	16.3
	Social Sciences	48	16
	Natural Sciences	56	18.7
	Other	23	7.7
Current Position	IT Support/Technician	33	11
	Network Administrator	30	10
	Systems Administrator	31	10.3
	Security Analyst	31	10.3
	Software Developer	38	12.7
	IT Manager/Director	43	14.3
	Chief Information Officer (CIO)	41	13.7
	Chief Information Security Officer (CISO)	35	11.7
	Other	18	6
Years of Experience in IT/Cybersecurity	Less than 1 year	54	18
	1-3 years	99	33
	4-6 years	58	19.3
	7-10 years	46	15.3
	More than 10 years	43	14.3
Industry Sector	Technology	36	12
	Finance	38	12.7
	Healthcare	46	15.3
	Education	38	12.7
	Government	44	14.7
	Retail	45	15
	Manufacturing	37	12.3
	Other	16	5.3
Size of Organisation	Small (1-50 employees)	69	23
	Medium (51-500 employees)	78	26
	Large (51-500 employees)	74	24.7
	Very Large (5001+ employees)	79	26.3

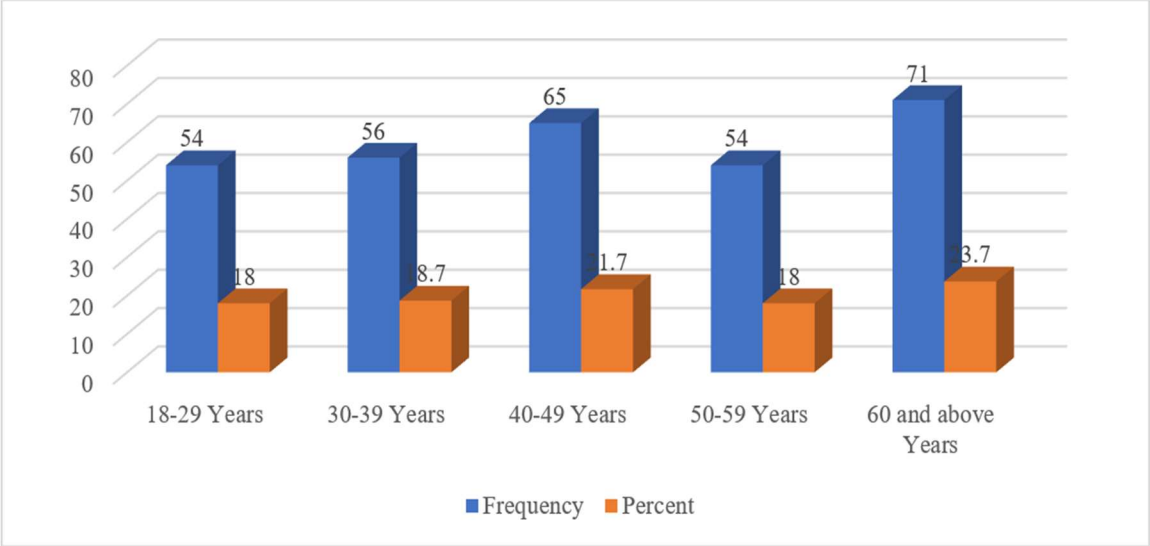

Figure 4.1: Age

The Figure 4.1 above gives the distribution of the respondents with the highest respondents being those aged 60 and above comprising 23.7% of the sample then those aged 40-49 years comprising 21.7% of the sample. The ages 30-39 years comprise 18.7% and 18-29 years and 50-59 years are both 18%. It shows that the distribution of the age categories is rather balanced, and older respondents have a minor majority.

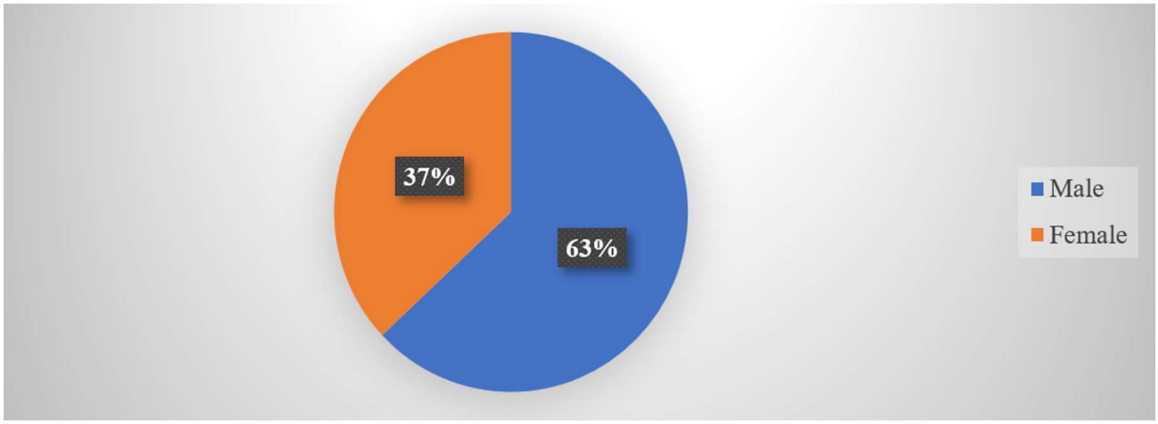

Figure 4.2: Gender

Figure 4.2 presents the gender distribution of the respondents, as 63 percent of them are men and 37 percent are women. This implies that the sample was composed of men, which, considering the nature of the study, as well as its setting, might influence the results.

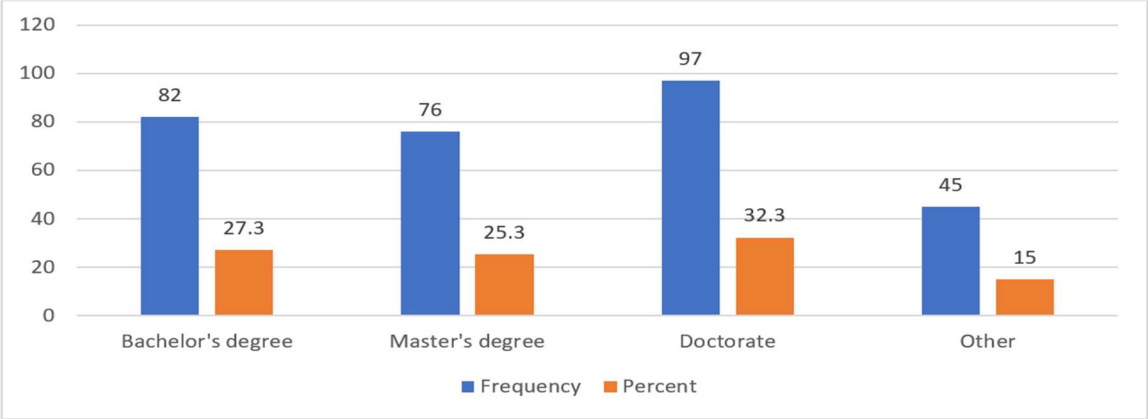

Figure 4.3: Educational Background

Figure 4.3 demonstrates that the educational level of the respondents is Doctorate degree 32.3 followed by the respondents with Bachelor and Master degrees with a 27.3 and 25.3% respectively. The others (15 percent) possess other educational qualifications. This distribution suggests that it is a well-educated sample with a considerable number of people who have advanced degrees.

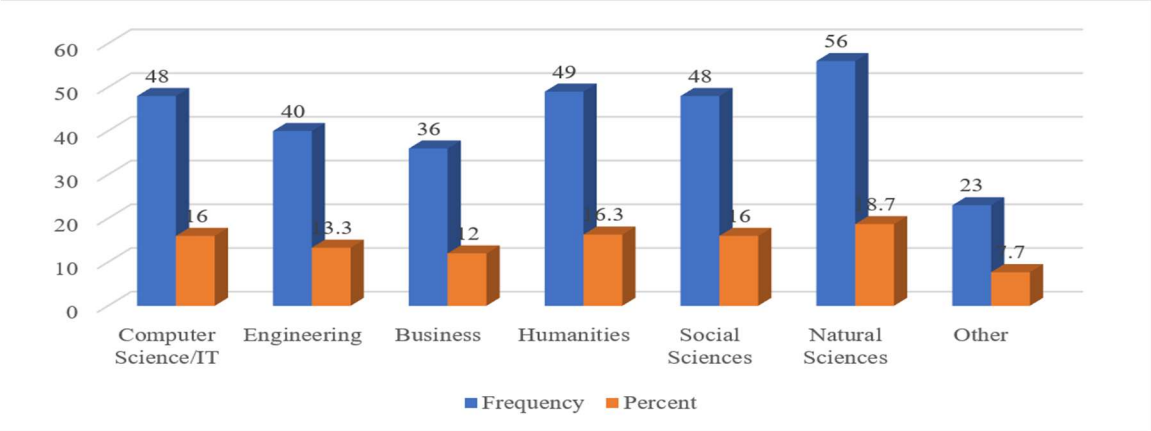

Figure 4.4: Field of Study

As Figure 4.4 demonstrates, the respondents are of various fields of study with the highest percentage of 18.7 presented by Natural Sciences, then 16.3 by Humanities, 16 by Computer Science/IT, and 16 by Social Sciences. The Engineering and Business respondents make up 13.3 and 12.0 respectively with 7.7 occupying the rest. It is a wide distribution of academic disciplines with a slight prevalence of natural and social sciences.

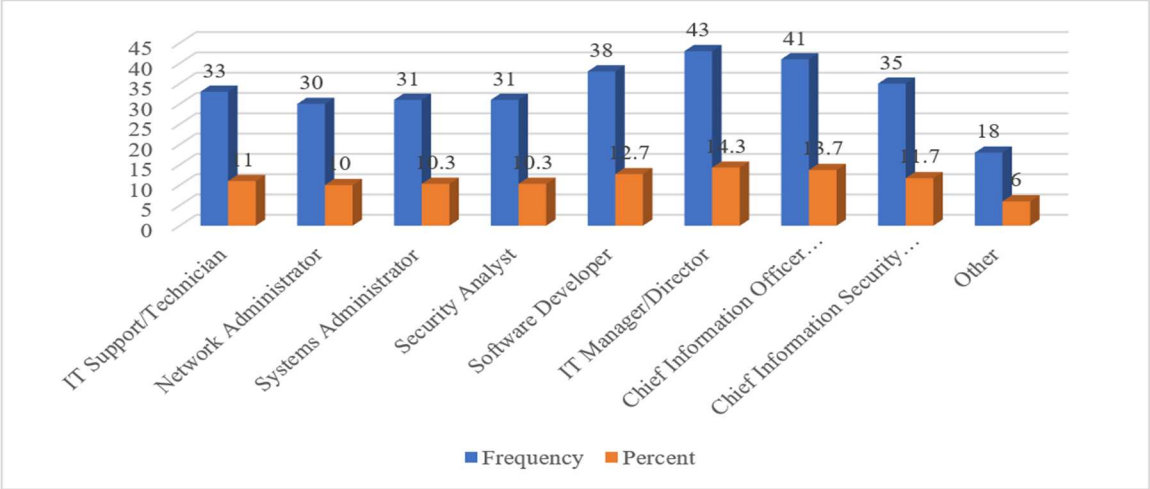

Figure 4.5: Current Position

As shown in Figure 4.5, the respondents are found to hold different positions in the IT sector. The most common are IT Manager/Director with 14.3% and Software Developer with 12.7% with Chief Information Officer (CIO) and Chief Information Security Officer (CISO) coming in the next with 13.7% and 11.7% respectively. Other jobs like IT Support/Technician 11%, Network Administrator 10%, Systems Administrator 10.3% and Security Analyst 10.3% are also well represented. Other is the smallest group with a proportion of 6% of the respondents. This distribution is a good representation of manager and technical positions in IT related career.

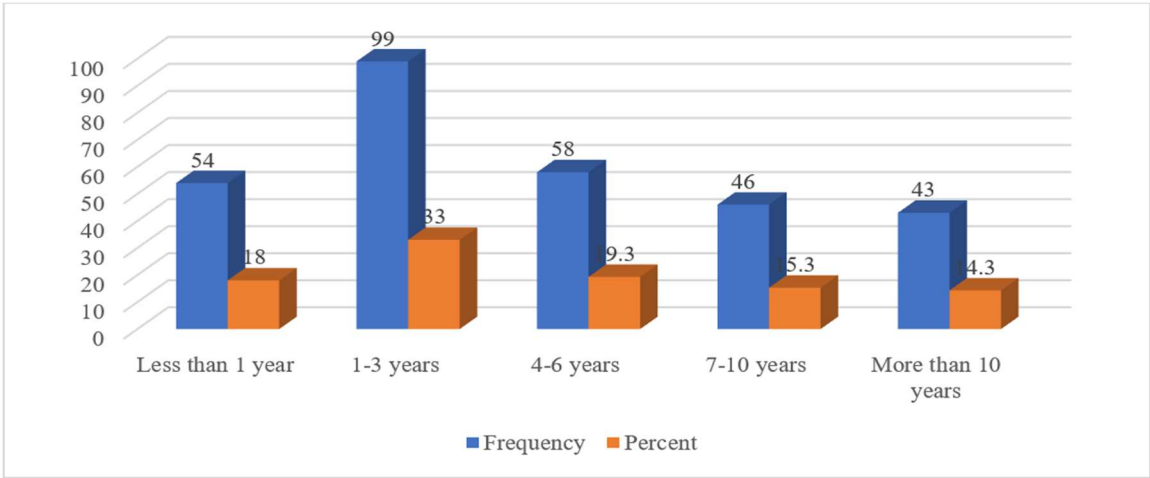

Figure 4.6: Years of Experience in IT/Cybersecurity

The distribution of years of the respondents in terms of experience in IT/Cybersecurity is as shown in Figure 4.6: the majority (33%), that had between 1-3 years of experience, comes next, and with years between four to ten (19.3%), more than ten years (14.3%). As the percentage of those respondents possessing one to three years of experience was quite high, it indicates that most of them are relatively inexperienced in the industry.

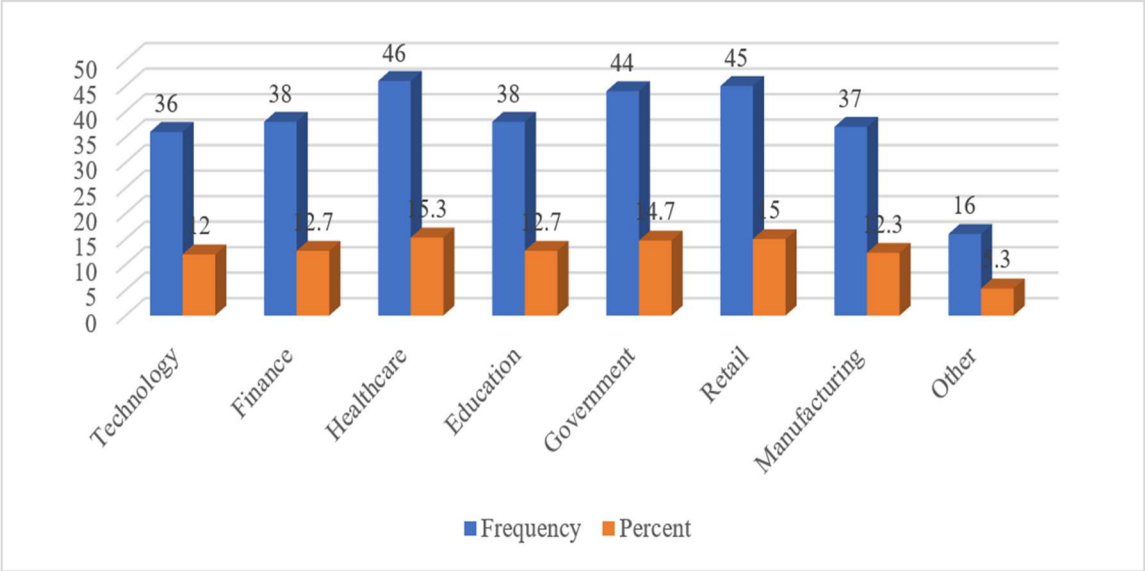

Figure 4.7: Industry Sector

Figure 4.7 indicates that the respondents represent other industrial sectors. The healthcare sector has the biggest representation at 15.3% then by Retail (15) and Government (14.7). Other sectors, namely, the Finance sector, the Education sector, each take 12.7 percent, and Technology takes 12%. The Manufacturing industry takes the 12.3% and the smallest number will be the Other group that will constitute 5.3% of the respondents. This distribution depicts a wide-ranging blend of industries with slight applications in the healthcare, retail and government sectors.

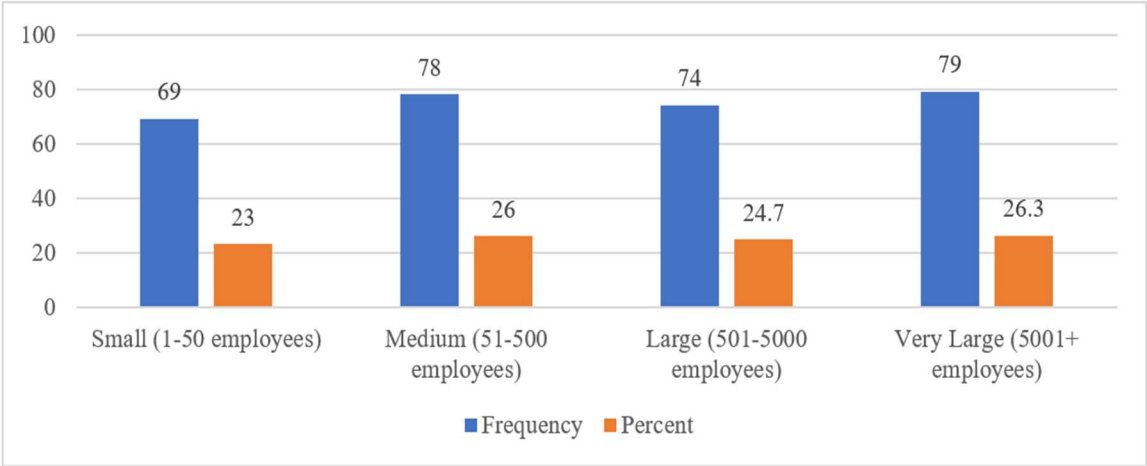

Figure 4.8: Size of Organisation

Figure 4.8 shows that the participants represent a range of organisational sizes. Organisations with 500 or more employees make up the biggest group, with 26.3% of the total. Medium-sized businesses, with 51 to 500 workers, come in second, with 26.3%. Companies with 1-50 employees make up 23% of all enterprises, while companies with 501-5000 employees account for 24.7% of all firms. While there is some concentration on large and medium-sized businesses, this distribution reveals a pretty consistent pattern across different sizes of organisations.

4.3 Analysis of Data Encryption Influence on Unauthorised Access and Data Loss

Table 4.3: Data Encryption

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Data Loss						
Effective measures are in place to prevent data loss.	Frequency	24	19	91	77	89
	Percent	8	6.3	30.3	25.7	29.7
There is a high level of awareness about data backup procedures.	Frequency	17	17	86	89	91
	Percent	5.7	5.7	28.7	29.7	30.3
	Frequency	15	13	81	92	99

Regular data backup and recovery tests are conducted to ensure data integrity.	Percent	5	4.3	27	30.7	33
Data loss incidents are promptly reported and effectively addressed.	Frequency	22	10	90	95	83
	Percent	7.3	3.3	30	31.7	27.7
Unauthorised Access						
Strict access control policies are implemented to prevent unauthorised access.	Frequency	17	22	93	89	79
	Percent	5.7	7.3	31	29.7	26.3
Strong passwords are used and changed regularly to enhance security.	Frequency	20	19	88	91	82
	Percent	6.7	6.3	29.3	30.3	27.3
Multi-factor authentication is employed to provide an additional layer of security.	Frequency	27	25	89	80	79
	Percent	9	8.3	29.7	26.7	26.3
Clear procedures are established for reporting and handling unauthorised access incidents.	Frequency	29	21	77	86	87
	Percent	9.7	7	25.7	28.7	29

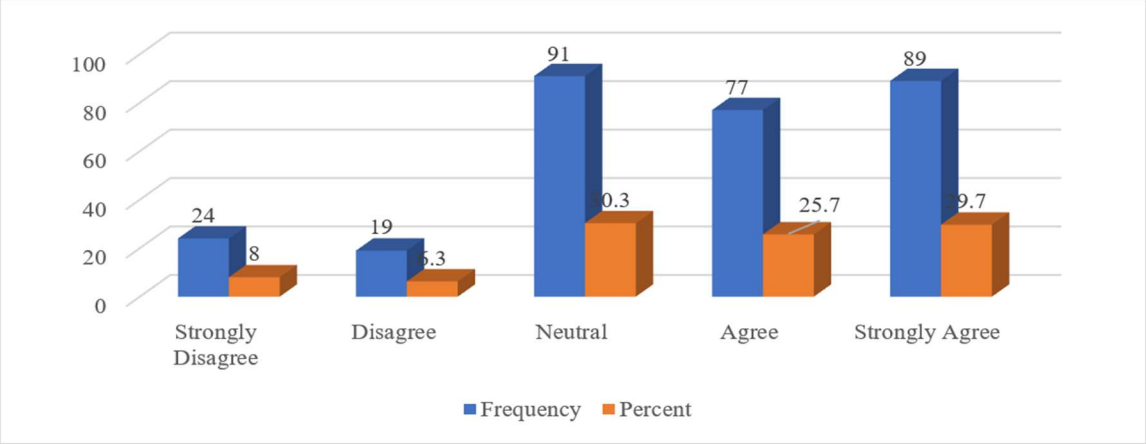

Figure 4.9: Effective measures are in place to prevent data loss.

Figure 4.9 shows that we polled people on how well current safeguards are doing in avoiding data loss. With 25.7% agreeing and 29.7% strongly agreeing, for a total of 55.4% of the sample, the statement was acknowledged by the majority of respondents. While a lower number of 8% strongly opposed and 6.3% disagreed, a considerable portion remained undecided at 30.3%. While most people think the right steps have been taken, it seems that a sizeable minority is either unsure or thinks they aren't going far enough.

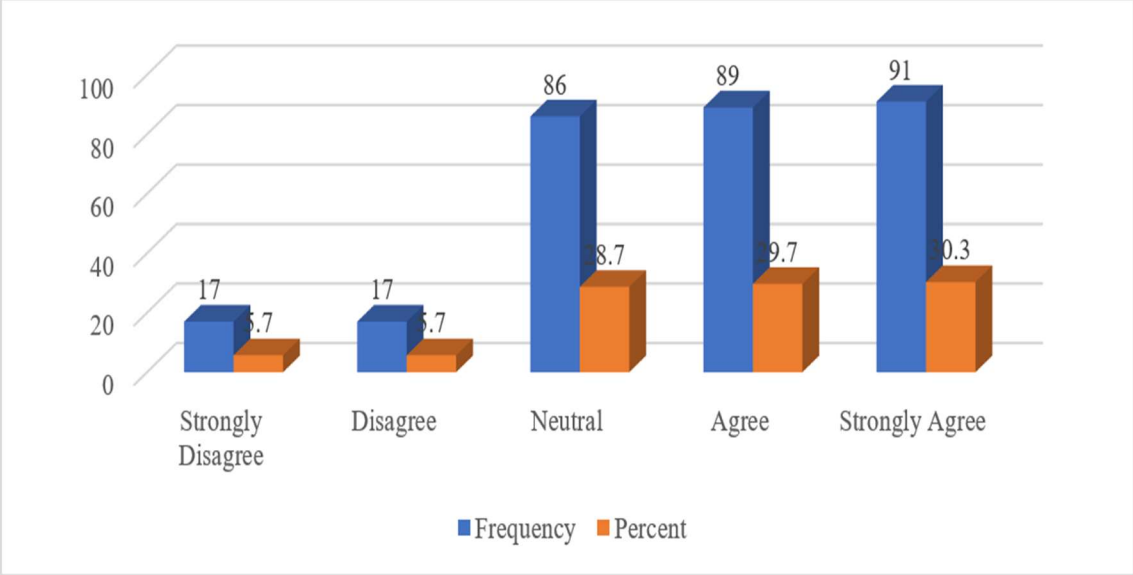

Figure 4.10: There is a high level of awareness about data backup procedures.

Figure 4.10 illustrates that most responders indicate a high level of awareness regarding data backup procedures. 29.7% agree, and 30.3% strongly agree with the statement, totalling 60% of the respondents expressing positive awareness. However, a notable portion of respondents remain neutral 28.7%, and smaller percentages 5.7% strongly disagree and disagree, respectively. This suggests that while most respondents are aware of data backup procedures, there remains a portion who are either unaware or uncertain.

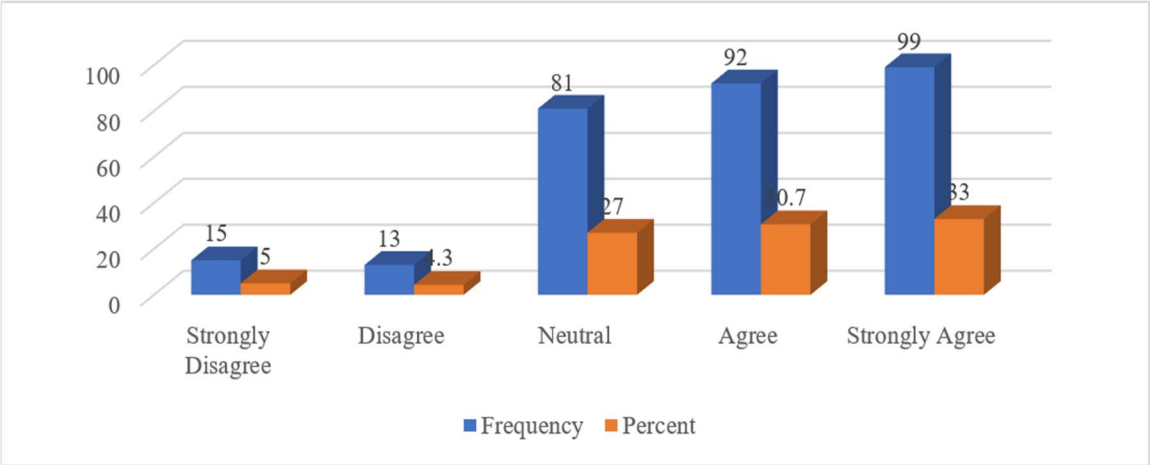

Figure 4.11: Regular data backup and recovery tests are conducted to ensure data integrity.

As seen in Figure 4.11 for an example of how the majority of respondents believe data backup and recovery testing is done often to guarantee data integrity. The poll found that these exams are done regularly by 63.7% of the persons who took it, with 30.7% agreeing and 33.0% strongly agreeing. While 5% strongly disagree and 4.3% disagree, a smaller minority of respondents (27% total) remain neutral. While some may be unsure or think these tests are not performed routinely, the vast majority of respondents seem to agree that data integrity is guaranteed through regular backup and recovery tests.

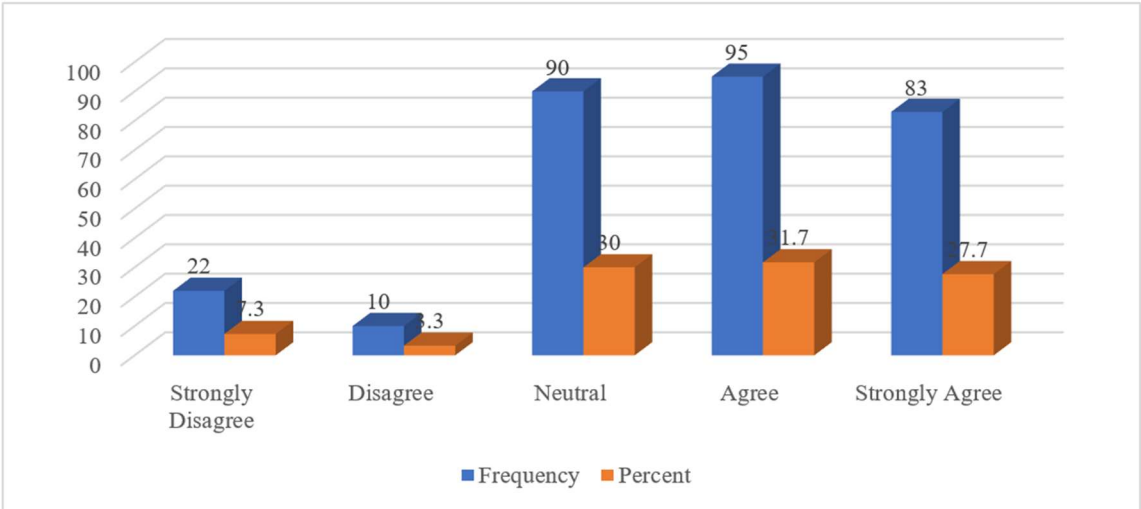

Figure 4.12: Data loss incidents are promptly reported and effectively addressed.

Figure 4.12 shows that most respondents believe data loss incidents are reported and addressed efficiently. In all, 59.4% of people who took the survey have faith in the procedure, with 31.7% being in agreement and 27.7% being very much so. Just a small percentage is ambivalent, compared to 30% who are agnostic, 7.3% who strongly disagree, and 3.3% who disagree. Although most respondents believe data loss situations are handled well, this indicates that there is still some uncertainty or dissatisfaction with the process.

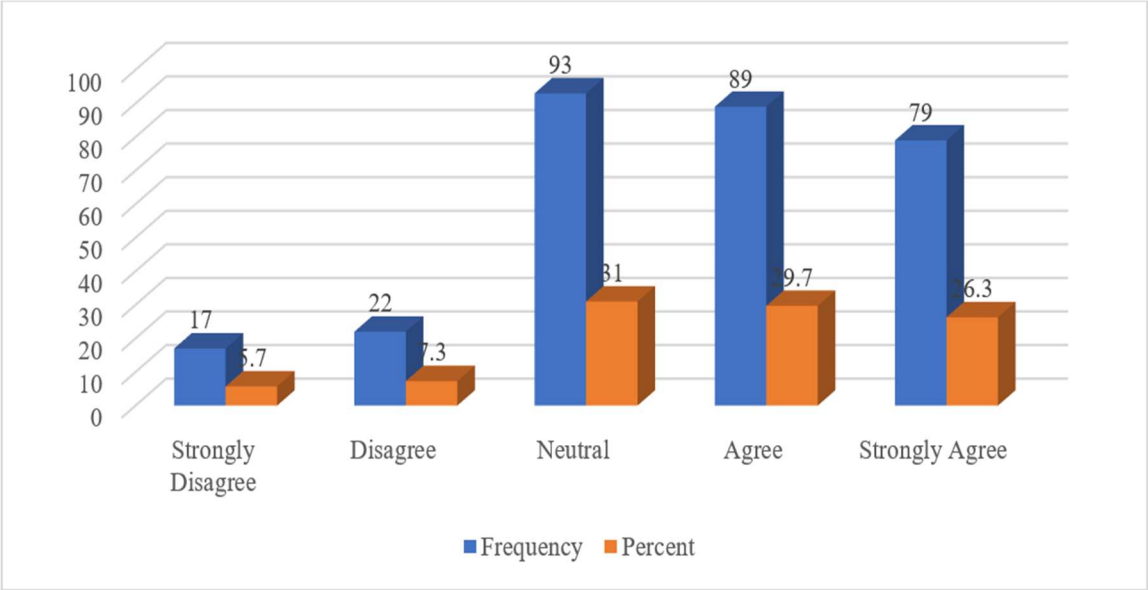

Figure 4.13: Strict access control policies are implemented to prevent unauthorised access.

Most respondents think there are stringent rules in place to prevent unauthorised access (Figure 4.13). With 29.7 percent in agreement and 26.3 percent in strong agreement, 56 percent of people who took the survey think these measures are working. With 31% remaining neutral, there is a sizable minority with 5.7% strongly disagreeing and 7.3% disagreeing. While many people think access control measures are strong, it seems that many aren't sure or aren't happy with how they're being put into practice.

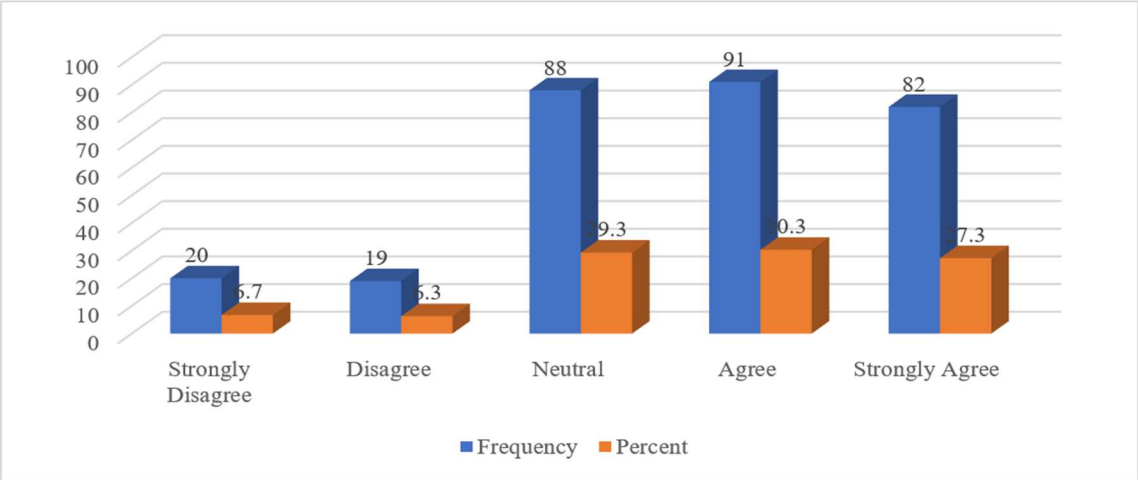

Figure 4.14: Strong passwords are used and changed regularly to enhance security.

According to Figure 4.14, the majority of respondents think that strong passwords are routinely changed in order to increase security. With 27.3% strongly agreeing and 30.3% agreeing, 57.6% of people who took the survey are in favour of this practice. A sizeable minority (6.7%) strongly disagrees and 6.3% disagree, while 29.3% are agnostic. This indicates that while most respondents acknowledge the importance of using and regularly changing strong passwords, there is still some uncertainty or lack of adherence to this security measure.

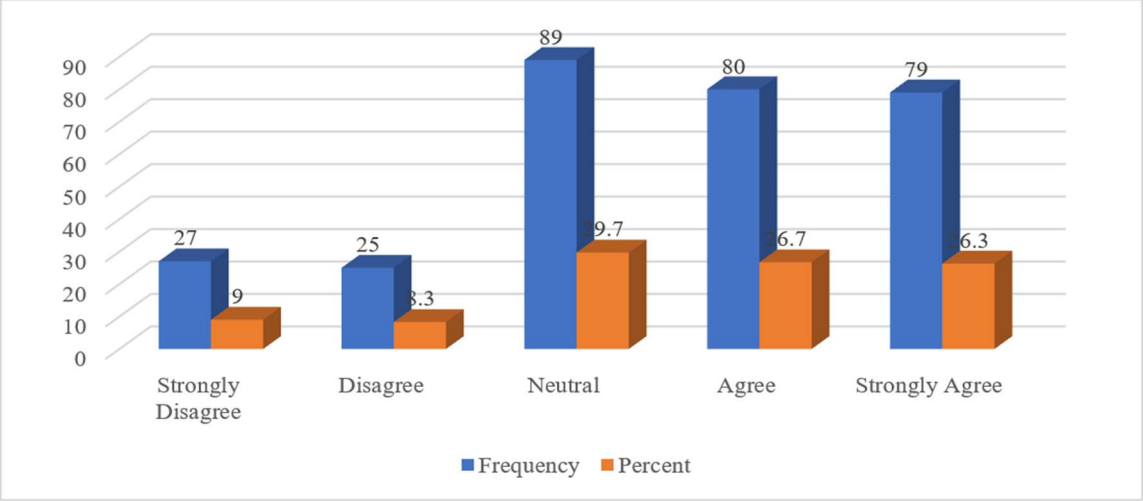

Figure 4.15: Multi-factor authentication is employed to provide an additional layer of security.

Figure 4.15 demonstrates that a significant number of respondents mention using multi-factor authentication (MFA) as an additional layer of security. Some 53% of people who took the survey have confirmed that MFA is used, with 26.7 percent agreeing and 26.3 percent strongly agreeing. Although just 9% strongly disagree and 8.3% disagree, a sizeable number (29.7% to be exact) stays undecided. This suggests that while many respondents acknowledge the use of MFA for enhanced security, there is still a considerable group who are either unsure or believe it is not implemented.

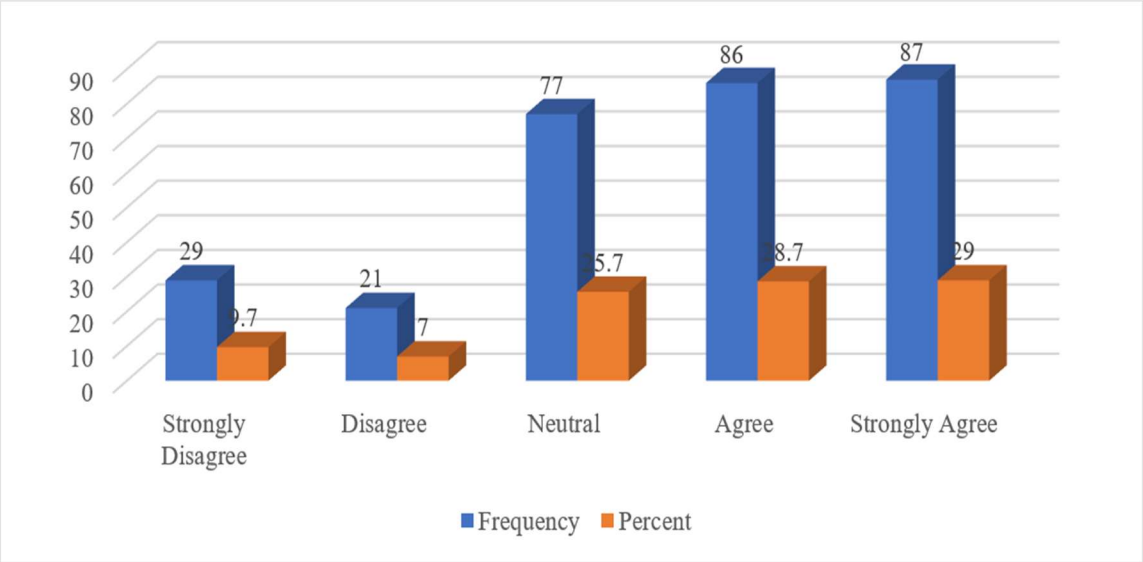

Figure 4.16: Clear procedures are established for reporting and handling unauthorized access incidents.

Figure 4.16 shows that the majority of respondents think there are well-defined processes for reporting and dealing with occurrences of unauthorised access. The presence of such procedures is confirmed by 57.7% of respondents, with 28.7% agreeing and 29% strongly agreeing. While a lesser percentage of people disagree and 9.7 percent strongly disagree, a significant portion of people (25.7 percent) remain undecided. This indicates that although the majority of respondents think the policies and procedures for dealing with unauthorised access are clear, some are unsure or unhappy with how things are laid out.

Hypothesis One

- **H1:** There is a significant impact of data encryption on mitigating the risks of unauthorized access and data loss in cloud computing environments.

Table 4.4: Correlations

			Unauthorised Access	Data Loss	Data Encryption
Spearman's rho	Unauthorised Access	Correlation Coefficient	1.000	.157**	.613**
		Sig. (2-tailed)	.	.006	.000
		N	300	300	300
	Data Loss	Correlation Coefficient	.157**	1.000	.526**
		Sig. (2-tailed)	.006	.	.000
		N	300	300	300
	Data Encryption	Correlation Coefficient	.613**	.526**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	300	300	300

According to table 4.4, there is a strong connection between data encryption, unauthorised access, and data loss in cloud computing environments. There is a high correlation between data encryption and unauthorised access (Spearman's rho = 0.613, $p < 0.01$), and a little correlation between data loss and data encryption (Spearman's rho = 0.526, $p < 0.01$). This suggests that the dangers of intrusion and data loss are considerably reduced as encryption technology advances. In addition, both unauthorised access and data loss have a weak but significant association (Spearman's rho = 0.157, $p < 0.01$), indicating that both risks are interdependent. Based on this data, Hypothesis H1 is supported, affirming that data encryption has a significant impact on reducing the risks of unauthorised access and data loss in CC environments.

4.4 Analysis of Access Control Influence on Insider Threats and Credential Theft

Table 4.5: Access Control

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Insider Threats						
Measures are in place to detect and prevent insider threats.	Frequency	22	23	82	92	81
	Percent	7.3	7.7	27.3	30.7	27
There is a high level of awareness about the potential risks posed by insider threats.	Frequency	28	19	90	82	81
	Percent	9.3	6.3	30	27.3	27
Regular training sessions are conducted on recognising and reporting suspicious behaviour.	Frequency	19	23	76	96	86
	Percent	6.3	7.7	25.3	32	28.7
Clear procedures are established for investigating and responding to insider threat incidents.	Frequency	15	23	83	76	103
	Percent	5	7.7	27.7	25.3	34.3
Credential Theft						
Strong measures are in place to prevent credential theft.	Frequency	27	24	77	78	94
	Percent	9	8	25.7	26	31.3
The importance of safeguarding login credentials is emphasised to all users.	Frequency	23	25	91	75	86
	Percent	7.7	8.3	30.3	25	28.7
Advanced authentication methods, such as biometrics or token-based authentication, are employed.	Frequency	15	13	106	74	92
	Percent	5	4.3	35.3	24.7	30.7
Protocols for quickly responding to and mitigating credential theft incidents are well-established.	Frequency	21	22	89	88	80
	Percent	7	7.3	29.7	29.3	26.7

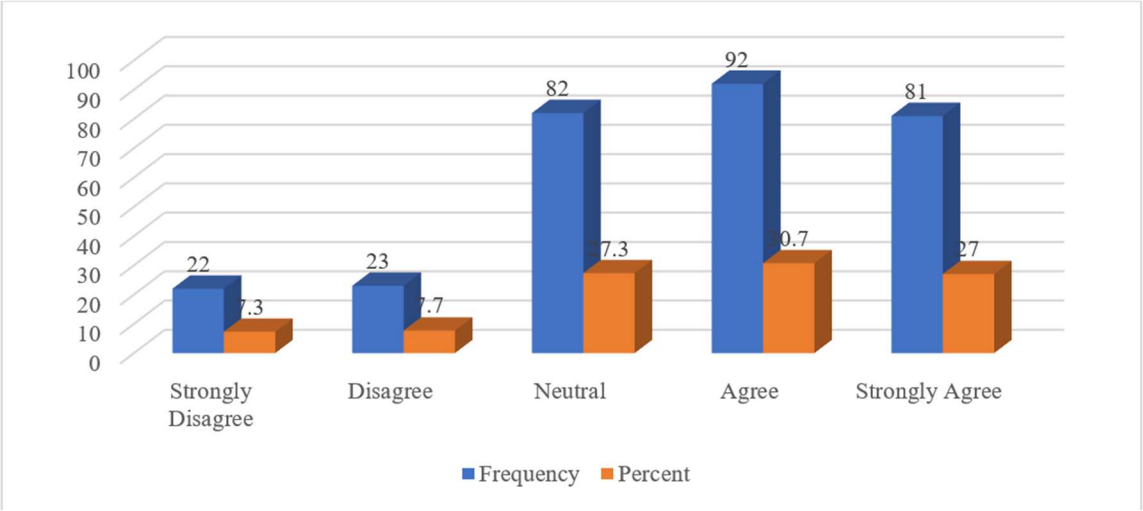

Figure 4.17: Measures are in place to detect and prevent insider threats.

Figure 4.17 shows that a large percentage of people think there are safeguards to identify and stop insider threats. A total of 57.7% of respondents have confirmed the existence of such measures, with 30.7% strongly agreeing and 27% agreeing. A considerable portion remains neutral, 27.3%, while smaller percentages, 7.7% disagree and 7.3% strongly disagree. This indicates that some respondents are unsure or unhappy with the efficacy of these measures, even though most think insider risks are sufficiently handled.

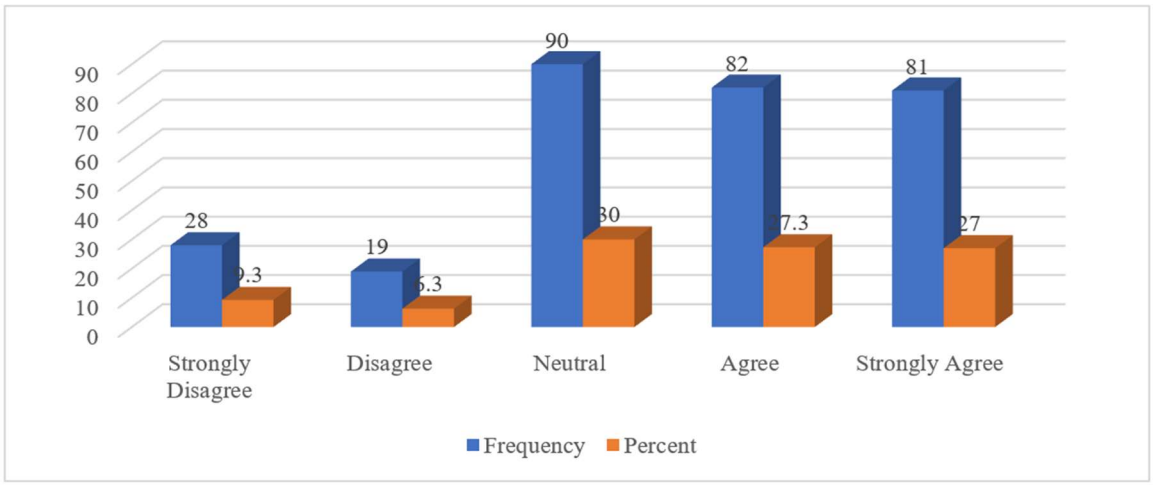

Figure 4.18: There is a high level of awareness about the potential risks posed by insider threats.

According to Figure 4.18, most respondents express a high degree of awareness about the possible dangers posed by insider threats. 27.3% agree, and 27% strongly agree, totalling 54.3% of respondents expressing awareness of these risks. While a lower amount of 9.3% strongly disagree and 6.3% disagree, a considerable portion (30%) stays neutral. The results show that although most people are aware of the dangers posed by insider threats, a sizeable minority is either unsure or fails to completely grasp the gravity of the situation.

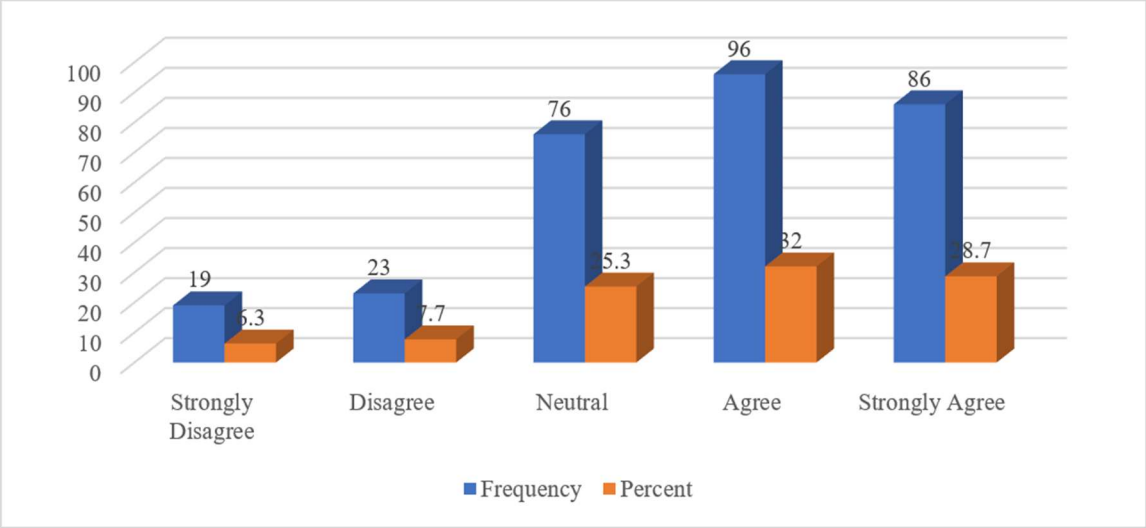

Figure 4.19: Regular training sessions are conducted on recognising and reporting suspicious behaviour.

Figure 4.19 illustrates that most responders believe that regular training sessions are conducted on recognizing and reporting suspicious behaviour. 32% agree and 28.7% strongly agree, totalling 60.7% of respondents affirming the occurrence of such training. A significant portion remains neutral, 25.3%, while smaller percentages, 6.3% strongly disagree, and 7.7% disagree. While the majority of respondents agree that training on suspicious behaviour is important, some are unclear or believe it is not happening often enough.

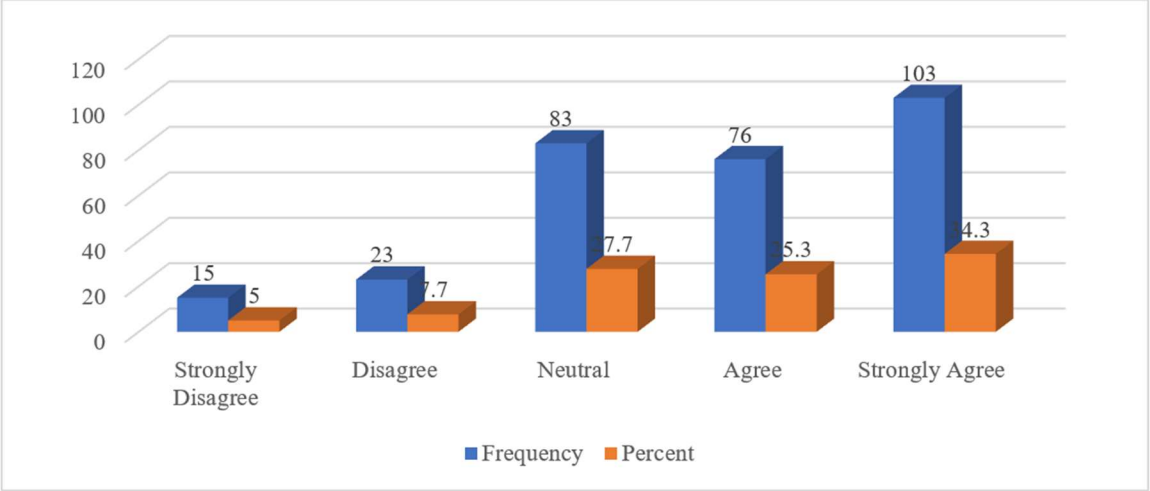

Figure 4.20: Clear procedures are established for investigating and responding to insider threat incidents.

Figure 4.20 shows that most responders think there are well-defined protocols for handling insider threat investigations. A total of 59.6% of respondents have confirmed the presence of such procedures, with 25.3% agreeing and 34.3% strongly agreeing. Of the total, 27.7% are agnostic, while 7.7% disagree and 5% are extremely opposed. Although the majority of respondents acknowledge the existence of processes for dealing with insider threats, there appears to be some lingering doubt or discontent over the efficacy and clarity of these protocols.

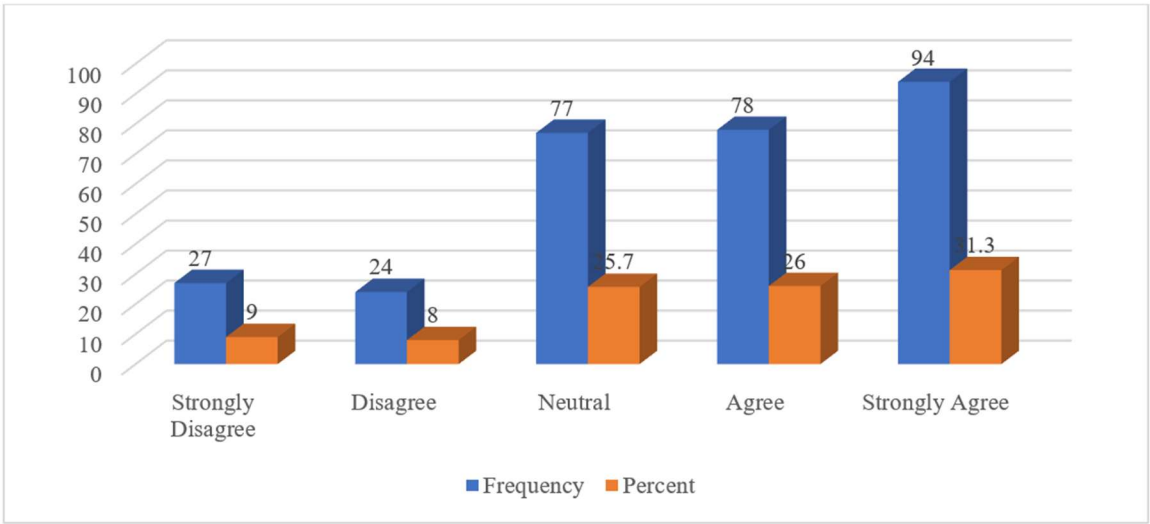

Figure 4.21: Strong measures are in place to prevent credential theft.

Evident in Figure 4.21 is the high percentage of respondents who believe there are robust protections against credential theft. With 26% in agreement and 31.3% in strong agreement, 57.3% of respondents verified the existence of such measures. A sizeable number of 25.7% is undecided, while a lesser percentage of 9% strongly disagrees and 8% disagree. Despite the fact that most people are sure the safeguards are in place to avoid credential theft, this reveals that some are unsure or think they are inadequate.

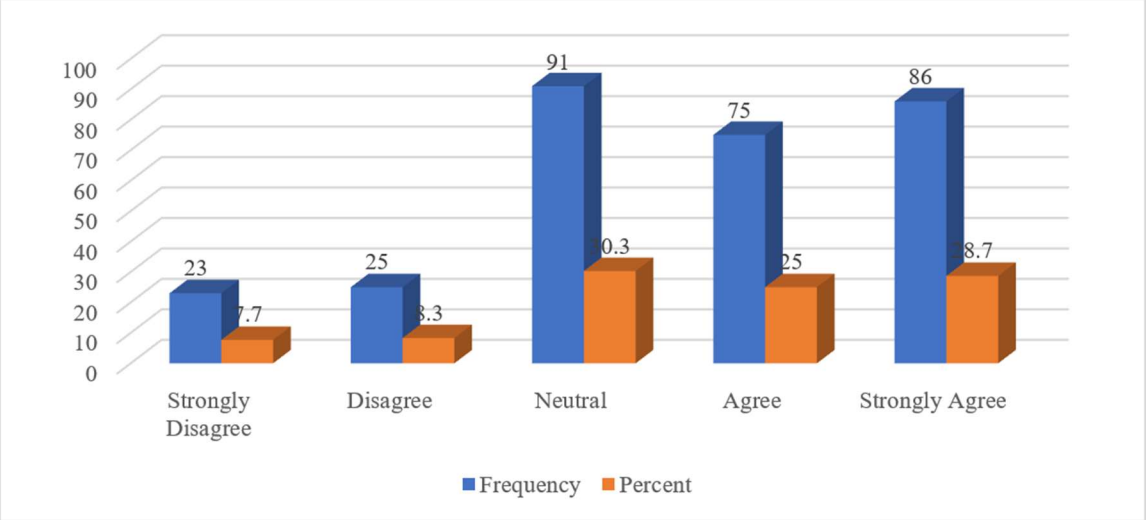

Figure 4.22: The importance of safeguarding login credentials is emphasized to all users.

Figure 4.22 shows that the majority of respondents think that all users are reminded of the significance of protecting their login credentials. With a total of 53.7 percent of respondents stating that the message is well conveyed, 25% agree and 28.7 percent strongly agree. While a smaller number of 8.3% disagree and 7.7% strongly disagree, a considerable portion of 30.3% remains undecided. This indicates that some respondents are neither sure nor think the message is sufficiently delivered regarding the significance of credential security, even if the majority of respondents hold this view.

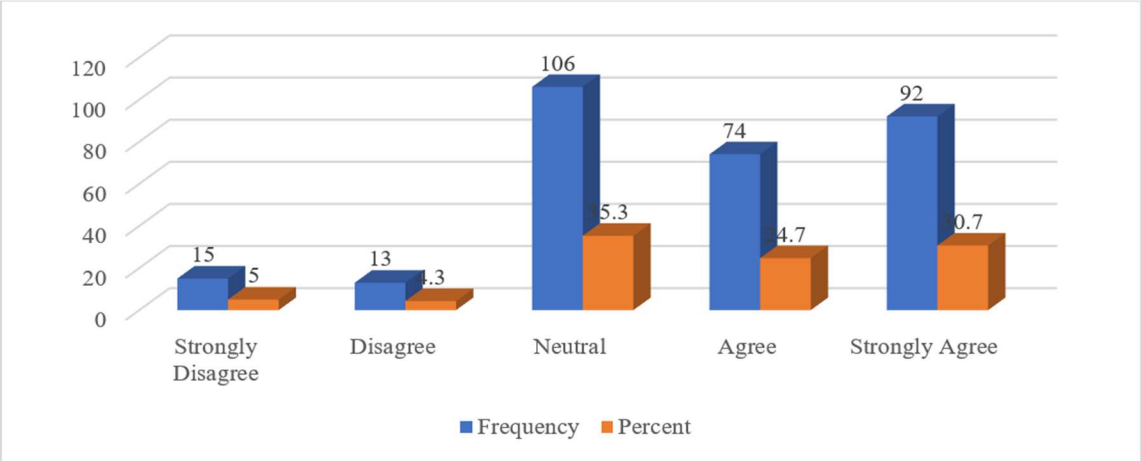

Figure 4.23: Advanced authentication methods, such as biometrics or token-based authentication, are employed.

Figure 4.23 shows that most respondents believe that advanced authentication methods are employed, such as biometrics or token-based authentication. In all, 55.4% of people who took the survey agree that these techniques are used, with 30.7% agreeing and 24.7% strongly agreeing. While a smaller minority of 5% strongly disagrees and 4.3% disagree, a significant part of 35.3% remains undecided. As a result, it is clear that although many respondents are aware of the usage of advanced authentication methods, a sizeable minority is either confused or thinks these methods are not in use.

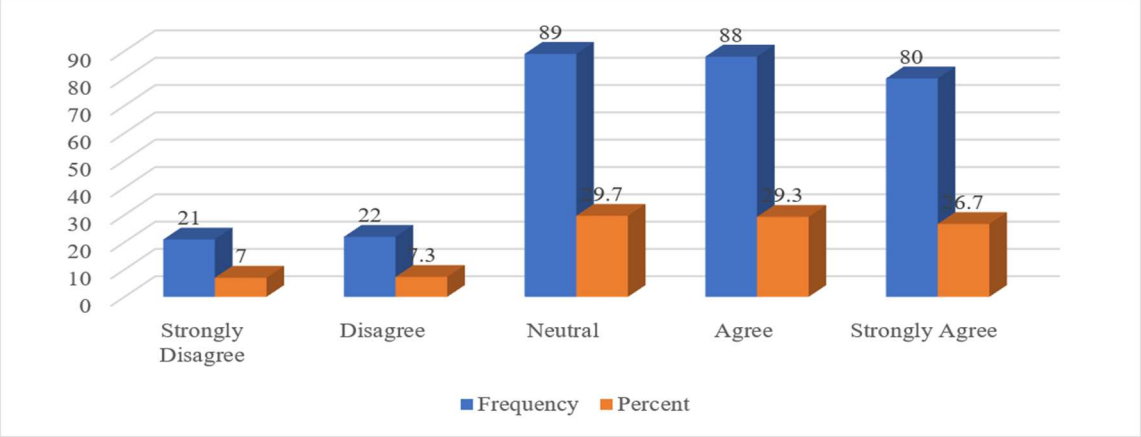

Figure 4.24: Protocols for quickly responding to and mitigating credential theft incidents are well-established.

Figure 4.24 shows that the majority of responders think there are defined methods for reacting to and minimising credential theft events. A total of 56% of respondents have confirmed the presence of these protocols, with 29.3% agreeing and 26.7% strongly agreeing. While a smaller amount of 7% strongly disagrees and 7.3% disagree, a significant portion of 29.7% stays undecided. Despite the majority of respondents believing that adequate mechanisms have been put in place to deal with credential theft, a sizeable fraction remains unsure or unhappy with the current processes.

Hypothesis Two

- **H2:** There is significant effectiveness of access control mechanisms in preventing insider threats and credential theft in cloud computing systems.

Table 4.6: Correlations

			Insider Threats	Credential Theft	Access Control
Spearman's rho	Insider Threats	Correlation Coefficient	1.000	.241**	.679**
		Sig. (2-tailed)	.	.000	.000
		N	300	300	300
	Credential Theft	Correlation Coefficient	.241**	1.000	.589**
		Sig. (2-tailed)	.000	.	.000
		N	300	300	300
	Access Control	Correlation Coefficient	.679**	.589**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	300	300	300

Credential theft, insider threats, and CC access control are all interrelated, as seen in tab 4.6. Statistical analysis reveals a robust positive relationship between access control and the decrease of insider threats (rho = 0.679, $p < 0.01$) and credential theft (rho = 0.589, $p < 0.01$). Furthermore, there is a weak but substantial correlation between insider threats and credential theft (Spearman's rho = 0.241, $p < 0.01$). This data lends credence to the null

hypothesis (H2) that attempts to restrict access do in fact reduce the likelihood of insider attacks and stolen credentials.

4.5 Analysis of Intrusion Detection Systems (IDS) Influence on Malware Infections and Data Exfiltration

Table 4.7: Intrusion Detection Systems (IDS)

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Malware Infections						
Anti-malware software is regularly updated and maintained to defend against new threats.	Frequency	26	17	91	76	90
	Percent	8.7	5.7	30.3	25.3	30
Incidents of malware infections are promptly detected, reported, and resolved.	Frequency	20	11	84	94	91
	Percent	6.7	3.7	28	31.3	30.3
Data Exfiltration						
Measures are in place to detect and prevent unauthorized data exfiltration attempts.	Frequency	18	12	86	96	88
	Percent	6	4	28.7	32	29.3
There is a protocol for monitoring and analysing network traffic to identify potential data exfiltration.	Frequency	17	17	87	89	90
	Percent	5.7	5.7	29	29.7	30
Employees are educated on the risks and methods of data exfiltration.	Frequency	21	19	72	95	93
	Percent	7	6.3	24	31.7	31
Immediate actions are taken upon detecting data exfiltration attempts to prevent data loss.	Frequency	21	14	82	97	86
	Percent	7	4.7	27.3	32.3	28.7

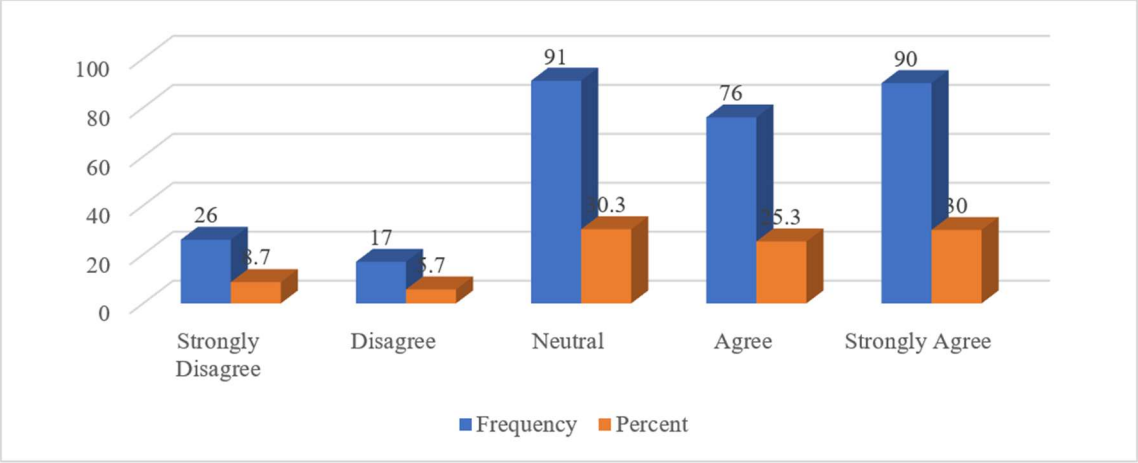

Figure 4.25: Anti-malware software is regularly updated and maintained to defend against new threats.

It is believed by most responders (as shown in Figure 4.25), that anti-malware software is updated and maintained periodically to protect against emerging threats. With 30% strongly agreeing and 25.3% agreeing, a total of 55.3% of respondents are in agreement on the regular upgrades and maintenance. While a lower number of 8.7% strongly disagree and 5.7% disagree, a considerable portion of 30.3% stays neutral. The majority of respondents seem to agree that anti-malware software is well-maintained, although others are unsure or unhappy about how often the updates are made.

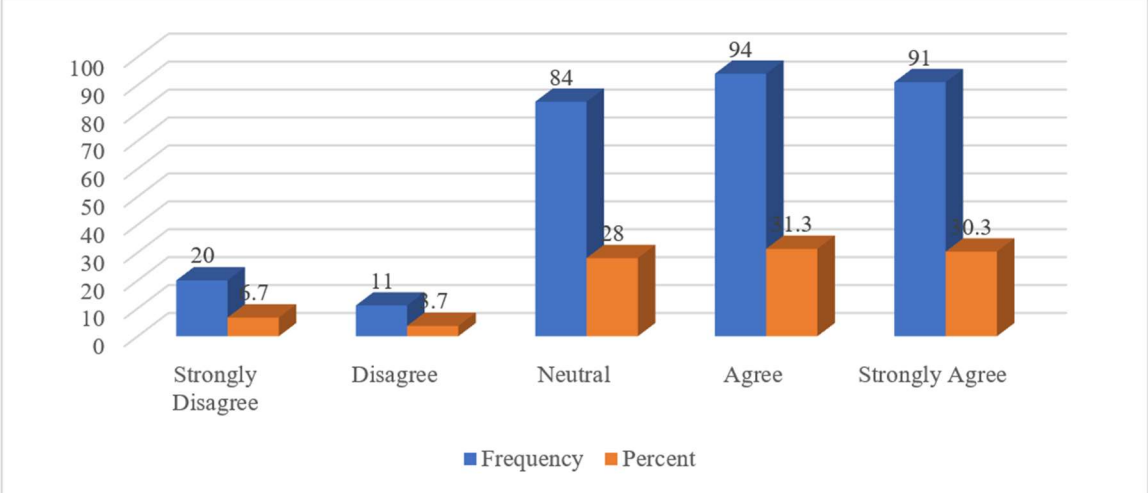

Figure 4.26: Incidents of malware infections are promptly detected, reported, and resolved.

Figure 4.26 shows that the majority of responders think that malware infections are quickly identified, reported, and fixed. A total of 61.6% of respondents confirm that these occurrences are appropriately handled, with 31.3% agreeing and 30.3% strongly agreeing. In contrast to the small percentages that strongly disagree (6.7% vs. 3.7%) and disagree (28%), a considerable majority remains indifferent. A tiny percentage of people are either unsure or dissatisfied with the way problems are handled, but most people think that malware infections are dealt with promptly.

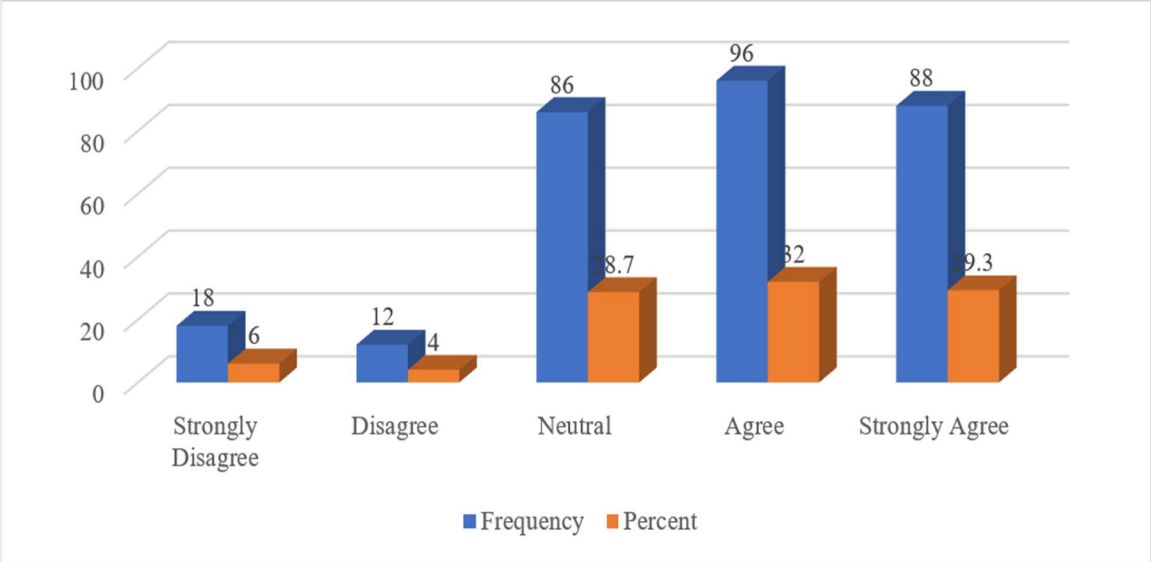

Figure 4.27: Measures are in place to detect and prevent unauthorized data exfiltration attempts.

Figure 4.27 shows that the majority of respondents think there are safeguards to identify and stop unauthorised data exfiltration attempts. The presence of such measures is confirmed by 61.3% of respondents, with 32% agreeing and 29.3% strongly agreeing. Notably, 28.7% are agnostic, whereas 6% are vehemently opposed and 4% are indifferent. This indicates that some respondents are unsure or unhappy with the current procedures in place to monitor and prevent data exfiltration attempts, even though the majority of respondents feel this way.

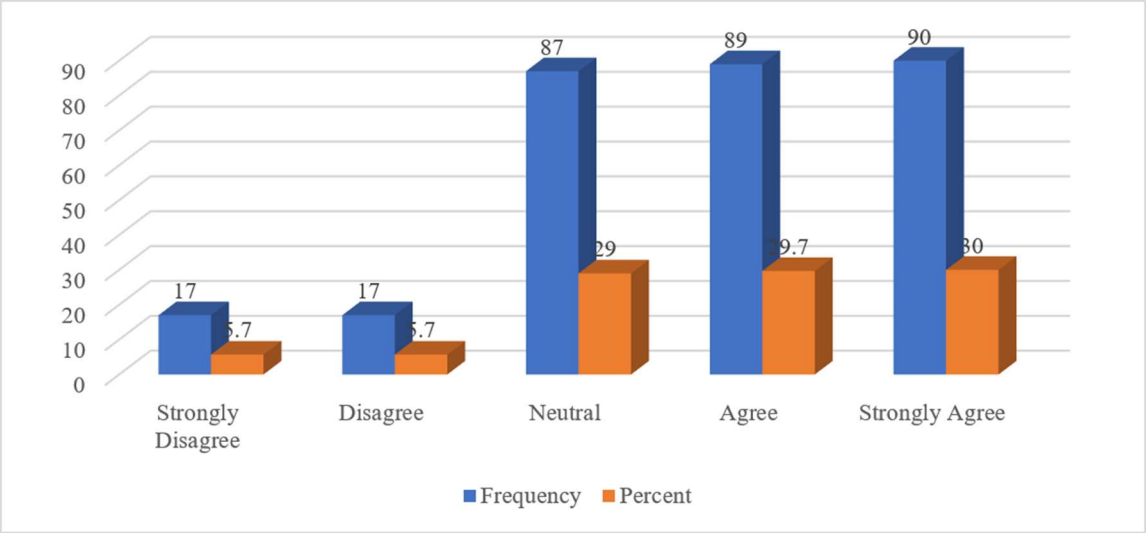

Figure 4.28: There is a protocol for monitoring and analysing network traffic to identify potential data exfiltration.

Figure 4.28 shows that most people who took the survey think there is a system in place to watch and analyse network traffic for signs of possible data leakage. With 30% strongly agreeing and 29.7% agreeing, a total of 59.7% of respondents are in agreement that such a process exists. Although just a small fraction, 29%, are agnostic, 5.7% strongly disagree, and 5.7% disagree. This indicates that although a large portion of the respondents are certain that the current methodology is sufficient to detect data exfiltration, a smaller portion are either uncertain or unhappy with it.

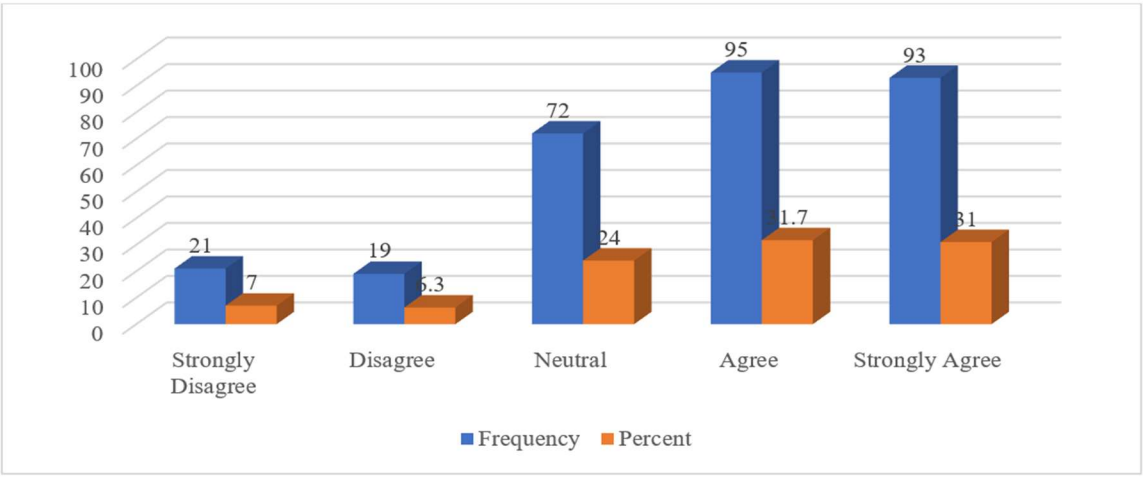

Figure 4.29: Employees are educated on the risks and methods of data exfiltration.

Figure 4.29 shows that most people think staff are informed about the dangers and ways of data exfiltration. With 31.7% in agreement and 31.0% in strong agreement, 62.7% of people who took the survey are saying that this kind of instruction is given. While a lower minority of 7% strongly disagrees and 6.3% disagree, a considerable portion stays neutral at 24%. This indicates that some respondents are unsure or think the education efforts are inadequate, even while the majority of respondents think that staff are sufficiently informed on data exfiltration.

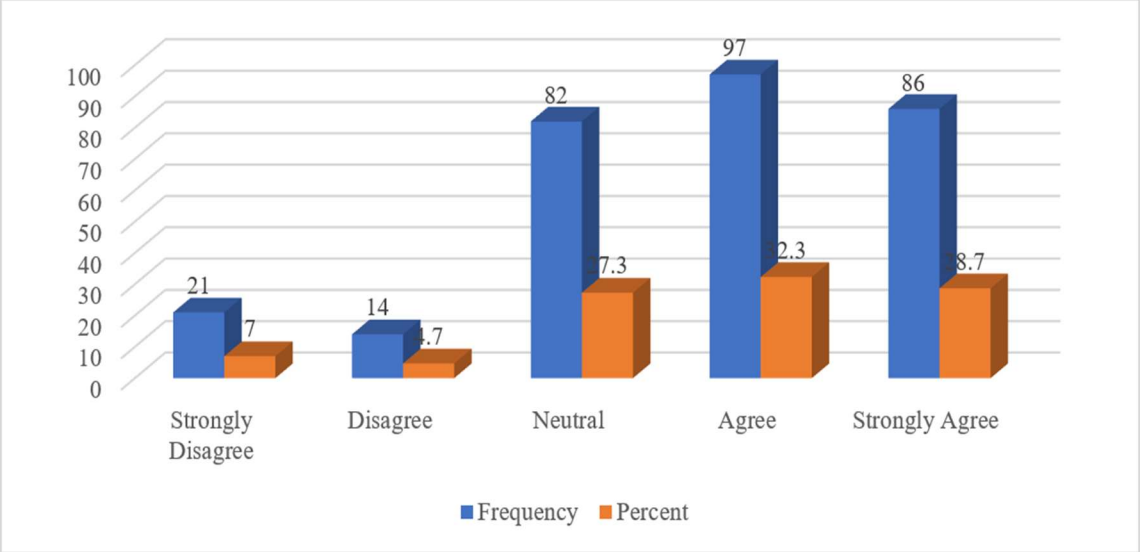

Figure 4.30: Immediate actions are taken upon detecting data exfiltration attempts to prevent data loss.

According to Figure 4.30, the majority of respondents think that measures are implemented promptly in response to the detection of data exfiltration efforts in order to avoid data loss. A total of 61% of respondents acknowledge that prompt steps are performed, with 32.3% agreeing and 28.7% strongly agreeing. Of the total, 27.3% are agnostic, while just 7% are vehemently opposed and 4.7% are indifferent. This shows that some respondents are unsure or unhappy with the measures adopted, even though the majority are confidence in the quick reaction to data exfiltration attempts.

Hypothesis Three

- **H3:** There is a significant role of Intrusion Detection Systems (IDS) in detecting and mitigating the risks of malware infections and data exfiltration in cloud environments.

Table 4.8: Correlations

			Malware Infections	Data Exfiltration	Intrusion Detection Systems (IDS)
Spearman's rho	Malware Infections	Correlation Coefficient	1.000	.027	.559**
		Sig. (2-tailed)	.	.640	.000
		N	300	300	300
	Data Exfiltration	Correlation Coefficient	.027	1.000	.560**
		Sig. (2-tailed)	.640	.	.000
		N	300	300	300
	Intrusion Detection Systems (IDS)	Correlation Coefficient	.559**	.560**	1.000
		Sig. (2-tailed)	.000	.000	.
		N	300	300	300

Interactions between intrusion detection systems (IDS), malware infections (malware), and data exfiltration from the cloud are illustrated in Table 4.8. Data exfiltration (rho = 0.560, $p < 0.01$) and malware infections (rho = 0.559, $p < 0.01$) are strongly correlated with intrusion detection systems (IDS). Malware infestations and data exfiltration can be detected and prevented with the help of intrusion detection systems. There is no evidence of data exfiltration due to malware infestations (Spearman's rho = 0.027, p = 0.640). This

provides credence to the third alternative hypothesis, which states that IDS greatly lessen these risks.

4.6 Analysis of Cloud Security Compliance

Table 4.9: Cloud Security Compliance.

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The cloud service provider (CSP) we use complies with industry standards for security.	Frequency	13	18	95	90	84
	Percent	4.3	6	31.7	30	28
Access to sensitive data in the cloud is restricted based on defined roles and permissions.	Frequency	23	15	88	91	83
	Percent	7.7	5	29.3	30.3	27.7
Our organisation regularly audits the security measures implemented by our CSP.	Frequency	24	17	91	80	88
	Percent	8	5.7	30.3	26.7	29.3
Our organisation conducts regular vulnerability assessments of our cloud infrastructure.	Frequency	26	23	75	85	91
	Percent	8.7	7.7	25	28.3	30.3
Our organisation ensures that data stored in the cloud is encrypted at rest.	Frequency	18	30	79	81	92
	Percent	6	10	26.3	27	30.7

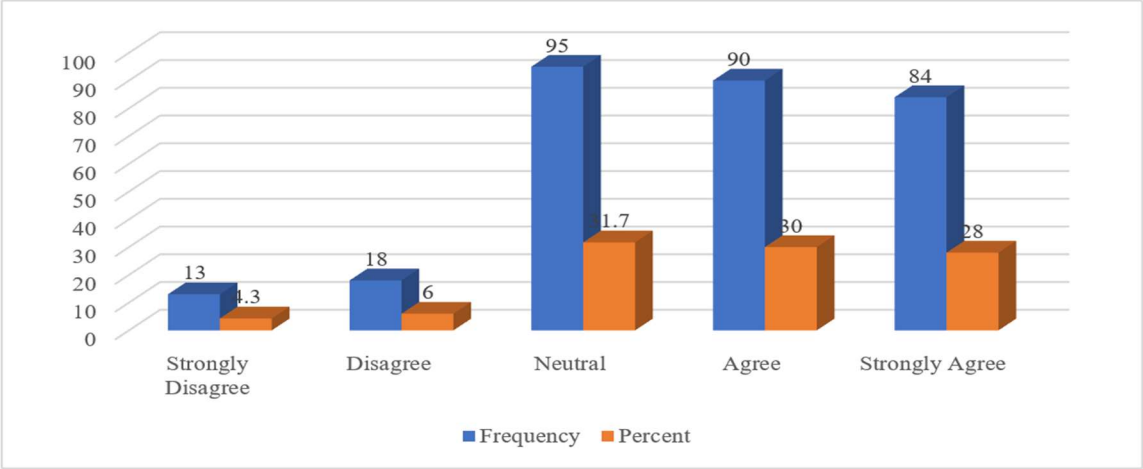

Figure 4.31: The cloud service provider (CSP) we use complies with industry standards for security.

The majority of respondents (as shown in Figure 4.31) are of the opinion that their cloud service provider (CSP) follows all applicable security regulations. Totalling 58% of respondents, 30% agree and 28% strongly agree that their CSP meets security standards. Along with lower percentages that strongly disagree (4.3%) and disagree (6%), a considerable portion (31.7%) stays neutral. The results show that although most people are sure their CSP follows all the rules when it comes to security, others aren't sure or aren't happy with how much compliance there is.

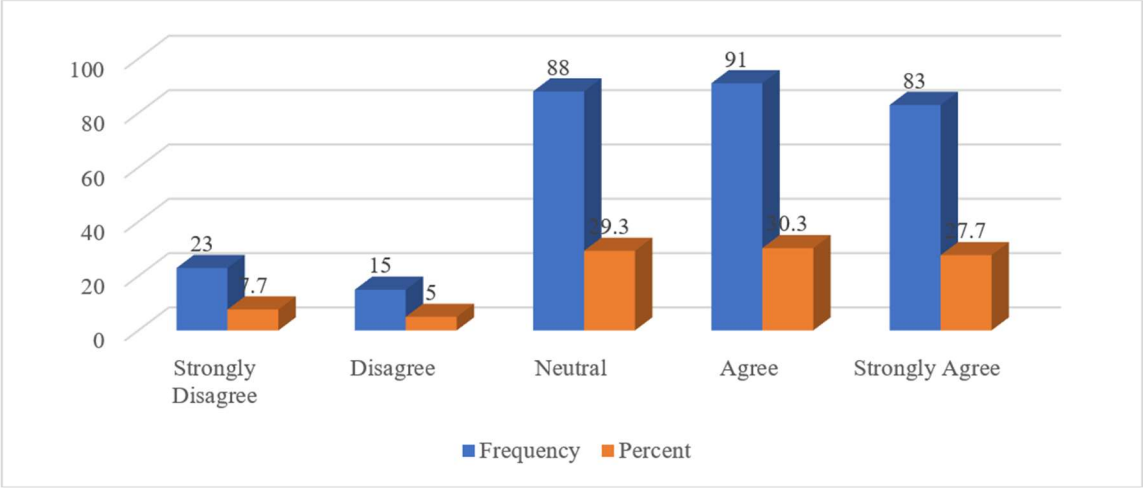

Figure 4.32: Access to sensitive data in the cloud is restricted based on defined roles and permissions.

The bulk of respondents believe that cloud data access is restricted based on predefined roles and permissions, as shown in Figure 4.32. Thirty-three percent of respondents strongly agree and twenty-seven percent agree that access is well-managed, for a total of 58 percent. While a lower amount of 7.7 percent strongly disagrees and 5.0 percent disagree, a considerable portion, 29.3 percent, stays indifferent. The majority of respondents are content with the role-based access control for sensitive data in the cloud, although a small percentage are unsure or unhappy with its implementation.

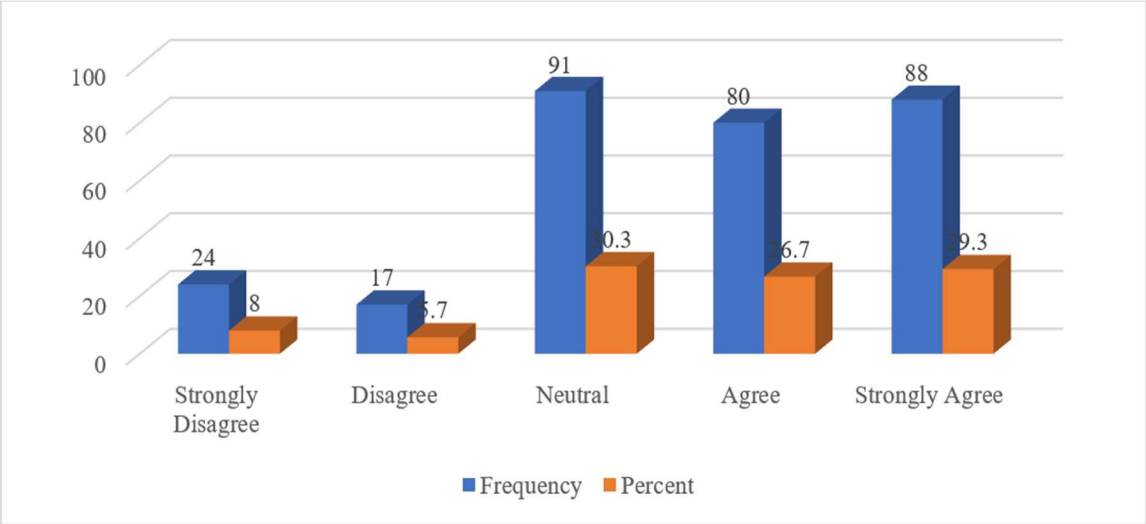

Figure 4.33: Our organization regularly audits the security measures implemented by our CSP.

Figure 4.33 shows that the majority of respondents think their company audits their CSP's security procedures on a regular basis. 56% of people who took the survey agree that security audits are done on a regular basis, with 26.7% strongly agreeing and 29.3% agreeing. Of the whole, 30.3% are agnostic, with only 8% strongly disagreeing and 5.7% disagreeing. This indicates that although a large portion of the respondents have faith in the routine auditing of CSP security measures, others are unsure or unhappy with the level of assurance they receive from these audits.

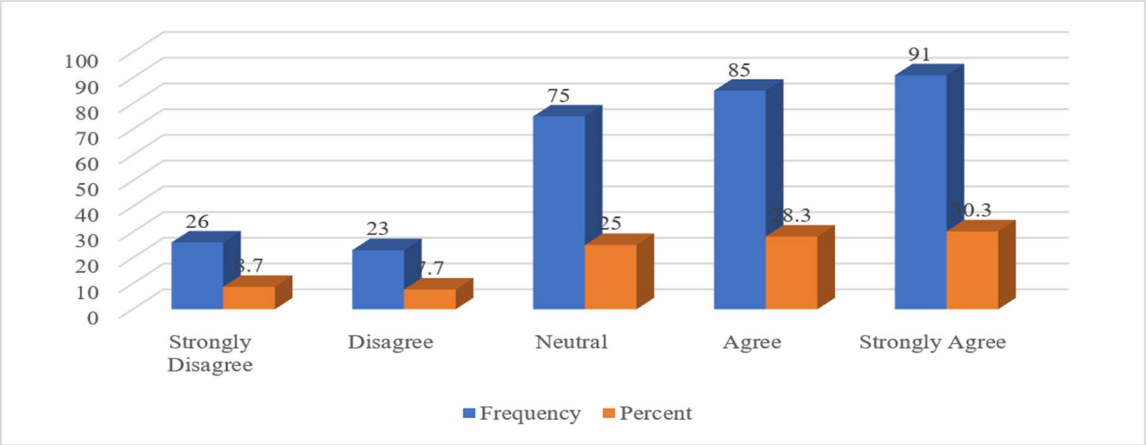

Figure 4.34: Our organisation conducts regular vulnerability assessments of our cloud infrastructure.

Figure 4.34 shows that most people who took the survey think their company checks the security of its cloud infrastructure often for vulnerabilities. A total of 58.6% of respondents acknowledge that these assessments are regularly carried out, with 28.3% agreeing and 30.3% strongly agreeing. While a lower amount of 8.7 percent strongly disagree and 7.7 percent disagree, a significant part of 25% stays neutral. This suggests that although the majority of respondents are secure in the regularity of vulnerability assessments, a small percentage are unsure or unhappy with how often or how thoroughly these assessments are conducted.

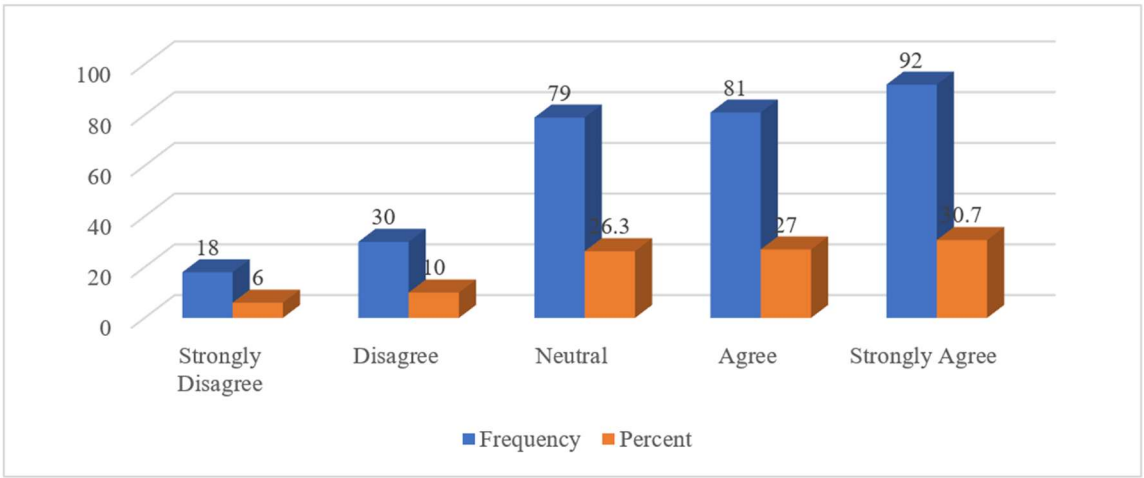

Figure 4.35: Our organization ensures that data stored in the cloud is encrypted at rest.

Figure 4.35 shows that the majority of respondents think their company takes precautions to encrypt data when it is on the cloud. With 27% in agreement and 30.7% in strong agreement, 57.7% of people who took the survey can confirm that encryption is used when data is in transit. Although just 6% strongly disagree and 10% disagree, a sizeable number (26.3% to be exact) stays undecided. It appears that there is a subset of respondents who are either unsure or unhappy with the current state of encryption for data kept in the cloud, even if the majority of respondents feel confident in this matter.

4.7 Analysis of Cloud Security Effectiveness

Table 4.10: Cloud Security Effectiveness

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Cloud security controls are consistently monitored and updated to address new vulnerabilities.	Frequency	22	17	96	75	90
	Percent	7.3	5.7	32	25	30
Our cloud security measures align with industry best practices and standards.	Frequency	18	21	92	105	64
	Percent	6	7	30.7	35	21.3
There is clear accountability for cloud security within our organization.	Frequency	22	20	93	77	88
	Percent	7.3	6.7	31	25.7	29.3
Our organisation has a proactive approach to identifying and mitigating cloud security risks.	Frequency	19	17	98	80	86
	Percent	6.3	5.7	32.7	26.7	28.7
Data integrity and confidentiality are well-maintained in our cloud environment.	Frequency	20	23	84	83	90
	Percent	6.7	7.7	28	27.7	30

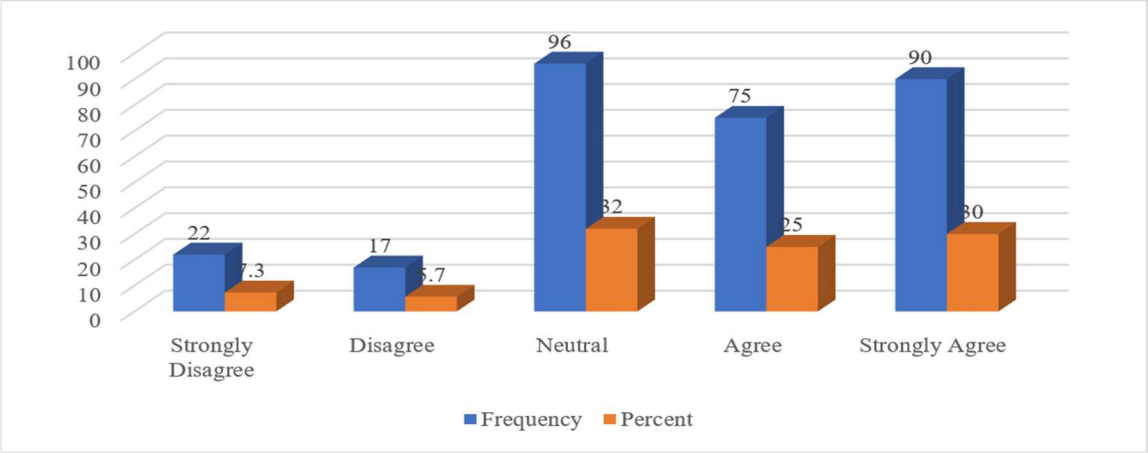

Figure 4.36: Cloud security controls are consistently monitored and updated to address new vulnerabilities.

Figure 4.36 shows that most people who took the survey think that cloud security controls are regularly checked for emerging vulnerabilities and updated accordingly. Fifty-five percent of people who took the survey agree or strongly agree that security restrictions are updated on a regular basis. While a lower amount of 7.3% strongly disagrees and 5.7% disagree, a considerable portion of 32% stays undecided. It appears that some respondents are unsure or unhappy with the frequency or efficacy of these updates, even though the majority are confident in the active maintenance and improvement of cloud security policies.

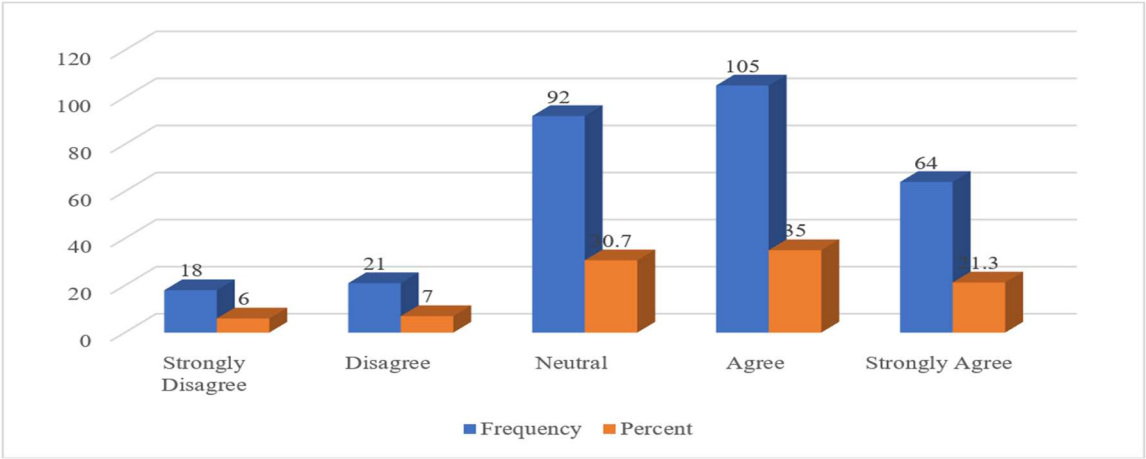

Figure 4.37: Our cloud security measures align with industry best practices and standards.

Figure 4.37 shows that the majority of respondents think their company follows all the rules and regulations when it comes to cloud security. A total of 56.3% of respondents, including 35.0% who strongly agree and 21.3% who agree, have confirmed that their cloud security measures are in line with industry standards. A sizeable minority (30.7%) maintains a neutral stance, whereas a smaller minority (6%) disagrees and 7% strongly disagree. The results show that although most respondents are content with how their cloud security measures are aligned with industry standards, others are unsure or unhappy about it.

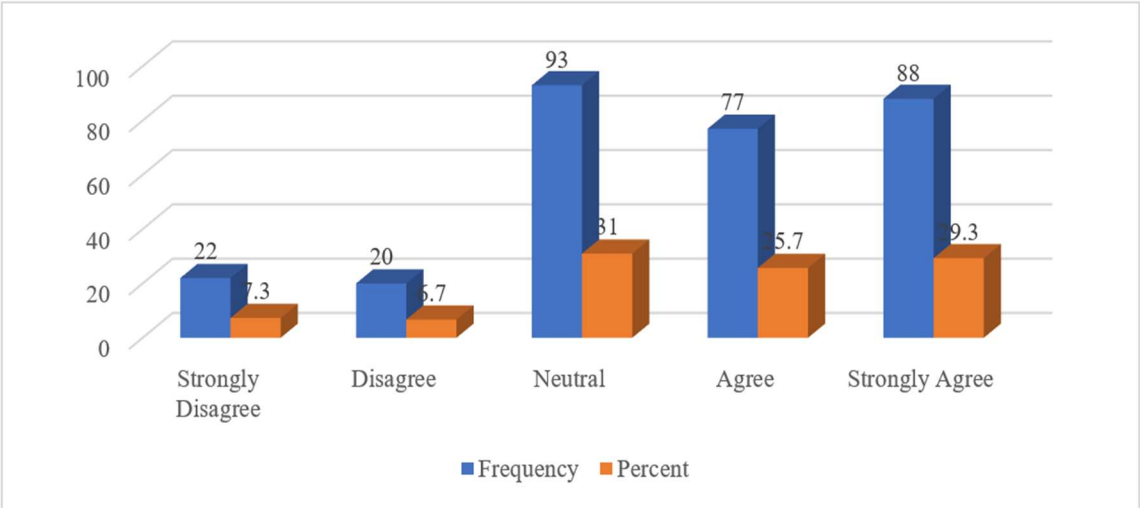

Figure 4.38: There is clear accountability for cloud security within our organisation.

Most respondents think that cloud security has an obvious responsibility inside their company, as seen in Figure 4.38. 55% of respondents acknowledge obvious accountability, with 25.7% agreeing and 29.3% strongly agreeing. While a smaller number of 7.3% strongly disagree and 6.7% disagree, a large portion stays neutral at 31%. It appears that some respondents are unsure or unhappy with their organisation's definition and management of cloud security duty, even while many are confident with the clarity of accountability.

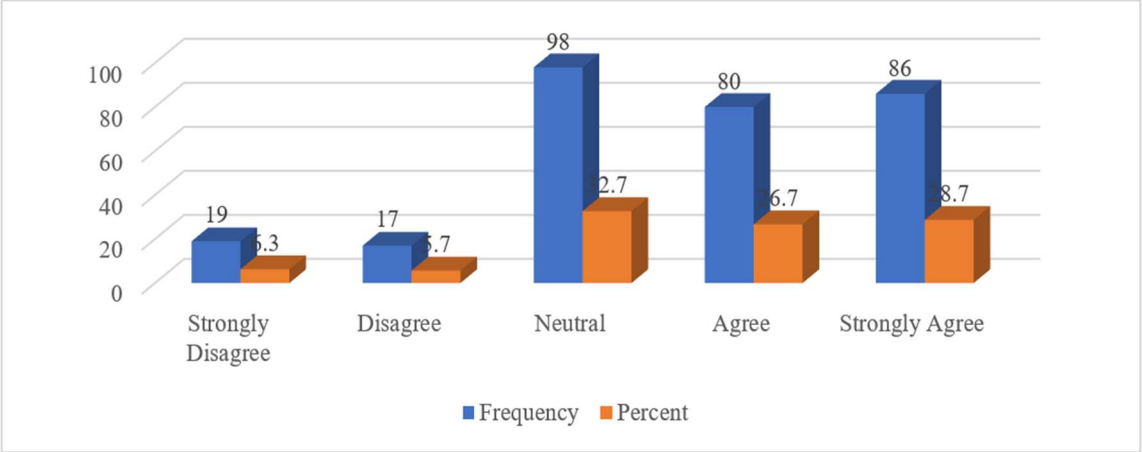

Figure 4.39: Our organisation has a proactive approach to identifying and mitigating cloud security risks.

Figure 4.39 shows that most respondents think their company is proactive in finding and reducing cloud security issues. Of those who took the survey, 55.4% claimed to be proactive, with 26.7% agreeing and 28.7% strongly agreeing. While a lower amount of 6.3% strongly disagree and 5.7% disagree, a considerable part of 32.7% stays neutral. It appears that there is a portion of the respondents who are unsure or unhappy with their organisation's proactive actions to handle cloud security concerns, even though the majority of respondents are confident in these procedures.

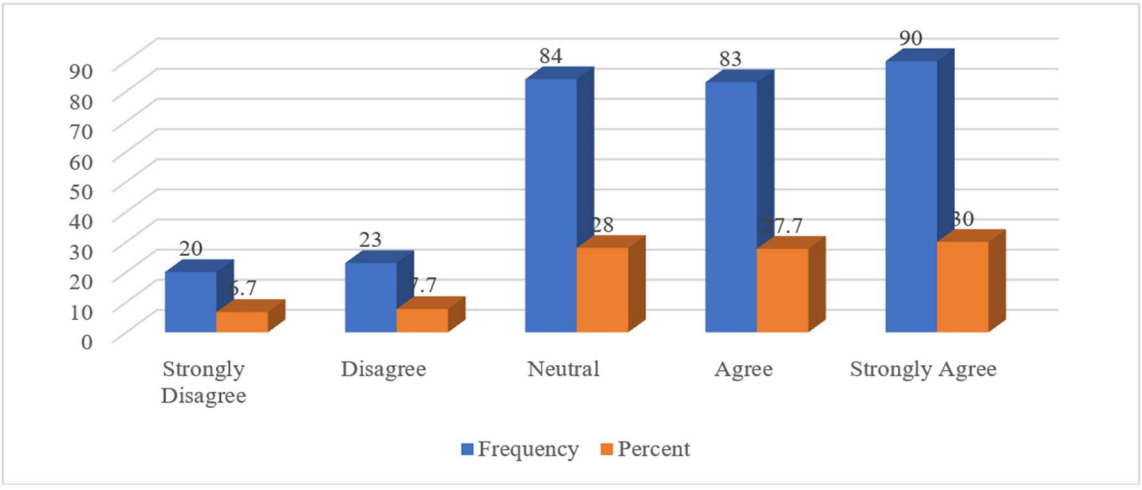

Figure 4.40: Data integrity and confidentiality are well-maintained in our cloud environment.

Figure 4.40 illustrates that the majority of responders believe that data integrity and confidentiality are well-maintained in their cloud environment. 27.7% agree and 30% strongly agree, totalling 57.7% of respondents affirming that data integrity and confidentiality are effectively protected. While a lower amount of 6.7% strongly disagrees and 7.7% disagree, a considerable portion of 28% stays neutral. This indicates that although the majority of respondents are satisfied with the current safeguards for data confidentiality and integrity in the cloud, a small percentage remain unsure or unhappy.

Hypothesis Four

- **H4:** There is a significant influence of various security solutions in cloud security compliance.

Table 4.11: Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	168.240			
Final	155.718	12.522	3	.006

Table 4.11 of the model fitting data employs a logit link to evaluate the goodness-of-fit of the logistic regression model. A -2 Log Likelihood of 168.240 is associated with the initial intercept-only model. The -2 Log Likelihood increases to 155.718 when predictors are included, indicating a more favourable fit. When compared to the intercept-only model, the predictors enhance the model's fit, as evidenced by a statistically significant Chi-Square value of 12.522 ($p = 0.006$) and three degrees of freedom. This implies that in this analysis, predictors have a considerable impact on the result variable.

Table 4.12: Goodness-of-Fit

	Chi-Square	df	Sig.
Pearson	102.358	109	.661
Deviance	85.712	109	.952

Table 4.12, labelled "Goodness-of-fit," assesses how well the logistic regression model fits the data. The results showed a deviation value of 85.712 (p = 0.952) and a Pearson Chi-Square value of 102.358 (p = 0.661) with 109 degrees of freedom. With p-values greater than 0.05 for both the observed and projected values, we can conclude that the model provides a good match to the data. This implies that the model does neither overfit or underfit and that it accurately depicts the patterns in the data.

Table 4.13: Pseudo R-Square

Cox and Snell	.041
Nagelkerke	.047
McFadden	.021

The logistic regression model's explanatory power is assessed by the pseudo-R-squared values. The following are the R-squared values for Cox and Snell: 0.047, Nagelkerke: 0.021, and McFadden: 0.021. With these numbers, it appears that the model captures some of the dependent variable's fluctuation. There may be some incongruence between pseudo-R-square values and R-square values from linear regression, but the model can still account for some of the observed variation in the data. There is a small improvement in the explanatory power of the revised Cox and Snell value, Nagelkerke.

Table 4.14: Parameter Estimates

		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Threshold	[CSC = 1.00]	-1.623	1.532	1.123	1	.289	-4.625	1.379
	[CSC = 2.00]	.041	1.237	.001	1	.974	-2.383	2.465
	[CSC = 3.00]	2.629	1.204	4.770	1	.029	.270	4.988
	[CSC = 4.00]	5.568	1.239	20.179	1	.000	3.138	7.997
Location	DE	.245	.219	1.250	1	.264	-.185	.675
	AC	.312	.178	3.064	1	.080	-.037	.660
	IDS	.484	.206	5.499	1	.019	.079	.888

A logistic regression model's parameter estimates, Table 4.14, show how security solutions affect cloud security compliance (CSC). The threshold estimations for CSC categories 1.00, 2.00, 3.00, and 4.00 differ in significance. Statistically significant estimates show that higher degrees of security solutions considerably impact compliance levels (CSC = 3.00 = 2.629, p = 0.029; CSC = 4.00 = 5.568, p < 0.001). CSC = 1.00 and 2.00 estimations are not significant (p = 0.289 and 0.974, respectively). IDS positively affect compliance (estimate = 0.484, p = 0.019), whereas Data Encryption (DE) and Access Control (AC) do not (p = 0.264 and 0.080, respectively). These findings support the alternative hypothesis (H4) that IDS solutions affect cloud security compliance.

Hypothesis Five

- **H5:** There is a significant impact of integrated security solutions on the overall effectiveness of cloud security.

Table 4.15: Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	157.080			
Final	150.409	6.671	3	.083

The model fitting information table 4.15 assesses the logistic regression model's goodness-of-fit with the logit link function. The original intercept-only model has a -2-log likelihood of 157.080. The -2 Log Likelihood increases to 150.409 once predictors are added, indicating a stronger model fit. The significance level is 0.083 and the Chi-Square value is 6.671 with three degrees of freedom. Since the p-value is more than 0.05, the model's fit is not statistically significantly superior to that of the intercept-only model.

Table 4.16: Goodness-of-Fit

	Chi-Square	df	Sig.
Pearson	147.277	109	.009
Deviance	77.251	109	.991

Table 4.16 assesses the logistic regression model's goodness-of-fit. It is possible that the model's predicted and observed values will not match, given the large number of degrees of freedom and the high Pearson Chi-Square value of 147.277 (p = 0.009). Since there are 109 degrees of freedom and the Deviance is 77.251 (p = 0.991), the model fits well without being statistically significant. Although the model fits the data well according to the Deviance statistic, the Pearson Chi-Square test reveals severe limits.

Table 4.17: Pseudo R-Square

Cox and Snell	.022
Nagelkerke	.025
McFadden	.011

Due to its limited ability to account for all possible values of the dependent variable, the model cannot be considered to have adequate explanatory power. Examples of low pseudo-R-square values include Cox and Snell = 0.022, Nagelkerke = 0.025, and McFadden = 0.011.

Table 4.18: Parameter Estimates

		Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
							Lower Bound	Upper Bound
Threshold	[CSE = 1.00]	-2.831	1.537	3.392	1	.066	-5.845	.182
	[CSE = 2.00]	-.713	1.225	.339	1	.560	-3.113	1.687
	[CSE = 3.00]	1.102	1.194	.853	1	.356	-1.237	3.442
	[CSE = 4.00]	4.112	1.222	11.329	1	.001	1.718	6.506
Location	DE	.390	.221	3.132	1	.077	-.042	.823
	AC	-.059	.178	.109	1	.742	-.407	.290
	IDS	.380	.206	3.400	1	.065	-.024	.784

A logistic regression model's parameter estimates table 4.18 shows how security solutions affect cloud security effectiveness (CSE). According to the estimations, CSE categories 1.00, 2.00, and 3.00 had no significant link with the predictors (p = 0.066, 0.560, and 0.356, respectively). However, CSE = 4.00 is significant (p = 0.001), demonstrating that stronger security solutions improve cloud security. Data Encryption (DE) has a marginally significant positive effect (estimate = 0.390, p = 0.077), Access Control (AC) is not significant (p = 0.742), and IDS is also significant (estimate = 0.380, p = 0.065). The alternative hypothesis (H4) suggests that security solutions, particularly DE and IDS, affect cloud security.

4.8 Summary of Findings

The statistical results whose analysis has been provided hereunder confirm the hypothesized relations regarding the impact of different security measures on cloud settings. To be more specific, the results show that the increased level of data encryption is likely to reduce the rates of unauthorised access and data loss significantly. A highly positive relationship with prevention of insider threats and credentialing fraud is also observed in other security measures especially access control. One research study indicates that IDS is positively related to malware and data leakage prevention to a high degree. The results of the logistic regression model comprehensively indicate that security solutions particularly the IDS have a special role to play in terms of compliance with cloud security. Therefore, the IDS and encryption of data will help enhance cloud security, especially on the compliance level. The results highlight the relevance of IDA, data encryption, and other combined security tools in managing various types of attacks and enhancing the security of CC systems.

4.9 Conclusion

The discussion in the current research brings solid proof of the efficiency of vigorous security controls in minimizing the risk and enhancing CC security. It has been established that data encryption, control access and IDS play key functions such as controlling unauthorized access, prevention of data leakage, discouragement of internal threats, countering authentication fraud, preventing malware intrusion and storage of data leakage attempts. The study further notes that in a bid to enhance the level of compliance and efficiency of cloud security, organisations should have security systems incorporated with IDS. These findings indicate that CSPs should possess an organized complex of multifaceted security that can be used to safeguard data and meet security practices. Consequently, the tolerance of the application of such security technologies will assist organisations to attain maximum levels of protection of CS against threats and ensure the privacy, integrity, and availability of the data in it.

CHAPTER V:
DISCUSSION

5.1 Discussion of Findings

Based on the study findings, it can be inferred that security solutions play a significant role in the handling of the different risks that are accredited to CC environments. As the given findings indicate, there is a distinct relationship between the data encryption, unauthorised access and the information loss. Data encryption has proven useful in terms of securing organisations against such risks. This evidence supports the hypothesis that increased encryption protects data and repels attempts at unauthorised access (Alouffi *et al.*, 2021). The connection between independent variables was highest in the case of data encryption and unauthorised access, meaning that encryption provides a strong shield (Wang, 2024). On the other hand, the coefficient determined between data encryption and data loss is moderate but positive, which shows that encryption helps to minimise data exposure (Gupta *et al.*, 2022). Additionally, as presented in the study, there is a very weak positive association between unauthorised access and data loss, which shows that these two risks have some association, and so the issues should be tackled in parallel with proper security measures.

As for the types of access controls (ACs), the results show a clear link with the decrease in the number of insider threats and credential thefts. This supports the research hypothesis that properly implemented access frameworks assist in deterring insider threats and, therefore, assist in shielding organisations' sensitive data from internal vice (Sarhan and Altwaijry, 2022). There seems to be a very low correlation between insider threats and credential theft. Nevertheless, the high correlations with access control, identify management, etc. show its necessity for managing user access and monitoring system

activity to avoid possible breaches. Such insights claim the internal threats (Rauf, Mohsen and Wei, 2023).

Intrusion Detection Systems (IDS) effectiveness of the given access control approach to enhance the cloud security and prevention also act as a critical gadget in minimising the risks involved by malware and a violation of data leakage (Attou *et al.*, 2023). The highly significant positive relationship between IDS and both malware and data exfiltration mean that these systems are capable of identifying viable security threats and stopping malware transmission or data leakage (Ullah *et al.*, 2018). However, the small correlation between malware infections and actual data exfiltration suggests that while the two risks are connected, they are not likely to happen concurrently; hence the need for individual strategies to combat each kind of threat (Souppaya and Scarfone, 2013).

The study also looks at the impact that security solutions have on cloud security compliance. According to the identified logistic regression model, some security measures as IDS have a strong influence on cloud security compliance, but on the other hand, measures such as data encryption and access control have a relatively weak impact (S Arvind, 2023). This indicates that cloud security standards' conformity is more a case of which tools are prevalent. It affirms the need for cloud practitioners to regularly upgrade their security practices in conjunction with new and increasingly strict regulatory standards (Yasar, 2024). Based on the findings of goodness-of-fit and pseudo-R-square test, the conclusions derived are that, even though the model in question demonstrates a modest level of variability in cloud security compliance, the ability to explain results in limited (Tariq *et al.*, 2017). This means that though an organisation implements security solutions to achieve compliance, other factors affect the implementation of security practices.

Finally, in assessing the integrated security solution's effectiveness, the findings indicate that IDS and data encryption have a positive and marginal impact on the cloud

security effectiveness. However, the explanatory power of the model is low. While these security measures boost security within a cloud environment, other factors define security efficiency, which is important in developing secure cloud services (Aldallal and Alisa, 2021). In light of the facts, the provided conclusion and recommendation for organisations are that organisations should implement cloud security in layers with IDS and data encryption in combination with access control; however, adequate security should be created by including bureaucratic regulations and user training and finally, constant monitoring of the cloud environment (Seth, Najana and Ranjan, 2024). .In aggregate, these findings underscore the fact that no silver bullet exists in the cloud security problem space and that employing a complex of measures is the optimal strategy of the matter (Sudalai and Smys, 2016).

5.2 Discussion of Research Question One

What are the primary cybersecurity risks related to cloud computing, and how can they be categorized?

The study identified unauthorised access, data loss, insider threats, credential theft, malware infections, and data exfiltration as critical risks in cloud environments. These security threats appear because of the joint management system and intricate cloud networks combined with expanded dependence on outside service providers. Incomplete access controls allow unauthorised users entry, while inadequate backup systems make data loss happen more easily. Internal security threats combine with stolen user credentials to demonstrate the weaknesses of privileged and fake employee access. Enhanced data security demands attention as cybercriminals shows new ways to harm enterprise cloud infrastructure.

These risks can be categorised into two broad groups: Humans create most of the security risks, but system weak points also put data at risk. Human-centric security hazards

emerge from mistakes by personnel who break rules on purpose or through carelessness (Gallagher, 2023). The system's weaknesses produce security issues like malware attacks, plus data removal results from tech issues such as incorrect settings, outdated programs, or poor network protection. Our analysis shows organisations need to combine approval systems with cryptography methods, use security monitoring technologies and teach people how to protect information safely to resist digital harms (Probst, J and Gollmann, 2010; Timonera, 2024). This categorisation provides a framework for organisations to prioritise and address specific vulnerabilities in their cloud environments.

5.3 Discussion of Research Question Two

How does data encryption mitigate the risks of unauthorized access and data loss in cloud computing environments?

Data encryption is widely applied in fighting with threats in CC space since it guarantees data confidentiality in case of data interception and unauthorised point of access to data. Encryption comes in handy when data is in motion through the Internet to other cloud servers, devices or applications, the underlying thought being that even if a bad camper picks the data, he cannot decipher it (Lord, 2019). Keeping sensitive information safe while in motion and stored is an essential component in CC systems that helps to reduce the chances of data loss and illegal access. Data is rendered unintelligible and can only be deciphered by authorised individuals with the proper decryption keys. This process safeguards information from unauthorised access, even if an attacker intercepts or breaches the system (Sriram, 2023).

Through cloud data encryption, organisations protect their information better because encrypted data becomes useless when shared without the proper key. Using encryption improves organisations' ability to meet regulations better while strengthening their overall data protection systems (Lord, 2019). Combined with strict access rules and

proper key storage methods, encryption forms a strong security perimeter that protects the data even when an attacker breaches the system or backups are lost.

5.4 Discussion of Research Question Three

How effective are access control mechanisms in preventing insider threats and credential theft in cloud computing systems?

Person-to-person control is greatly essential and efficient in minimising internal threats as well as aggressive credential manipulations in cloud-based systems because control dictates who has the freedom to access what data inside the cloud.

Access control systems protect CS by stopping both internal security violations and unauthorised password use. The security system manages who can access and work with valuable assets within its boundaries (Frontegg, 2022). The research proves that adding access control helps defend against insider threats and prevents unauthorised users from taking sensitive information.

Their results show that though insider threats and credential theft are linked together, they remain mostly separate risks. To address security challenges effectively, organisations need to put together access controls with ongoing monitoring and quick incident response practices (Kent and Murugiah Souppaya, 2019; Golightly *et al.*, 2023). The research shows access controls deliver high-security value when organisations use them alongside other security systems and policy enhancements.

5.5 Discussion of Research Question Four

What is the role of Intrusion Detection Systems (IDS) in detecting and mitigating the risks of malware infections and data exfiltration in cloud environments?

The Intrusion Detection System (IDS) detects and prevents cloud vulnerabilities by locating unproductive access and policy violations in traffic over the networks and

computers. IDS can be used to monitor all the traffic across the network and all system activity, which could provide hints as to the presence of malware or data exfiltration efforts on the network or systems. Besides the inbound and outbound traffic, IDS can detect the presence of abnormal traffic activities, including high bandwidth data transmission or relaying of messages to and out of identified malicious IPs, which point to the existence of Trojans and or viruses and unauthorised information transfer.

IDSs employ signature matching, whereby IDSs log current activity against the defined attack signature. This helps to alert the system administrator within a short time to possible infections that belong to certain categories or particular modes of attack (Holm, 2014). If you're looking for known vulnerabilities and current malware, signature-based detection is your best bet. By examining unusual data transfer patterns, it can detect data exfiltration, which includes the movement of information to unapproved routes. Such systems can also detect data movement out of well-defined corporate parameters, which is useful when dealing with leaks to unauthorised persons (Martinez, 2024).

Subsequently, malware which has gained a foothold may seek to move around the network laterally. IDS systems can identify similar movement relating to this abhorrence, including any form of traffic flow between the hosts or attempts to access encoded data over the different cloud resources (fortinet, 2023). Thus, IDS prevent the infections from extending their damage within the cloud environment by identifying all these activities.

5.6 Discussion of Research Question Five

How do various security solutions influence cloud security compliance?

A range of security measures serves as critical in enhancing cloud security compliance by supplying the right equipment, measures, and even checks that help meet typical legislations as well as standards that apply to CC architecture (Aqua, 2024). This is

why cloud security compliance has proved important in ensuring that data privacy and integrity are maintained to meet the shareholders' expectations.

The study reveals that various security solutions significantly influence cloud security compliance by ensuring adherence to industry standards and regulatory requirements. IDS emerged as a particularly strong predictor of compliance, providing robust monitoring capabilities to detect and prevent potential security breaches (Shah and Singh, 2024). While data encryption and access control mechanisms also contribute to compliance, their impact was less pronounced in this study (BluueXp, 2019).

The findings demonstrate the necessity of a combined security strategy, which includes intrusion detection systems (IDS), encryption, and access control. The adherence can also be enhanced through periodic vulnerability assessment and in line with the standard procedures. Finally, the sound security solutions improve the capacity of an organisation to adjust to the standards of compliance and risks reduction in the cloud environment.

5.7 Discussion of Research Question Six

What is the impact of integrated security solutions on the overall effectiveness of cloud security?

Security Solutions are better at improving the performance of cloud security because they integrate the protection measures in a single cohesive system (Gangwani *et al.*, 2023). The study shows that integrating security systems enhances overall protection of the cloud as it addresses many of the weak points at the same time. IDS and DE became the key components of a sophisticated security system design.

This inquiry confirms that the integration of security tools is always effective to ensure that the entire cloud protection mechanism is more effective in comparison to single methodologies. It is through this synergy that organisations are in a good position to

identify and mitigate risks proactively, stay in compliance with regulations and react effectively in case of security incidents.

Even though AC alone was not as significant in this study, its contribution to an integrated framework is imperative. Thus, it is important to embrace integrated security solutions to improve and maximise the effectiveness of cloud security and provide a reliable and durable environment against the changing cyber-threats.

CHAPTER VI:

SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

6.1 Summary

The combination of security in CC environments is a basic way of enhancing security. The paper also highlights the benefits of these solutions to added risk management and protection by integrating different levels and tools that enhance security such as firewalls, IDS, and Data Loss Prevention (DLP). As a result of this integration, the interventions, preventations and total regulation of the threats are effective which minimise many points on the cloud infrastructure.

One of the key findings emphasises the need to increase visibility by tracking the process. Consolidated security solutions offer management consoles so that an organisation can manage the different aspects of its cloud security on one platform. Lastly, centralised visibility ensures that potential threats and outliers of the normal ranges are detected early enough to respond to threats early enough to prevent breaches. This way, the chapter also shows how integrated systems lower the concern of complexity as they consolidate several security processes. The meeting of routine security functions, including patching and vulnerability scans, improves functional effectiveness. It frees human resources from the ordinary, mundane, repetitive security routine tasks that may otherwise have been executed by the human personnel, with less efficiency, guarded more by complacency than by professional skill, technological onboard, and frequently violating key security policies due to the monotony of their routine.

Finally, the study outlines the future of integrated security solutions in terms of scalability, flexibility, and integration, noting that security solutions are to be elastic to market environments and scale with cloud ecosystems. These solutions scale up or scale out when a company needs to increase data storage/sharing capacity or processor power

and do so without reducing system security or performance in any way, making them perfect for the flexible and ever-changing cloud environment. The novelty of integrated security systems is a fourth discovery as they reduce the costs of purchasing, supporting, and training individual security gadgets since they are in a single system.

Another important topic discussed within the research is connected to using integrated solutions to enhance reaction time to incidents. By incorporating data correlating and automating capabilities, these systems help to accurately detect, minimise, contain, and even recover from such breaches more quickly, thus lowering the risks of breaches. Compliance facilitation is another factor whereby integrated solutions come equipped with tools for meeting compliance needs and making auditing and reporting easy.

The findings hereunder may have greater relevance to organisations that use hybrid or even multi-cloud environments, whereby the integration that the vendors provide helps in delivering consistent policies or controls across the various interfaces and thereby assists in mitigating security vulnerabilities. Moreover, such solutions are enriched by the integration of AI and ML to prevent and mitigate uncertainties that have the potential to turn into threats affecting an organisation in the long run.

6.2 Implications

The implications of this study are as follows:

- **Enhanced Risk Management and Threat Mitigation:** Cloud security solutions have a beneficial impact on risk management by organisations. This appears to be actual as with the combination of IDSs, firewalls, and encryption, both external and internal threats are stopped to the businesses in a more effective way. Incorporating this solution, one is less likely to face breaches, data loss, and malware intrusion, which, in its turn, will provide a secure cloud infrastructure.

- **Operational Efficiency and Cost Savings:** This is largely due to the fact that the integrated security systems provide a single system that monitors a variety of areas as far as security in a facility is concerned. This is not only helpful in managing the various security tools, but also reduces the aspects of operation of the security tools in terms of training, maintenance, and acquisition. The cloud environment enables companies to optimise their resources better and enhance security characteristics of their organisations and their value at an optimal cost that is suboptimal.
- **Regulatory Compliance and Reporting:** When it comes to companies that handle large volumes of information or companies in highly recognised industries, integrated solutions bring about comprehensive benefits concerning the compliance levels on security. Tools that are integrative, to include audit logs, monitors, and reports, help to show that the company has complied with the set requirements, such as GDPR, HIPAA, or PCI-DSS, hence reducing legal implications.
- **Improved Incident Response and Recovery**: Integrated security solutions allow organisations to identify and address security issues quickly. Authority of the sources and the correlation, real-time notifications, and small-sized dashboards improve the incidence of identifying and consequently rectifying the incident, making it faster to address. This also reduces the effects of security breaches and overall general security of the system.
- **Scalability and Flexibility for Growing Cloud Environments:** This security solution is also integrated and can be useful in the situation when cloud environments grow in scale and structure and demand additional security levels. It is highly adaptive to alter the security tools and policies depending on

the variations in the requirements, e.g., the volumes of data, the resources involved in the computation, or the integration of additional clouds as the organisational need demands with or without compromising the security. Scalability is also significant to ensure that security infrastructure can be scaled as cloud structures of the organisation are developed.

- **Cross-Platform Security Consistency:** It is particularly so in the case of hybrid or multi-cloud, where cloud providers and cloud platforms are used differently. Then, integrated security solutions offer uniform security controls and policies across the platform. This, when deprived of the security breach between the systems and all components of the cloud environment are secured to the same extent.

6.3 Recommendations for Future Research

- **Exploring the Integration of Advanced AI and Machine Learning in Security Solutions:** To some extent, future work should consider how these technologies can be leveraged further to enhance cloud security mechanisms. Analysing its application in predictive modelling, anomaly detection, and the automation of responses to security breaches helps researchers uncover the potential for increasing the efficiency of protecting cloud infrastructures as part of the future generation of cloud security systems.
- **Assessment of Multi-Cloud and Hybrid Cloud Security Solutions:** Since multi-cloud and hybrid cloud models are gradually becoming the tendency among organisations, the usefulness of integrated security solutions should also be assessed in future studies involving these models. Studies could focus on issues – for instance, the difficulty of implementing the same security measures

across different cloud environments – and present workable guidelines on enhancing security management in an environment with multiple clouds.

- **Impact of Emerging Threats on Integrated Security Frameworks:** As to new trends in the threat landscape, research should be devoted to the impact of new types of threats, including quantum computing, ransomware, and APTs on integrated security solutions. It can bring significant useful information on how it is possible to develop viable ways to apply security solutions for disrupting threats that originate from emerging new threat modes in CC facilities.
- **User Experience and Usability of Integrated Security Solutions:** Like in the present study, integrated security solutions offer the platform of manageable and holistic security; future studies in this area should conduct surveys on the usability of integrated security solutions as seen by an end consumer. Maybe, research might be conducted to analyze the complexity of such solutions in the context of deployment, management as well as the end-users /consumers of the solutions. Research might attempt to idealize the technology to an extent that the complexity it brings about in the security systems would not affect its effectiveness and efficiency.
- **Evaluation of Compliance in Global Cloud Deployments:** The potential concerns of research that can be explored are the compliance matters with the various international and regional security policies on the use of integrated security solutions on clouds. Analysis of how security solutions can meet specific compliance requirements like GDPR, CCPA, and HIPAA in multiple regions will ensure that organisations are equipped with the necessary skills on how they will stay compliant even when they go to the cloud.

- **Economic Impact of Integrated Cloud Security on Business Performance:** It could also be possible to investigate the effectiveness of integrated security solutions and the cost of securing a cloud environment. In this way, the cost-benefit analysis could help researchers learn how integrated security investments affect business results, such as revenues, client loyalty, and future company cost savings. The knowledge of the return on investment (ROI) will assist businesses in their decision-making concerning security measures.

6.4 Conclusion

Security solutions in the context of CC platforms represent an important aspect of protecting data, compliance, and minimising the rising cybercrime threats. This study reveals that enclosing measures such as encryption, access control, IDS and real-time threat intelligence comprehensively protect from intrusion, malware attacks, and data leakage. While more organisations are adopting cloud technologies for scalability, flexibility, and reducible costs, a proper and effective information security solution is inevitably required.

However, as it stands, there are still some complications, which include the complexity of policies in multi-cloud and hybrid cloud arrangements, complicated compliance with different regulatory frameworks and avoiding new risks. Cyber threats are fluid and ever-changing by nature, which means that security, technologies and processes have to be dynamic and adapt to constantly moving goalposts.

Hence, there is a need for further research to investigate the application of newer and emerging AI technology, the security requirements of the specific industries, the privacy preservation measures used, and the cost-benefit analysis of cloud security investment. By tackling these aspects, organisations will be equipped to handle challenges that relate to cloud security, achieve the long-term viability of the business, and improve trust in cloud solutions. In conclusion, the efficient deployment of integrated security

solutions will remain a prerequisite for future development and further advancement of CC as a business enabler and a secure environment for organisations' IT projects and operations.

REFERENCES

A, R. *et al.* (2023) 'Enhanced Cloud Storage Encryption Standard for Security in Distributed Environments', *Electronics*, 12(3), p. 714. Available at: https://doi.org/10.3390/electronics12030714.

Abayomi, J. (2022) 'Emerging Cloud Computing Security Threats', *Research Gate* [Preprint], (October 2021).

Abdullayeva, F. (2023) 'Cyber resilience and cyber security issues of intelligent cloud computing systems', *Results in Control and Optimization*, 12, pp. 1–16. Available at: https://doi.org/10.1016/j.rico.2023.100268.

Abid, R. *et al.* (2023) 'RETRACTED ARTICLE: An optimised homomorphic CRT-RSA algorithm for secure and efficient communication', *Personal and Ubiquitous Computing*, 27(3), pp. 1405–1418. Available at: https://doi.org/10.1007/s00779-021-01607-3.

Abraham, D. (2009) 'Why 2FA in the cloud?', *Network Security*, 2009(9), pp. 4–5. Available at: https://doi.org/10.1016/S1353-4858(09)70097-2.

Abrahams, T. *et al.* (2024) 'A Review of Cybersecurity Strategies in Modern Organizations: Examining The Evolution and Effectiveness of Cybersecurity Measures for Data Protection', *Computer Science & IT Research Journal*, 5, pp. 1–25. Available at: https://doi.org/10.51594/csitrj.v5i1.699.

Abroshan, H. (2021) 'A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms', *International Journal of Advanced Computer Science and Applications*, 12(6), pp. 31–37. Available at: https://doi.org/10.14569/IJACSA.2021.0120604.

Abu-Alhaija, M. (2020) 'Cyber security: Between challenges and prospects', *ICIC Express Letters, Part B: Applications*, 11(11), pp. 1019–1028. Available at:

https://doi.org/10.24507/icicelb.11.11.1019.

Adee, R. and Mouratidis, H. (2022) 'A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography', *Sensors*, 22(3). Available at: https://doi.org/10.3390/s22031109.

Ahi, A.A. *et al.* (2022) 'Advanced technologies and international business: A multidisciplinary analysis of the literature', *International Business Review*, 31(4), p. 101967. Available at: https://doi.org/10.1016/j.ibusrev.2021.101967.

Ahlstrom, D. and Bruton, G.D. (2001) 'Learning from successful local private firms in China: Establishing legitimacy', *Academy of Management Perspectives*, 15(4), pp. 72–83. Available at: https://doi.org/10.5465/ame.2001.5897661.

Ahmad, W. *et al.* (2022) 'Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey', *Electronics*, 11(1), p. 16. Available at: https://doi.org/10.3390/electronics11010016.

Ahmadi, A.N. (2021) 'A Comprehensive Cybersecurity Framework for Afghanistan's Cyberspace', *International Journal of Engineering Applied Sciences and Technology*, 6(2), pp. 213–230. Available at: https://doi.org/10.33564/IJEAST.2021.v06i02.032.

Ahmed, H.A.S. *et al.* (2017) 'A review of challenges and security risks of cloud computing', *Journal of Telecommunication, Electronic and Computer Engineering*, 9(1–2), pp. 87–91.

Akherfi, K., Gerndt, M. and Harroud, H. (2018) 'Mobile cloud computing for computation offloading: Issues and challenges', *Applied Computing and Informatics* [Preprint]. Available at: https://doi.org/10.1016/j.aci.2016.11.002.

Al-khafajiy, M. *et al.* (2020) 'COMITMENT: A Fog Computing Trust Management Approach', *Journal of Parallel and Distributed Computing* [Preprint]. Available at:

https://doi.org/10.1016/j.jpdc.2019.10.006.

Al-Khater, W.A. *et al.* (2020) 'Comprehensive review of cybercrime detection techniques', *IEEE Access* [Preprint]. Available at: https://doi.org/10.1109/ACCESS.2020.3011259.

Alani, M.M. (2014) 'Securing the Cloud: Threats, Attacks and Mitigation Techniques', *Journal of Advanced Computer Science & Technology* [Preprint]. Available at: https://doi.org/10.14419/jacst.v3i2.3588.

Albakri, S.H. *et al.* (2014) 'Security risk assessment framework for cloud computing environments', *Security and Communication Networks*, 7(11), pp. 2114–2124. Available at: https://doi.org/10.1002/sec.923.

Aldallal, A. and Alisa, F. (2021) 'Effective Intrusion Detection System to Secure Data in Cloud Using Machine Learning', *Symmetry*, 13, pp. 1–26. Available at: https://doi.org/10.3390/sym13122306.

Algarni *et al.* (2021) 'Quantitative Assessment of Cybersecurity Risks for Mitigating Data Breaches in Business Systems', *Applied Sciences*, 11(8), p. 3678. Available at: https://doi.org/10.3390/app11083678.

Alhenaki, L. *et al.* (2019) 'A Survey on the Security of Cloud Computing', in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, pp. 1–7. Available at: https://doi.org/10.1109/CAIS.2019.8769497.

Ali, A. (2018) 'Electronic Contract and Consumer Protection Issues in India; Emerging Legal Challenges and Remedial Measures', *International Journal of Research in Social Sciences and Humanities*, pp. 2249–2496.

Ali, H. (2018) 'Securing Cloud Storage: Encryption, Access Controls, and Data Loss Prevention', *Research Gate* [Preprint], (July).

Ali, M., Khan, S.U. and Vasilakos, A. V. (2015) 'Security in cloud computing: Opportunities and challenges', *Information Sciences*, 305, pp. 357–383. Available at: https://doi.org/10.1016/j.ins.2015.01.025.

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.

Allioui, H. and Mourdi, Y. (2023) 'Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey', *Sensors*, 23(19). Available at: https://doi.org/10.3390/s23198015.

Almaiah, M.A. *et al.* (2024) 'Classification of Cybersecurity Threats, Vulnerabilities and Countermeasures in Database Systems', *Computers, Materials & Continua*, 81(2), pp. 3189–3220. Available at: https://doi.org/10.32604/cmc.2024.057673.

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.

Alrehaili, N. and Mutaha, A. (2020) 'Cloud Computing Security Challenges', *IARJSET*, 7(8), pp. 120–123. Available at: https://doi.org/10.17148/IARJSET.2020.7817.

Ansari, M.F. (2022) 'A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs', *International Journal of Smart Sensor and Adhoc Network.*, pp. 1–8. Available at: https://doi.org/10.47893/IJSSAN.2022.1212.

Aqua (2024) '10 Cloud Security Standards You Must Know About'.

Arani, H.V. *et al.* (2023) 'How to charge in servicizing: Per period or per use?', *European Journal of Operational Research* [Preprint]. Available at: https://doi.org/10.1016/j.ejor.2022.05.002.

ARAVINDA A KUMAR and Divya TL (2024) 'Security measures implemented in RESTful API Development', *Open Access Research Journal of Engineering and Technology* [Preprint]. Available at: https://doi.org/10.53022/oarjet.2024.7.1.0042.

Arce, I. *et al.* (2014) 'Avoiding the top 10 software security design flaws', *IEEE Computer Societys Center for Secure Design* [Preprint].

Armbrust, A. Fox, and R. Griffith, M. (2009) 'Above the clouds: A Berkeley view of cloud computing', *University of California, Berkeley, Tech. Rep. UCB* [Preprint]. Available at: https://doi.org/10.1145/1721654.1721672.

Armbrust, M. *et al.* (2010) 'A view of cloud computing', *Communications of the ACM* [Preprint]. Available at: https://doi.org/10.1145/1721654.1721672.

Arvidsson, B., Johansson, J. and Guldåker, N. (2021) 'Critical infrastructure, geographical information science and risk governance: A systematic cross-field review', *Reliability Engineering and System Safety* [Preprint]. Available at: https://doi.org/10.1016/j.ress.2021.107741.

Ashari, A. and Setiawan, H. (2011) 'Cloud Computing : Solusi ICT ?', *Sriwijaya Journal of Information Systems*, 3(2).

Attou, H. *et al.* (2023) 'Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques', *Big Data Mining and Analytics*, 6(3), pp. 311–320. Available at: https://doi.org/10.26599/BDMA.2022.9020038.

Babu, B.M. and Bhanu, M.S. (2015) 'Prevention of Insider Attacks by Integrating Behavior Analysis with Risk based Access Control Model to Protect Cloud', *Procedia Computer Science*, 54, pp. 157–166. Available at: https://doi.org/10.1016/j.procs.2015.06.018.

Bagherzadeh, L. *et al.* (2020) 'Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions', in *2020 International*

Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE). IEEE, pp. 1–8. Available at: https://doi.org/10.1109/CISPSSE49931.2020.9212195.

Baker, T. *et al.* (2013) 'Intention-oriented programming support for runtime adaptive autonomic cloud-based applications', *Computers and Electrical Engineering* [Preprint]. Available at: https://doi.org/10.1016/j.compeleceng.2013.04.019.

Baldini, I. *et al.* (2017) 'Serverless computing: Current trends and open problems', in *Research Advances in Cloud Computing*. Available at: https://doi.org/10.1007/978-981-10-5026-8_1.

Baron, J. *et al.* (2014) 'How to withstand mobile virus attacks, revisited', in *Proceedings of the Annual ACM Symposium on Principles of Distributed Computing*. Available at: https://doi.org/10.1145/2611462.2611474.

Barrow, P. and Kumari, R. (2016) 'Security in Cloud Computing For Service Delivery Models: Challenges and Solutions', *Journal of Engineering Research and Applications www.ijera.com*, 6(2), pp. 76–85.

Batar, S. (2021) 'An overview on cyber crime', *Asian Journal of Multidimensional Research*, 10(12), pp. 167–172. Available at: https://doi.org/10.5958/2278-4853.2021.01202.7.

Belal, M.M. and Sundaram, D.M. (2022) 'Comprehensive review on intelligent security defences in cloud: Taxonomy, security issues, ML/DL techniques, challenges and future trends', *Journal of King Saud University - Computer and Information Sciences* [Preprint]. Available at: https://doi.org/10.1016/j.jksuci.2022.08.035.

Bhadra, S. (2020) 'Cloud Computing Threats and Risks: Uncertainty and Unconrollability in the Risk Soceity', *Journal of Emerging Technologies and Innovative Research (JETIR)*, 7(2), pp. 1047–1070.

Bishop, M. *et al.* (2017) 'Cybersecurity Curricular Guidelines', in *IFIP Advances in Information and Communication Technology*, pp. 3–13. Available at: https://doi.org/10.1007/978-3-319-58553-6_1.

Blessing, M. (2024) 'Cloud Encryption Strategies and Key Management Author : Moses Blessing Date : 2 nd September , 2024', *Research Gate* [Preprint], (September).

BluueXp (2019) 'Data Compliance for Regulations Around the World'.

Brodkin, B.J. (2008) 'Gartner : Seven cloud-computing security risks', *InfoWorld* [Preprint].

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.

Catteddu, D. (2010) 'Cloud Computing: Benefits, Risks and Recommendations for Information Security', in, pp. 17–17. Available at: https://doi.org/10.1007/978-3-642-16120-9_9.

Catteddu, D. and Hogben, G. (2009) 'The European Network and Information Security Agency (ENISA)', *Computing* [Preprint].

Cearley, D. *et al.* (2019) 'Gartner Top 10 Strategic Technology Trends for 2020 - Smarter With Gartner', *Gartner* [Preprint].

Cerezo, A.I., Lopez, J. and Patel, A. (2007) 'International cooperation to fight transnational cybercrime', in *Proceedings - 2nd International Annual Workshop on Digital Forensics and Incident Analysis, WDFIA 2007*. Available at: https://doi.org/10.1109/WDFIA.2007.4299369.

Chang, E.C. and Xu, J. (2008) 'Remote integrity check with dishonest storage server', in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial*

Intelligence and Lecture Notes in Bioinformatics). Available at: https://doi.org/10.1007/978-3-540-88313-5_15.

Chen, F. *et al.* (2022) 'IoT Cloud Security Review', *ACM Computing Surveys*, 54(4), pp. 1–36. Available at: https://doi.org/10.1145/3447625.

Chinazor Prisca Amajuoyi, Luther Kington Nwobodo and Mayokun Daniel Adegbola (2024) 'Transforming business scalability and operational flexibility with advanced cloud computing technologies', *Computer Science & IT Research Journal* [Preprint]. Available at: https://doi.org/10.51594/csitrj.v5i6.1248.

Cloud, O. (2012) 'Open Cloud', *Technology* [Preprint].

Computing, M. (2014) 'RESEARCH ARTICLE CYBER SECURITY -Trends and Challenges Abstract : Cybersecurity is a necessary consideration for information technology as well as Internet services . We need', 3(2), pp. 586–590.

Coppolino, L. *et al.* (2016) 'Cloud security : Emerging threats and current solutions', *Computers and Electrical Engineering*, 0, pp. 1–15. Available at: https://doi.org/10.1016/j.compeleceng.2016.03.004.

Cormack, G. V. (2006) 'Email spam filtering: A systematic review', *Foundations and Trends in Information Retrieval* [Preprint]. Available at: https://doi.org/10.1561/1500000006.

Csa (2019) *Cloud Security Alliance*, *httpwwwcloudsecurityallianceorg*.

Daalen, O.L. van (2023) 'The right to encryption: Privacy as preventing unlawful access', *Computer Law & Security Review*, 49, p. 105804. Available at: https://doi.org/10.1016/j.clsr.2023.105804.

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

Dillon, T., Wu, C. and Chang, E. (2010) 'Cloud Computing: Issues and Challenges', in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*. IEEE, pp. 27–33. Available at: https://doi.org/10.1109/AINA.2010.187.

Djebbar, F. and Nordström, K. (2023) 'A Comparative Analysis of Industrial Cybersecurity Standards', *IEEE Access*, 11, pp. 85315–85332. Available at: https://doi.org/10.1109/ACCESS.2023.3303205.

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.

Elhady, A.M., El-Bakry, H.M. and Abou Elfetouh, A. (2019) 'Comprehensive Risk Identification Model for SCADA Systems', *Security and Communication Networks* [Preprint]. Available at: https://doi.org/10.1155/2019/3914283.

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.

Eungoo, K. and Hwang, H.-J. (2023) 'The Importance of Anonymity and Confidentiality for Conducting Survey Research', *Journal of Research and Publication Ethics*, 4(1), pp. 1–7. Available at: https://doi.org/10.15722/jrpe.4.1.202303.1.

Fernandes, D.A.B. *et al.* (2014) 'Security issues in cloud environments: a survey', *International Journal of Information Security*, 13(2), pp. 113–170. Available at: https://doi.org/10.1007/s10207-013-0208-7.

fortinet (2023) 'What is a Lateral Movement_ Prevention and Detection Methods _ Fortinet'.

Frontegg (2022) 'What Is Role-Based Access Control (RBAC)_ A Complete Guide'.

G, S. and S, M. (2013) ‘Securing Software as a Service Model of Cloud Computing: Issues and Solutions’, *International Journal on Cloud Computing: Services and Architecture*, 3(4), pp. 1–11. Available at: https://doi.org/10.5121/ijccsa.2013.3401.

Gai, K. *et al.* (2016) ‘Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing’, in *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*. IEEE, pp. 273–278. Available at: https://doi.org/10.1109/CSCloud.2016.52.

Gai, K. and Li, S. (2012) ‘Towards cloud computing: A literature review on cloud computing and its development trends’, in *Proceedings - 2012 4th International Conference on Multimedia and Security, MINES 2012*. Available at: https://doi.org/10.1109/MINES.2012.240.

Gaikwad, B.P. (2007) ‘A Critical Review on Risk of Cloud Computing in Commercial’, *International Journal of Innovative Research in Computer and Communication Engineering (An ISO*, 3297(5), p. 9.

Gallagher, K. (2023) ‘Data Security and Privacy: Risks, Best Practices, and Compliance’.

Gangwani, D. *et al.* (2023) ‘A Comprehensive Review on Cloud Security Using Machine Learning Techniques’, in, pp. 1–24. Available at: https://doi.org/10.1007/978-3-031-28581-3_1.

George, D. and Mallery, P. (2024) *IBM SPSS Statistics 29 Step by Step*, *IBM SPSS Statistics 29 Step by Step*. New York: Routledge. Available at: https://doi.org/10.4324/9781032622156.

Ghobaei-Arani, M. *et al.* (2019) ‘ControCity: An Autonomous Approach for Controlling Elasticity Using Buffer Management in Cloud Computing Environment’, *IEEE Access*, 7, pp. 106912–106924. Available at:

https://doi.org/10.1109/ACCESS.2019.2932462.

Ghosh, S. *et al.* (2023) 'Improved End-to-End Data Security Approach for Cloud Computing', *Sustainability*, 15(22), p. 16010. Available at: https://doi.org/10.3390/su152216010.

Gill, S.S. *et al.* (2022) 'AI for next generation computing: Emerging trends and future directions', *Internet of Things (Netherlands)* [Preprint]. Available at: https://doi.org/10.1016/j.iot.2022.100514.

Gill, S.S. *et al.* (2024) 'Modern computing: Vision and challenges', *Telematics and Informatics Reports*, 13, p. 100116. Available at: https://doi.org/10.1016/j.teler.2024.100116.

Giri, S. (2018) 'Reform of civil service of Nepal with e-government practice', *Journal of Personnel Training Academy,* 1(6), pp. 22–36.

Golightly, L. *et al.* (2023) 'Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN', *Cyber Security and Applications*, 1, p. 100015. Available at: https://doi.org/https://doi.org/10.1016/j.csa.2023.100015.

Grigoriou, K., Retana, G. and Rothaermel, F.T. (2012) 'IBM (in 2010) and the Emerging Cloud-Computing Industry', *Harvard Business Review* [Preprint].

Grispos, G., Hanvey, S. and Nuseibeh, B. (2017) 'Use of organisational topologies for forensic investigations', in *SERF 2017 - Proceedings of the 1st ACM SIGSOFT International Workshop on Software Engineering and Digital Forensics, Co-located with FSE 2017*. Available at: https://doi.org/10.1145/3121252.3121253.

Grobauer, B., Walloschek, T. and Stöcker, E. (2011) 'Understanding cloud computing vulnerabilities', *IEEE Security and Privacy* [Preprint]. Available at: https://doi.org/10.1109/MSP.2010.115.

Gudimetla, S.R. (2024) 'Data Encryption in Cloud Storage', *International Research Journal of Modernization in Engineering Technology and Science*, (March), pp. 4–7. Available at: https://doi.org/10.56726/IRJMETS50637.

Gupta, I. *et al.* (2022) 'Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions', *IEEE Access*, 10, pp. 71247–71277. Available at: https://doi.org/10.1109/ACCESS.2022.3188110.

Habes, M., Ali, S. and Pasha, S.A. (2021) 'Statistical Package for Social Sciences Acceptance in Quantitative Research: From the Technology Acceptance Model's Perspective', *FWU Journal of Social Sciences* [Preprint]. Available at: https://doi.org/10.51709/19951272/Winter-2021/3.

Harfoushi, O. and Obiedat, R. (2018) 'An Insight to Middleware Technologies used for Cloud Computing Frameworks: From the Perspective of Successful Enterprise Application Integration', *Modern Applied Science*, 12(9), p. 234. Available at: https://doi.org/10.5539/mas.v12n9p234.

Harknett, R.J. and Stever, J.A. (2009) 'The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen', *Journal of Homeland Security and Emergency Management* [Preprint]. Available at: https://doi.org/10.2202/1547-7355.1649.

Heininger, R. (2012) 'IT Service Management in a Cloud Environment: A Literature Review', *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/ssrn.2119030.

Holm, H. (2014) 'Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter?', in *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 4895–4904. Available at:

https://doi.org/10.1109/HICSS.2014.600.

Hou, Y. *et al.* (2020) 'A Data Security Enhanced Access Control Mechanism in Mobile Edge Computing', *IEEE Access*, 8, pp. 136119–136130. Available at: https://doi.org/10.1109/ACCESS.2020.3011477.

Imran, A. (2014) 'An Overview of Service Models of Cloud Computing', *International Journal of Multidisciplinary and Current Research*, 2(August 2014), p. 5.

Ismail, N. (2011) 'Cursing the cloud (or) controlling the cloud?', *Computer Law and Security Review* [Preprint]. Available at: https://doi.org/10.1016/j.clsr.2011.03.005.

Jagadale, B.B. *et al.* (2024) 'Security Issues and Research Challenges in Cloud Computing', *International Journal of Engineering and Computer Science*, 13(05), pp. 26158–26171. Available at: https://doi.org/10.18535/ijecs/v13i05.4820.

Jasim Mohammed, H., Abdulmohsin AL-dahneem, E. and Hamadi, A.K. (2016) *a Comparative Analysis for Adopting an Innovative Pedagogical Approach of Flipped Teaching for Active Classroom Learning*, *Journal of Global Business and Social Entrepreneurship (GBSE) Journal*.

Jathanna, R. and Jagli, D. (2017) 'Cloud Computing and Security Issues', *International Journal of Engineering Research and Applications*, 07(06), pp. 31–38. Available at: https://doi.org/10.9790/9622-0706053138.

El Kafhali, S., El Mir, I. and Hanini, M. (2022) 'Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing', *Archives of Computational Methods in Engineering*, 29(1), pp. 223–246. Available at: https://doi.org/10.1007/s11831-021-09573-y.

Kalaiprasath *et al.* (2017) 'Cloud security and compliance - A semantic approach in end to end security', *International Journal of Mechanical Engineering and Technology*, 8(5), pp. 987–994.

Kanwal, I. *et al.* (2021) 'Cloud Computing Security Challenges: A Review', in *Advanced Sciences and Technologies for Security Applications*, pp. 459–469. Available at: https://doi.org/10.1007/978-3-030-68534-8_29.

Kar Yee, C. and Zolkipli, M.F. (2021) 'Review on Confidentiality, Integrity and Availability in Information Security', *Journal of ICT in Education* [Preprint]. Available at: https://doi.org/10.37134/jictie.vol8.2.4.2021.

Karam, Y., Baker, T. and Taleb-Bendiab, A. (2012) 'Security support for intention driven elastic cloud computing', in *Proceedings - UKSim-AMSS 6th European Modelling Symposium, EMS 2012*. Available at: https://doi.org/10.1109/EMS.2012.17.

Kemmerer, R.A. (2003) 'Cybersecurity', in *25th International Conference on Software Engineering, 2003. Proceedings.* IEEE, pp. 705–715. Available at: https://doi.org/10.1109/ICSE.2003.1201257.

Kent, K. and Murugiah Souppaya (2019) 'Guide to Computer Security Log Management'.

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.

Khorshed, M.T., Ali, A.B.M.S. and Wasimi, S.A. (2012) 'A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing', *Future Generation Computer Systems*, 28(6), pp. 833–851. Available at: https://doi.org/10.1016/j.future.2012.01.006.

Kim, S.S. and Kim, Y.J. (2017) 'The effect of compliance knowledge and compliance support systems on information security compliance behavior', *Journal of Knowledge Management*, 21(4), pp. 986–1010. Available at: https://doi.org/10.1108/JKM-08-2016-0353.

Kim, W. *et al.* (2009) 'Adoption issues for cloud computing', in *MoMM2009 - The 7th*

International Conference on Advances in Mobile Computing and Multimedia. Available at: https://doi.org/10.1145/1821748.1821751.

King, N.J. and Raja, V.T. (2012) 'Protecting the privacy and security of sensitive customer data in the cloud', *Computer Law and Security Review* [Preprint]. Available at: https://doi.org/10.1016/j.clsr.2012.03.003.

Kliazovich, D., Bouvry, P. and Khan, S.U. (2012) 'GreenCloud: a packet-level simulator of energy-aware cloud computing data centers', *The Journal of Supercomputing*, 62(3), pp. 1263–1283. Available at: https://doi.org/10.1007/s11227-010-0504-1.

Kumar, D. and Panchanatham, N. (2015) 'A case study on Cyber Security in E-Governance', *International Research Journal of Engineering and Technology (IRJET)* [Preprint].

Kumar, V., Chaisiri, S. and Ko, R. (2017) *Data Security in Cloud Computing*, *Data Security in Cloud Computing*. Edited by V. Kumar, S. Chaisiri, and R. Ko. Institution of Engineering and Technology. Available at: https://doi.org/10.1049/PBSE007E.

Larsson, L., Henriksson, D. and Elmroth, E. (2011) 'Scheduling and monitoring of internally structured services in cloud federations', in *Proceedings - IEEE Symposium on Computers and Communications*. Available at: https://doi.org/10.1109/ISCC.2011.5984012.

Lee, B.-H., Dewi, E.K. and Wajdi, M.F. (2018) 'Data security in cloud computing using AES under HEROKU cloud', in *2018 27th Wireless and Optical Communication Conference (WOCC)*. IEEE, pp. 1–5. Available at: https://doi.org/10.1109/WOCC.2018.8372705.

Li, Y. and Liu, Q. (2021) 'A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments', *Energy Reports* [Preprint].

Available at: https://doi.org/10.1016/j.egyr.2021.08.126.

Liu, L. *et al.* (2009) 'GreenCloud', in *Proceedings of the 6th international conference industry session on Autonomic computing and communications industry session*. New York, NY, USA: ACM, pp. 29–38. Available at: https://doi.org/10.1145/1555312.1555319.

Lord, N. (2019) 'Data Protection: Data In transit vs. Data At Rest', *Digital Guardian's Blog*, p. 1.

Lubitz, L., Battle, A. and Eichler, R. (2025) *5 ATM Scams That Can Break the Bank*, *Investopedia*.

Man, Z. *et al.* (2023) 'Research on cloud data encryption algorithm based on bidirectional activation neural network', *Information Sciences*, 622, pp. 629–651. Available at: https://doi.org/10.1016/j.ins.2022.11.089.

Martinez, J. (2024) 'What Is Data Exfiltration_ Examples, Detection & Prevention'.

Massoud Amin, S. and Wollenberg, B.F. (2005) 'Toward a smart grid: power delivery for the 21st century', *IEEE Power and Energy Magazine* [Preprint]. Available at: https://doi.org/10.1109/mpae.2005.1507024.

Mathisen, E. (2011) 'Security challenges and solutions in cloud computing', in *IEEE International Conference on Digital Ecosystems and Technologies*. Available at: https://doi.org/10.1109/DEST.2011.5936627.

McIntosh, M. and Austel, P. (2005) 'XML signature element wrapping attacks and countermeasures', in *Proceedings of the 2005 workshop on Secure web services*. New York, NY, USA: ACM, pp. 20–27. Available at: https://doi.org/10.1145/1103022.1103026.

Mehraj, S. and Banday, M.T. (2020) 'Establishing a zero trust strategy in cloud computing environment', in *2020 International Conference on Computer Communication and*

Informatics, ICCCI 2020. Available at: https://doi.org/10.1109/ICCCI48352.2020.9104214.

Mei, J., Li, Kenli and Li, Keqin (2017) 'Customer-Satisfaction-Aware Optimal Multiserver Configuration for Profit Maximization in Cloud Computing', *IEEE Transactions on Sustainable Computing* [Preprint]. Available at: https://doi.org/10.1109/TSUSC.2017.2667706.

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.

Modi, C. *et al.* (2013) 'A survey on security issues and solutions at different layers of Cloud computing', *Journal of Supercomputing* [Preprint]. Available at: https://doi.org/10.1007/s11227-012-0831-5.

Mohiyuddin, A. *et al.* (2022) 'Secure Cloud Storage for Medical IoT Data using Adaptive Neuro-Fuzzy Inference System', *International Journal of Fuzzy Systems*, 24(2), pp. 1203–1215. Available at: https://doi.org/10.1007/s40815-021-01104-y.

Mosbah, M.M., Soliman, H. and El-Nasr, M.A. (2013) 'Current Services in Cloud Computing: A Survey', *International Journal of Computer Science, Engineering and Information Technology*, 3(5), pp. 1–8. Available at: https://doi.org/10.5121/ijcseit.2013.3501.

Muhammad, M. *et al.* (2018) 'An analysis of security challenges and their perspective solutions for cloud computing and IoT', *ICST Transactions on Scalable Information Systems*, pp. 1–11. Available at: https://doi.org/10.4108/eai.23-10-2020.166718.

Mulligan, D.K. and Schneider, F.B. (2011) 'Doctrine for cybersecurity', *Daedalus* [Preprint]. Available at: https://doi.org/10.1162/DAED_a_00116.

Narayan, D. (2022) 'Platform capitalism and cloud infrastructure: Theorizing a hyper-scalable computing regime', *Environment and Planning A: Economy and Space*, 54(5), pp. 911–929. Available at: https://doi.org/10.1177/0308518X221094028.

Nasir, M. *et al.* (2022) 'Feature engineering and deep learning-based intrusion detection framework for securing edge IoT', *The Journal of Supercomputing*, 78(6), pp. 8852–8866. Available at: https://doi.org/10.1007/s11227-021-04250-0.

National Institute of Standards and Technology (2022) *Computer Security Resource Center*, *Post-Quantum Cryptography PQC*.

Ngozi Samuel Uzougbo, I. and Adewusi, A.O. (2024) 'Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations', *International Journal of Science and Research Archive*, 12(1), pp. 533–548. Available at: https://doi.org/10.30574/ijsra.2024.12.1.0802.

Nwobodo, I. (2016) 'Cloud computing: Models, services, utility, advantages, security issues, and prototype', in *Lecture Notes in Electrical Engineering*. Available at: https://doi.org/10.1007/978-81-322-2580-5_110.

Odeh, A. *et al.* (2024) 'Data Privacy and Compliance in IoT', in *AFRICAN-EUROPEAN REGIONAL GOVERNANCE & DEVELOPMENT CONFERENCE*, pp. 128–144. Available at: https://doi.org/10.4018/979-8-3693-3451-5.ch006.

Oh, T.H. *et al.* (2010) 'State of the Art of Network Security Perspectives in Cloud Computing', in *Communications in Computer and Information Science*, pp. 629–637. Available at: https://doi.org/10.1007/978-3-642-16444-6_79.

Olomu, M.O., Binuyo, G.O. and Oyebisi, T.O. (2023) 'The adoption and impact of Internet-based technological innovations on the performance of the industrial cluster firms', *Journal of Economy and Technology* [Preprint]. Available at: https://doi.org/10.1016/j.ject.2023.11.004.

Oluremi, D. *et al.* (2025) ‘Cloud Computing and Cybersecurity: Emerging Threats and Defense Mechanisms’.

Onumo *et al.* (2021) ‘Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures’, *ACM Transactions on Management Information Systems*, 12(2), pp. 1–29. Available at: https://doi.org/10.1145/3424282.

Pallant, J. (2020) *SPSS Survival Manual*. Routledge. Available at: https://doi.org/10.4324/9781003117452.

Parto, S. (2005) ‘Economic Activity and Institutions: Taking Stock’, *Journal of Economic Issues*, 39(1), pp. 21–52. Available at: https://doi.org/10.1080/00213624.2005.11506779.

Paul, A., Sharma, V. and Olukoya, O. (2024) ‘SQL injection attack: Detection, prioritization & prevention’, *Journal of Information Security and Applications* [Preprint]. Available at: https://doi.org/10.1016/j.jisa.2024.103871.

Podsakoff, P.M. *et al.* (2003) ‘Common method biases in behavioral research: A critical review of the literature and recommended remedies.’, *Journal of Applied Psychology*, 88(5), pp. 879–903. Available at: https://doi.org/10.1037/0021-9010.88.5.879.

Prasad, G.S. *et al.* (2018) ‘A Survey on User Awareness of Cloud Security’, *International Journal of Engineering & Technology*, 7(2.32), p. 131. Available at: https://doi.org/10.14419/ijet.v7i2.32.15386.

Priya, A.S. and Sangeetha, S. (2024) ‘Security Challenges and Solutions in Cloud Computing Environments’, *IARJSET*, 11(3), pp. 67–73. Available at: https://doi.org/10.17148/IARJSET.2024.11311.

Probst, C., J, H. and Gollmann, D. (2010) ‘Insider threats in cybersecurity’, *Insider Threats*

in Cyber Security [Preprint].

Pureti, N. (2023) 'Encryption 101: How to Safeguard Your Sensitive Information', *International Journal of Advanced Engineering Technologies and Innovations*, 01(01), p. 1.

Puthal, D. *et al.* (2015) 'Cloud computing features, issues, and challenges: A big picture', in *Proceedings - 1st International Conference on Computational Intelligence and Networks, CINE 2015*. Available at: https://doi.org/10.1109/CINE.2015.31.

Qureshi, M.B. *et al.* (2022) 'Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud', *Symmetry*, 14(4). Available at: https://doi.org/10.3390/sym14040695.

R.Sharma (2012) 'Study of Latest Emerging Trends on Cyber Security and its challenges to Society', *international journal of scientific & engineering reasearch*, 03, pp. 67–75.

Radu, L.D. (2017) 'Green Cloud Computing: A Literature Survey', *Symmetry*, 9(12), p. 295. Available at: https://doi.org/10.3390/sym9120295.

Ramgovind, S., Eloff, M.M. and Smith, E. (2010) 'The management of security in cloud computing', in *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*. Available at: https://doi.org/10.1109/ISSA.2010.5588290.

Rao, P.M. and Saraswathi, P. (2021) 'Evolving cloud security technologies for social networks', in *Security in IoT Social Networks*. Elsevier, pp. 179–203. Available at: https://doi.org/10.1016/B978-0-12-821599-9.00008-X.

Rasal, P. (2021) 'Cloud Computing Security Issues and Challenges : A Survey', *research gate*, 8, pp. 680–683.

Rasheed, H. (2014) 'Data and infrastructure security auditing in cloud computing environments', *International Journal of Information Management* [Preprint].

Available at: https://doi.org/10.1016/j.ijinfomgt.2013.11.002.

Rauf, U., Mohsen, F. and Wei, Z. (2023) ‘A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations’, *Journal of Cyber Security and Mobility* [Preprint]. Available at: https://doi.org/10.13052/jcsm2245-1439.1225.

Reece, M. *et al.* (2023) ‘Emergent (In)Security of Multi-Cloud Environments’, *Cormell University*, pp. 1–2. Available at: https://doi.org/https://doi.org/10.48550/arXiv.2311.01247.

Rittinghouse, J.W. and Ransome, J.F. (2017) *Cloud Computing*, *Cloud Computing: Implementation, Management, and Security*. CRC Press. Available at: https://doi.org/10.1201/9781439806814.

Robinson, N. *et al.* (2010) ‘The Cloud: Understanding the Security, Privacy and Trust Challenges’, *SSRN Electronic Journal* [Preprint]. Available at: https://doi.org/10.2139/ssrn.2141970.

Rong, C., Nguyen, S.T. and Jaatun, M.G. (2013) ‘Beyond lightning: A survey on security challenges in cloud computing’, *Computers and Electrical Engineering* [Preprint]. Available at: https://doi.org/10.1016/j.compeleceng.2012.04.015.

Ryan, P. and Falvey, S. (2012) ‘Trust in the clouds’, *Computer Law and Security Review*, 28(5), pp. 513–521. Available at: https://doi.org/10.1016/j.clsr.2012.07.002.

S Arvind, E. al. (2023) ‘A Study on Data Protection in Cloud Environment’, *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(10), pp. 1748–1753. Available at: https://doi.org/10.17762/ijritcc.v11i10.8750.

Sabahi, F. (2011) ‘Cloud computing security threats and responses’, in *2011 IEEE 3rd International Conference on Communication Software and Networks, ICCSN 2011*. Available at: https://doi.org/10.1109/ICCSN.2011.6014715.

Sarathy, V., Narayan, P. and Mikkilineni, R. (2010) 'Next generation cloud computing architecture: Enabling real-time dynamism for shared distributed physical infrastructure', in *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE*. Available at: https://doi.org/10.1109/WETICE.2010.14.

Sarhan, B. Bin and Altwaijry, N. (2022) 'Insider Threat Detection Using Machine Learning Approach', *Applied Sciences*, 13(1), p. 259. Available at: https://doi.org/10.3390/app13010259.

Sarker, I.H. *et al.* (2023) 'Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions', *Mobile Networks and Applications* [Preprint]. Available at: https://doi.org/10.1007/s11036-022-01937-3.

Saxena, N. *et al.* (2020) 'Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses', *Electronics*, 9(9), p. 1460. Available at: https://doi.org/10.3390/electronics9091460.

Security, C. (2014) 'Cloud Security: Theory and Practice', pp. 1–3.

Segun-Falade, O.D. *et al.* (2024) 'Evaluating the role of cloud integration in mobile and desktop operating systems', *International Journal of Scholarly Research in Engineering and Technology*, 4(1), pp. 019–031. Available at: https://doi.org/10.56781/ijsret.2024.4.1.0019.

Sen, A.K. and Tiwari, P.K. (2017) '"Security Issues and Solutions in Cloud Computing".', *IOSR Journal of Computer Engineering*, 19(2), pp. 67–72. Available at: https://doi.org/10.9790/0661-1902046772.

Seth, D., Najana, M. and Ranjan, P. (2024) 'Compliance and Regulatory Challenges in Cloud Computing: A Sector-Wise Analysis', *International Journal of Global*

Innovations and Solutions (IJGIS), 3. Available at: https://doi.org/10.21428/e90189c8.68b5dea5.

Shabbir, M. *et al.* (2021) 'Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing', *IEEE Access* [Preprint]. Available at: https://doi.org/10.1109/ACCESS.2021.3049564.

Shah, S. and Singh, S. (2024) 'Serverless Computing with Containers: A Comprehensive Overview', 3, pp. 637–659.

Shahzad, F., Iqbal, W. and Bokhari, F.S. (2015) 'On the use of CryptDB for securing Electronic Health data in the cloud: A performance study', in *2015 17th International Conference on E-Health Networking, Application and Services, HealthCom 2015*. Available at: https://doi.org/10.1109/HealthCom.2015.7454484.

Shital, P. and R., C. (2017) 'Web Browser Security: Different Attacks Detection and Prevention Techniques', *International Journal of Computer Applications*, 170(9), pp. 35–41. Available at: https://doi.org/10.5120/ijca2017914938.

El Sibai, R. *et al.* (2020) 'A survey on access control mechanisms for cloud computing', *Transactions on Emerging Telecommunications Technologies*, 31(2). Available at: https://doi.org/10.1002/ett.3720.

Singh, A. and Gupta, B. (2022) 'Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions', *International Journal on Semantic Web and Information Systems*, 18, pp. 1–43. Available at: https://doi.org/10.4018/IJSWIS.297143.

Souppaya, M. and Scarfone, K. (2013) 'Guide to Malware Incident Prevention and Handling for Desktops and Laptops', *NIST Special Publication*, 800, p. 83.

Sreehari, A. *et al.* (2018) 'A Study of Awareness of Cyber Crime Among College Students

with Special Reference to Kochi', *international journal of pure and applied mathematics*, 119(16), pp. 1353–1360.

Sriram, D. (2023) 'Keep Your Cloud Data Safe with Encryption'.

Subashini, S. and Kavitha, V. (2011) 'A survey on security issues in service delivery models of cloud computing', *Journal of Network and Computer Applications* [Preprint]. Available at: https://doi.org/10.1016/j.jnca.2010.07.006.

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.

Sudalai, S. and Smys, S. (2016) 'A Survey on Cloud Security Issues and Challenges with Possible Measures', in.

Suwandi, W.S. (2022) 'Do Economic Growth, Income Distribution, and Investment Reduce Poverty Level?', *Jurnal Berkala Ilmiah Efisiensi* [Preprint].

Symantec (2019) *Internet Security Threat Report (ISTR) 2019 | Symantec*, *Symantec*.

Tabrizchi, H. and Rafsanjani, M.K. (2020) 'A survey on security challenges in cloud computing: issues, threats, and solutions', *The Journal of Supercomputing*, 76(12), pp. 9493–9532. Available at: https://doi.org/10.1007/s11227-020-03213-1.

Taleb, N. and Mohamed, E.A. (2020) 'Cloud Computing Trends: A Literature Review', *Academic Journal of Interdisciplinary Studies*, 9(1), p. 91. Available at: https://doi.org/10.36941/ajis-2020-0008.

Tariq, U. *et al.* (2017) 'A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review', *Cybersecurity* [Preprint].

Tariq, U. *et al.* (2023) 'A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review', *Sensors* [Preprint]. Available at: https://doi.org/10.3390/s23084117.

Ten, C.W., Manimaran, G. and Liu, C.C. (2010) 'Cybersecurity for critical infrastructures: Attack and defense modeling', in *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*. Available at: https://doi.org/10.1109/TSMCA.2010.2048028.

Teneyuca, D. (2011) 'Internet cloud security: The illusion of inclusion', *Information Security Technical Report*, 16(3–4), pp. 102–107. Available at: https://doi.org/10.1016/j.istr.2011.08.005.

Teoh, T.T. *et al.* (2018) 'Analyst intuition inspired neural network based cyber security anomaly detection', *International Journal of Innovative Computing, Information and Control*, 13(01), pp. 379–386.

The Australian Cyber Security Centre (2015) *The Australian Cyber Security Centre Threat Report 2015*, *The Australian Cyber Security Centre Threat Report 2015*.

Thompson, M. and Reynolds, L. (2022) 'Metadata-Based Spoofing Detection Using Unified Database Logging Architectures'.

Timonera, K. (2024) 'What Is Data Availability? Best Practices and Challenges'.

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.

Tripathi, A. and Mishra, A. (2011) 'Cloud computing security considerations', in *2011 IEEE International Conference on Signal Processing, Communications and Computing, ICSPCC 2011*. Available at: https://doi.org/10.1109/ICSPCC.2011.6061557.

Tuli, B., Kumar, S. and Gautam, N. (2022) 'An Overview on Cyber Crime and Cyber Security', *Asian Journal of Engineering and Applied Technology*, 11(1), pp. 36–

45. Available at: https://doi.org/10.51983/ajeat-2022.11.1.3309.

Tyagi, A.K. and Sreenath, N. (2021) 'Cyber Physical Systems: Analyses, challenges and possible solutions', *Internet of Things and Cyber-Physical Systems* [Preprint]. Available at: https://doi.org/10.1016/j.iotcps.2021.12.002.

Ullah, A. *et al.* (2023) 'Cloud and internet-of-things secure integration along with security concerns', *International Journal of Informatics and Communication Technology (IJ-ICT)*, 12(1), p. 62. Available at: https://doi.org/10.11591/ijict.v12i1.pp62-71.

Ullah, F. *et al.* (2018) 'Data exfiltration: A review of external attack vectors and countermeasures', *Journal of Network and Computer Applications*, 101, pp. 18–54. Available at: https://doi.org/10.1016/j.jnca.2017.10.016.

Vaquero, L.M. *et al.* (2009) 'A Break in the Clouds: Towards a Cloud De nition', *Computer Communication Review* [Preprint].

Varadharajan, V. and Suri, N. (2024) 'Security challenges when space merges with cyberspace', *Space Policy* [Preprint]. Available at: https://doi.org/10.1016/j.spacepol.2023.101600.

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.

Velumadhava Rao, R. and Selvamani, K. (2015) 'Data security challenges and its solutions in cloud computing', *Procedia Computer Science*, 48(C), pp. 204–209. Available at: https://doi.org/10.1016/j.procs.2015.04.171.

Vitunskaite, M. *et al.* (2019) 'Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership', *Computers & Security*, 83, pp. 313–331. Available at: https://doi.org/10.1016/j.cose.2019.02.009.

Wang, J. (2024) ‘Research and Design of Encryption Standards Based on IoT Network Layer Information Security of Data’, *ICST Transactions on Scalable Information Systems*, 11(5). Available at: https://doi.org/10.4108/eetsis.5826.

Wang, L. *et al.* (2010) ‘Cloud Computing: a Perspective Study’, *New Generation Computing*, 28(2), pp. 137–146. Available at: https://doi.org/10.1007/s00354-008-0081-5.

Wang, Z. (2011) ‘Security and privacy issues within the cloud computing’, in *Proceedings - 2011 International Conference on Computational and Information Sciences, ICCIS 2011*. Available at: https://doi.org/10.1109/ICCIS.2011.247.

Wilson, K.S. and Kiy, M.A. (2014) ‘Some fundamental cybersecurity concepts’, *IEEE Access* [Preprint]. Available at: https://doi.org/10.1109/ACCESS.2014.2305658.

Wooley, P.S. (2011) ‘Identifying Cloud Computing Security Risks.’, *Continuing Education*, pp. 1–88.

Xia, T. *et al.* (2021) ‘CSPM’, *International Journal of Systems and Software Security and Protection*, 12(2), pp. 68–85. Available at: https://doi.org/10.4018/IJSSSP.20210101.oa1.

Xue, J. and Zhang, J.J. (2010) ‘A brief survey on the security model of cloud computing’, in *Proceedings - 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, DCABES 2010*. Available at: https://doi.org/10.1109/DCABES.2010.103.

Yalla, R.K.M.K. (2021) ‘Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data’, *International Journal of Engineering Research and Science and Technology*, 17(3), pp. 18–28. Available at: https://doi.org/10.62643/ijerst.2021.v17.i03.pp18-28.

Yasar, K. (2024) ‘What is Cloud Computing? | Definition from TechTarget’.

Yaseen, Q. *et al.* (2017) 'An insider threat aware access control for cloud relational databases', *Cluster Computing*, 20(3), pp. 2669–2685. Available at: https://doi.org/10.1007/s10586-017-0810-y.

Yimam, D. and Fernandez, E.B. (2016) 'A survey of compliance issues in cloud computing', *Journal of Internet Services and Applications*, 7(1), p. 5. Available at: https://doi.org/10.1186/s13174-016-0046-8.

Yogamangal, R. and Sriram, V.S.S. (2012) 'A Review on Security Issues in Cloud Computing', *Journal of Artificial Intelligence*, 6(1), pp. 1–7. Available at: https://doi.org/10.3923/jai.2013.1.7.

Yoshida, H. (2017) 'Storage Networking Industry Association', in *Encyclopedia of Database Systems*. New York, NY: Springer New York, pp. 1–1. Available at: https://doi.org/10.1007/978-1-4899-7993-3_1347-2.

Youseff, L., Butrico, M. and Da Silva, D. (2008) 'Toward a unified ontology of cloud computing', in *Grid Computing Environments Workshop, GCE 2008*. Available at: https://doi.org/10.1109/GCE.2008.4738443.

Yousefpour, A. *et al.* (2019) 'All one needs to know about fog computing and related edge computing paradigms: A complete survey', *Journal of Systems Architecture*, 98, pp. 289–330. Available at: https://doi.org/10.1016/j.sysarc.2019.02.009.

Youssef, A. and Alageel, M. (2011) 'Security Issues in Cloud Computing', *International Journal on Computing*, 1(3), pp. 7–12.

Zadeh, A. *et al.* (2023) 'A cybersecurity risk quantification and classification framework for informed risk mitigation decisions', *Decision Analytics Journal*, 9(August), p. 100328. Available at: https://doi.org/10.1016/j.dajour.2023.100328.

Zaid, T. and Garai, S. (2024) 'Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers', *Blockchain*

in Healthcare Today [Preprint]. Available at: https://doi.org/10.30953/bhty.v7.302.

Zarichuk, O. (2024) 'Security in cloud computing: Methods for ensuring privacy and integration in modern applications', *Development management*, 23(1), pp. 37–45. Available at: https://doi.org/10.57111/devt/1.2024.37.

Zhang, Xuan *et al.* (2010) 'Information security risk management framework for the cloud computing environments', in *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010*. Available at: https://doi.org/10.1109/CIT.2010.501.

Zissis, D. and Lekkas, D. (2012) 'Addressing cloud computing security issues', *Future Generation Computer Systems*, 28(3), pp. 583–592. Available at: https://doi.org/https://doi.org/10.1016/j.future.2010.12.006.

APPENDIX A:

DATASET

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	Age	Gender	Education	Field of Stu	Current Pos	Years of E	Industry Sec	Size of Orga	Effective m	There is a	Regular da	Data loss i	Strict acce	Strong pas	Multi-factor	Clear proc	Measures	There is a	Regular tra	Clear proc	Strong mea	The import
3	3	1	5	7	9	4	3	3	3	3	5	4	4	2	3	3	3	5	5	5	4	4
4	5	2	3	6	2	3	7	4	4	1	5	4	4	4	5	5	3	4	3	3	5	4
5	5	2	5	5	7	2	2	1	2	3	4	4	5	3	5	3	4	3	3	3	4	3
6	3	2	6	4	2	5	4	2	4	5	4	3	3	3	5	5	5	4	4	4	5	5
7	3	2	4	5	3	3	4	4	1	5	3	3	3	5	3	1	3	4	4	5	1	3
8	1	1	5	7	9	2	5	3	5	4	3	4	4	5	4	4	5	3	3	4	5	4
9	1	1	6	6	2	1	4	2	2	5	4	5	4	2	2	4	2	5	1	5	5	3
10	1	1	5	2	7	1	7	3	2	3	5	4	2	4	4	4	3	3	5	5	1	1
11	1	2	5	2	3	2	1	1	4	4	3	4	3	3	4	3	4	5	5	5	3	3
12	1	1	3	2	5	2	3	3	3	1	4	3	2	2	2	3	1	5	4	2	2	2
13	4	1	5	7	6	2	8	3	1	2	5	3	4	3	5	3	5	5	4	5	1	5
14	1	1	4	1	8	2	1	3	3	4	3	5	3	1	2	3	4	5	3	4	4	3
15	4	1	5	7	2	3	2	3	5	1	3	5	3	5	3	5	2	5	4	5	5	2
16	3	1	6	4	3	1	5	4	3	3	4	3	3	5	2	4	5	3	2	5	5	3
17	5	1	6	6	5	2	7	1	4	3	4	2	5	3	4	3	5	5	4	5	3	3
18	1	1	6	1	9	1	3	1	2	5	5	3	5	3	3	5	2	1	2	4	1	3
19	4	2	4	3	8	4	4	2	5	5	3	3	2	5	4	2	4	4	5	5	4	2
20	5	2	6	3	1	5	3	3	3	3	5	5	5	3	5	4	4	1	3	3	2	5
21	2	2	4	4	2	3	4	3	3	4	5	3	3	4	4	5	5	1	2	4	3	5
22	5	2	6	6	1	2	5	3	4	5	4	5	3	4	1	4	4	5	3	3	5	4
23	2	1	4	1	5	1	6	3	4	5	4	4	1	5	3	5	4	5	4	5	3	4
24	5	2	5	3	8	1	7	1	3	3	5	4	4	5	3	5	3	4	4	2	4	3
25	3	1	5	5	1	1	6	1	5	4	3	3	4	5	4	1	4	5	3	5	3	3
26	1	2	6	6	3	1	2	3	3	3	3	4	3	3	3	4	4	4	5	3	4	3
27	2	1	3	2	3	3	8	2	5	5	3	4	3	2	5	4	5	4	4	4	4	3

	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO
1	Advanced	Protocols f	Measures	Anti-malwa	Incidents o	Measures	There is a	Employees	Immediate	The cloud s	Access to	Our organi	Our organi	Our organi	Cloud secu	Our cloud s	There is cl	Our organi	Data integr
3	5	1	3	3	5	4	5	4	1	3	4	5	5	5	4	4	1	3	3
4	5	3	5	3	4	4	3	5	5	4	3	4	2	3	4	3	3	3	3
5	5	3	4	3	5	1	5	5	1	3	2	5	2	4	5	3	4	5	4
6	4	5	5	4	5	3	3	5	5	4	4	3	5	3	5	3	3	3	3
7	4	3	4	5	4	2	3	5	3	3	3	1	4	3	4	5	5	3	4
8	3	3	5	5	5	3	5	4	3	3	1	4	3	4	4	5	3	3	3
9	4	2	3	5	3	2	4	5	1	3	4	2	4	3	1	4	3	4	1
10	5	4	5	5	3	5	5	4	4	3	3	5	5	3	4	5	5	5	3
11	4	3	5	2	5	5	3	5	5	5	4	4	4	4	4	5	3	4	5
12	4	4	4	4	5	3	3	3	4	5	3	4	4	3	3	3	2	5	3
13	3	5	4	3	4	5	5	3	5	3	1	1	5	5	4	1	4	3	4
14	3	3	1	4	5	4	2	5	3	3	5	4	4	3	3	4	4	3	4
15	4	3	3	3	3	4	3	5	3	3	5	4	4	4	3	5	5	3	5
16	4	4	3	5	4	5	4	4	4	4	2	4	1	5	5	4	1	2	4
17	3	5	1	4	4	4	3	2	5	4	3	5	4	2	3	4	5	3	3
18	3	4	3	3	5	5	5	4	4	5	4	1	4	5	4	5	4	5	4
19	5	5	3	3	3	3	5	4	4	3	5	3	4	4	5	3	5	4	4
20	2	4	3	4	4	3	4	5	5	5	2	4	3	4	5	4	3	5	5
21	2	5	4	5	5	3	4	4	4	5	5	4	5	5	4	5	3	1	2
22	5	3	4	5	5	5	5	1	2	3	4	5	4	3	4	4	1	1	4
23	2	1	4	3	4	3	5	2	4	3	4	4	4	5	5	4	5	4	4
24	5	5	4	4	3	4	3	5	3	3	3	3	5	4	3	2	4	5	3
25	3	4	2	5	4	4	4	5	3	4	3	5	1	5	5	4	5	3	4
26	5	4	1	5	3	4	5	4	5	3	5	5	2	3	2	4	3	4	5
27	4	4	5	3	3	5	4	5	4	2	5	5	5	3	1	5	3	5	3
28	4	3	4	5	3	3	4	1	4	4	3	5	5	5	4	4	3	3	5