African Journal of Emerging Issues
Peer reviewed | Double blind | Interdisciplinary

African Journal of Emerging Issues (AJOEI)
Online ISSN: 2663 - 9335
Available at: https://ajoeijournals.org

INFORMATION TECHNOLOGY

DESIGNING A COMPREHENSIVE FRAMEWORK FOR DATA AND NETWORK SECURITY IN CLOUD COMPUTING: CASE OF KENYAN BANKING INDUSTRY

[1*]Ouma Geoffrey, [2]Awuor Mzee, [3]Wamuyu Kanyi Patrick, [4]Maake Bernard
[1]Department of Computing Sciences, Kisii University, Kenya*
oumageoffrey29@gmail.com

[2]Department of Computing Sciences, Kisii University, Kenya
fawuor@kisiiuniversity.ac.ke

[3]School of Science and Technology, USIU-A, Kenya
patrickkanyi@hotmail.com

[4]Department of Computing Sciences, Kisii University, Kenya
bmaake@kisiiuniversity.ac.ke

Publication Date: February 2024

ABSTRACT

This study sought to develop a tailored framework for secure cloud computing implementation in the Kenyan banking industry, addressing the unique security challenges faced by these banks. Kenyan banks encounter distinct security challenges in cloud adoption, including concerns regarding data abstraction, multitenancy, and the increasing prevalence of cyber threats, particularly phishing attacks. Regulatory compliance adherence emerges as a critical consideration, with 87.3% of respondents recognizing its significance. Additionally, resilience and disaster recovery planning are identified as strategic imperatives, with 88.2% of participants prioritizing these aspects in their cloud adoption strategies. The framework is conceptualized based on a meticulous analysis of industry-specific requirements and an extensive literature review. It is built on the foundational principles of Identity and Access Management (IAM), Security Reference Architecture (SRA), and an Integrated Intrusion Detection and Prevention System (IDPS). Validation of the framework demonstrates its effectiveness in aligning with identified industry-specific gaps and challenges, offering a reliable solution to enhance cloud computing security. The proposed framework leverages IAM to establish robust access controls, extends SRA to create a tailored architectural blueprint, and integrates IDPS for proactive threat detection. These components operate synergistically, fortifying cloud security for the banking industry. The proposed framework stands as a blueprint for secure cloud computing implementation in the Kenyan banking industry, offering a robust solution to safeguard sensitive financial data in the cloud. By incorporating fine-grained access control, encryption, and the utilization of a Cloud Security Trusted Authority (CSTA), the framework ensures secure operations within the cloud environment. It addresses concerns regarding both data security and network security, providing a level of security equivalent to or surpassing traditional in-house IT environments.

Keywords: *Cloud computing security, IAM, network security, CSTA.*

1. INTRODUCTION

The rapid advancement of cloud computing technology has revolutionized the way businesses operate and manage their data. The banking industry, being highly data-driven and security-sensitive, has recognized the potential benefits of adopting cloud computing solutions (Ahmad, Rasool, Javed, Baker, & Jalil, 2022). Cloud computing offers banks the opportunity to enhance their operational efficiency, scalability, and cost-effectiveness (Tiwari, Bharadwaj, & Joshi, 2021). However, security concerns remain a significant obstacle in the widespread adoption of cloud computing within the banking sector (Al-Marsy, Chaudhary, & Rodger, 2021). Traditional IT infrastructures have limitations in terms of scalability, flexibility, and cost efficiency, prompting banks to explore cloud computing solutions. Cloud computing offers on-demand access to shared computing resources, enabling banks to streamline their operations and focus on core banking activities (Gyau, Owiredu-Ghorman, Amaning, & Kpimekuu, 2023). However, the dynamic nature of cloud environments and the shared responsibility model introduce unique security challenges. To address these challenges, a comprehensive framework for data and network security in cloud computing is necessary to ensure the protection of sensitive information and maintain regulatory compliance. To fully leverage the advantages of cloud computing while ensuring the confidentiality, integrity, and availability of sensitive data, it is crucial to design a comprehensive framework for data and network security tailored specifically to the banking industry's needs. The banking industry deals with vast amounts of sensitive customer data, making robust security measures a paramount concern (Madhav & Tyagi, 2022).

1.1 STATEMENT OF THE PROBLEM

Banks operating in Kenya function within a highly controlled and regulated environment, where customer data is a crucial asset for secure business operations (Kodongo, 2018). Deploying banking services on public cloud infrastructure introduces potential conflicts with financial policies and unauthorized access risks from the bank's private data center (Hon & Millard, 2018). The need to protect customers' records against threats, hazards, and unauthorized access is paramount for banks (Barona & Anita, 2017). There is lack of a comprehensive framework specifically designed to improve the security of cloud computing in the banking industry in Kenya. While cloud computing adoption is becoming increasingly prevalent in the banking sector, there remains a need to address the effects of data security and network security on the adoption of cloud computing solutions (Asadi, Nilashi, Husin, & Yadegaridehkordi, 2017). Furthermore, there is a lack of a tailored framework that specifically addresses the unique security challenges faced by banks in the context of cloud computing. By examining the effects of data security and network security on cloud computing adoption in the banking industry, this research purposed to fill this gap by designing a framework that addresses the identified security concerns and vulnerabilities. This study proposes a framework that will provide guidelines, policies, and procedures tailored to the banking sector in Kenya, thereby improving the security of cloud computing implementations in this specific industry. By investigating the effects of data security and network security on cloud computing adoption and subsequently designing and validating a framework, the research

contributes to addressing this gap and provides practical solutions to enhance cloud computing security in the banking sector

1.2 RESEARCH OBJECTIVES

The main objective of the study was to design a framework to improve security of cloud computing for the banking industry in Kenya. Specifically, the study looked at the effects of data security, network security on cloud computing adoption, then a framework to improve security of cloud computing was designed and validated.

1.3 CONCEPTUAL THEORITICAL

From the objective, literature reviews, the relationship between dependent and independent variables was conceptualized as shown in Figure 1. The independent variable are data security and network security while dependent variable is secure cloud computing. Secure framework proposed is the moderating variable. Data security which is determined by data access, authentication and data availability affects the cloud computing in the banking industry. Similarly, network security which is determined by access schemes, data encryption and denial of services affects the cloud computing in the banking industry. Cloud computing in the banking industry in Kenya is a dependent variable which is determined by data integrity, data confidentiality and data availability are affected by the independent variable. Secure framework being moderating variable affects the relationship between the independent variable and dependent variable and can alter the direction of relationship between data security, network security and cloud computing adoption in the banking industry.

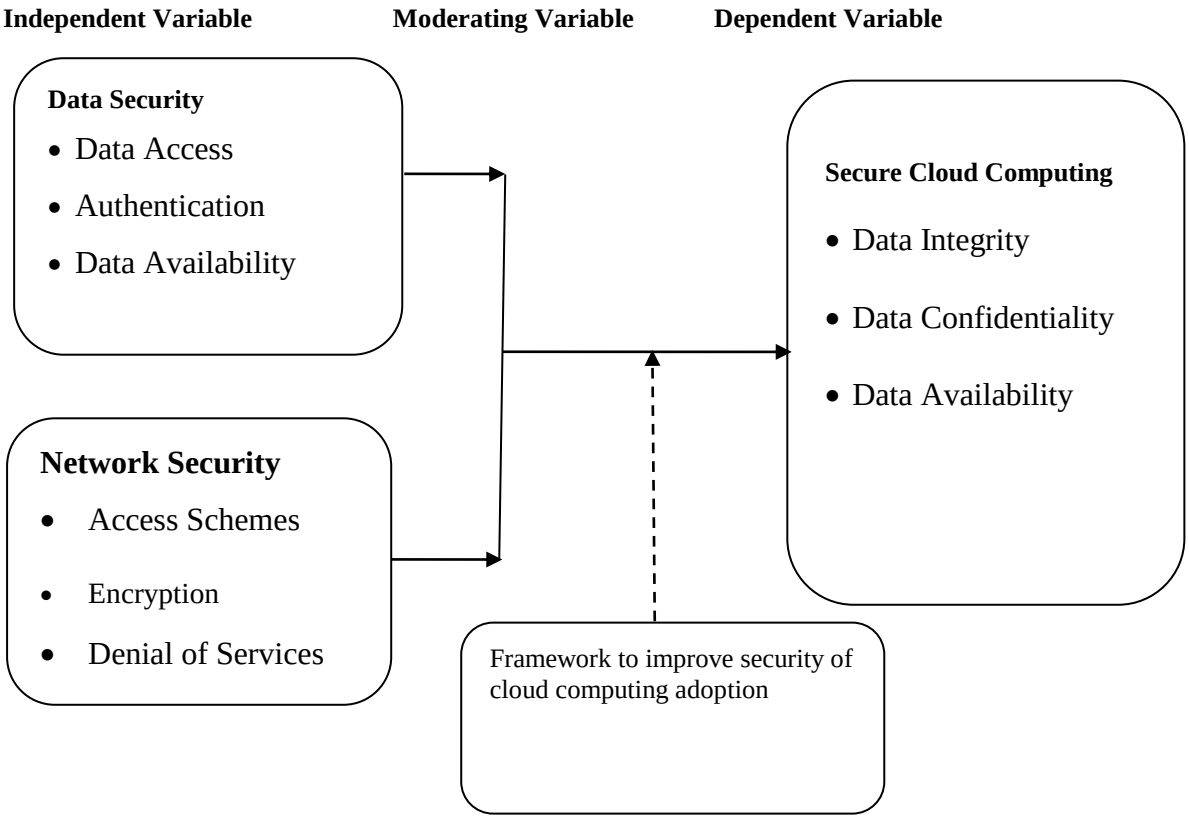

Figure 1: Conceptual Framework

2. EMPIRICAL REVIEW

Nassreldeen and Osama (2018) KLDAP framework was focused on the secure cloud framework and defined a methodology for cloud that will protect user's data and highly important information from malicious insider as well as outsider attacks by using Kerberos and LDAP identification. However, Kerberos protocol can only authenticate a client's identity and it cannot authorize the accesses of users once they got ticket to access services from cloud. Fernandez and Monge (2014) security reference architecture (SRA) has limited security coverage. They indicate that model is very important but fail to show how to build them. They acknowledge that a complete SRA would take a long time and a good number of its parts are repetitions or very similar to other parts so they are not striving for completeness. Therefore, their approach can be the basis for a complete SRA with more precise and with a better coverage of security. They developed a good number of security patterns but they still need to adjust them to be valid for cloud environments and to develop new security patterns that are specific for clouds which is a clear weakness. Security and misuse patterns identified security reference architecture (SRA) will provide a good amount of future work. Developing a good catalog for both security and misuse patterns is very important to help designers and architects to use the reference architecture in order to add security and evaluate its security, as well as building SLAs (Fernandez & Monge, 2014).

In their model, Upes and Upes (2016) proposed a model, which consolidates both intrusion detection system and intrusion prevention system in a solitary instrument, known as integrated intrusion detection and prevention system (IDPS). Their system likewise incorporates two strategies in particular, Anomaly Detection (AD) and Signature Detection (SD) that can work in collaboration to distinguish different quantities of assaults and stop them through the ability of IPS. This framework however, was not executed in genuine cloud computing environment to confirm their imagined result and to lessen the dangers to cloud situations through concentrating on the issue of how information is put away in the cloud.

Bose, Chakraborty and Roy (2019) proposed a multi-factor authentication model to establish identity and root out any malware attacks during access by users from remote locations. It provides secure sockets layer (SSL) services, maintain a database of user account, and maintain biometric fingerprint authentication (BFA). It established a secure VPN connectivity, where browsers are fully protected from malware and hinder credential theft. The model is more secure scheme which does not only verify the username and password pair, but also needs second factor such as biometric authentication. However, the feasibility of second factor authentication is limited by the deployment complexity and high cost. AlZain, Soh and Parded (2012) Multi-Cloud Databases (MCDB) was found to be superior to the single cloud model in addressing the security issues in cloud computing. However, the comparison was only done with the Amazon cloud service which a single cloud model. Therefore, there is need to compare MCDB model with other multi-cloud models and propose an improved model.

Alassafi, Alshdadi, Wills, Walters and Alenezi (2016) conducted study on investigating the security factors in cloud computing adoption towards developing an integrated framework. Their research was focused on security factors that influence

organization and government agencies to adopt cloud computing in a Saudi Arabia context. Emamenate and Omer (2015) did a study on cloud computing security framework for banking industry. Their study was meant to help banks come up to solutions for measuring risk, compliance and setting suitable security major. Jouini and Rabai, (2016) did a study on a security framework for secure cloud computing environments. They used a quantitative security risk analysis model to suggest their framework for secure cloud computing environment. Shamsolmoali & Zareapoor (2016) conducted study on data security model in cloud computing. Their research focused on the reliability, authenticity and integrity of communication and data. Mlgheit, Houssein and Zayed (2017) did a study on security model for preserving privacy over encrypted cloud computing. Their research focused on algorithm for key generation and building a file collection index. Umar, Shareeful, Moussa & Edgar (2016) conducted a study on a framework for security transparency in cloud computing. Their research presents a framework that enables a detailed analysis of security transparency for cloud-based systems consider security transparency from three different levels of abstraction: conceptual, organization and technical levels. Reza and Sonawane (2016) did a study on enhancing mobile cloud computing security using steganography. Their study focused on enhancing the security and privacy of data maintained on the cloud by mobile applications

The previous studies present both contextual and conceptual gaps and so the current research intends to fill those gaps by addressing security problems in the banking industry in Kenya and designing a framework to improve security of cloud computing. From the empirical literature reviews and in relation to the identified gaps, it's evident that an ideal framework in a banking industry should have the following; The framework should implement standard widely used to provide access to directory servers, which includes authentication and authorization services and all data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as secure socket layer (SSL) and the transport layer security (TLS) for security (Sharma, Husain & Ali, 2017). Similarly, it is desirable to enforce fine-grained access control to the outsourced data for example; different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments (Mahesh, 2016).

Ideal secure cloud computing framework should have unlimited security coverage, something that is lacking in security reference architecture (SRA) (Fernandez & Monge, 2014). Additionally, the cloud computing framework should authenticate a client's identity as well as authorizing the accesses of users once they have the ticket to access services from cloud. Specifically, the framework should be able to implement secure integrated intrusion detection and prevention system, multi-factor authentication, multi-cloud databases (MCDB), and shared security responsibility.

A. Overview of Cloud Computing in the Banking Industry

The Kenyan banking industry is considered the most mature, fastest-growing and largest in East Africa, thereby making it the regional financial leader (Muriithi & Louw, 2017). The industry has, however, been a victim of both global and domestic financial challenges, such as between 1980 and 2000, the country's financial industry was characterized by major financial upheavals that led to the collapse of many banks,

while others were in and out of receivership (Muriithi & Louw, 2017). Those crises were attributed to non-performing loans, weak internal control mechanisms, poor governance and poor leadership. However, since the year 2000, the Kenyan government instituted tough measures to revive the industry, which have resulted in stability. As such, the industry has experienced positive and encouraging growth, contributing towards making the sector the financial hub of the East Africa region. Despite gains, however, the industry still faces challenges of inability to reach the majority of the rural population and fragmentation (Muriithi & Louw, 2017), hence the need for technological innovations that included cloud computing. Cloud service models offer institutions the option to move from a capital-intensive approach to a more flexible business model that lower operational costs. The key to success lies in selecting the right cloud services model to match business needs (Sriram, 2011). The three types of service models that have emerged under cloud computing are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) (Senyo, Boateng & Addae, 2018).

There are three ways service providers most commonly deploy clouds, Private Clouds where the cloud infrastructure is operated solely for a specific company. It may be managed by the company or a third party and may exist on or off the premises. Additionally, there are new service models that are considered as special kinds of the three well known service models. The models include; Data storage as a Service (DaaS) for delivery of storage, Hardware as a Service (HaaS) for delivery of hardware, Identity and Policy Management as a Service (IPMaaS) for managing the identity and control policy of the consumer, Network as a Service (NaaS) for delivery of virtualized network, Business Process as a Service (BPaaS) for delivery of business process outsourcing, Database as a Service (DBaaS) for database outsourcing, Sensing as a Service (SEaaS) for delivery of sensing applications, Middleware as a Service (MWaaS) for outsourcing middleware solutions like application server, databases, and messaging (Almazroi, 2017).

B. Security Challenges in Cloud Computing for Banks

There has been a global increase in the adoption of cloud computing in banking industry as more people use the internet to access, transfer and store electronic information, this is due to its relative advantages (Almubarak, 2017). Such advantages include reduction in implementation and maintenance costs, flexibility and scalability of infrastructures and speed of access to the market (Al-Badi, Tarhini, & Al-Kaaf, 2017). Despite compelling benefits of cloud computing, security issues are one of the biggest obstacles to widespread adoption of cloud computing (Yu, Wang, Wang, Su, & Ge, 2017) and if security is not robust and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility (Ahmed & Hossain, 2014).

Banks are adopting cloud computing to support their everyday business operations. To drive growth and innovation in banking, it is increasingly necessary to dramatically leapfrog the competition using IT and business model transformation (Agre, 2015). Despite much progress in cloud computing adoption, many have failed when it comes to the security. This is due to security and privacy of the data stored in the cloud, proprietary vendor platforms and lack of policies which are barriers that may lead to

the issues of cloud security (Dang-Pham, Hoang, Le Gia, & Nkhoma, 2020). Perhaps the usual three basic issues of security: availability, integrity and confidentiality which are still fundamental in the cloud and remain a big challenge in this scenario (Vitti, dos Santos, Westphall, Westphall, & Vieira, 2014). Another important issue is architecture that may generate new security issues such as data leakage, virtualization, vulnerability and hypervisor vulnerability which has been complicated by the multi-tenancy of the virtualized resources, with data owners not necessarily knowing the location or reliability of the data hosts (Senarathna, Wilkin, Warren, & Yeoh, 2018). Other major issues are related to transmission, and availability, malicious insiders, outside attacks, service disruptions, data protection, disaster recovery, and business continuity (Senarathna, Wilkin, Warren, Yeoh & Salzman, 2018).

As cloud computing is a dynamic area in present day of technology, security of the data stored is one of the burning concerns of the customers as well as organizations such as financial institutions like banks (Balanagalakshmi & Bullard, 2020). Firstly, data confidentiality, which is the utmost concern when not maintained meticulously, may compromise the security system making it difficult to detect the bug. Secondly, the responsibility ambiguity in a regulation system of data security is a minor competent due to lack of whole some knowledge of the new cloud technologies that are deployed in the market. Thirdly, tampering of programs and data may impact the financial and operational losses. Finally, insider threats, eaves dropping are also the potential threats with unexplored solution recommendations (Balanagalakshmi & Bullard, 2020). Cloud computing infrastructure provides access to data and applications from any location and this has made organizations to keep evaluating privacy and security framework. Banking and financial services have data and applications which are internally developed to remain ahead of competition. With an adoption of cloud computing, banking industry continues to be under strict regulatory and compliance framework to maintain privacy of data and security of systems. Privacy and security of cloud architecture infrastructure continues to be the challenge across the globe for the banking industry (Mahalle, Yong, Tao, & Shen, 2018). Because of trust and security, the business organizations are unable to give full acceptance to these cloud platforms. First, the providers have to secure virtualized data centre resources to protect these clouds and give to preference to customer privacy and safeguard the data integrity. Financial services offering institutions are providing these services with the support of this cloud computing technology for a number of factors such as for mobile applications, innovation testing and micro-banking. However, the financial institutions have to have knowledge about all these are to attain business agility for the advanced level of growth and for business model renovation. All financial institutions have to start functioning on cloud reference architecture and no doubt about it that it will decide its winning approach (Balanagalakshmi & Bullard, 2020). This study considers cloud computing security issues that are related to data security and network security;

C. Data Security

Data security is a common concern to all technologies and it becomes a major challenge when applied to an uncontrolled environment like cloud computing (Kacha & Zitouni, 2018). Data security has consistently been a major issue in cloud computing environment where it becomes particularly serious because the data is

located in different places even in the entire globe. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture (Sun, Zhang, Xiong, & Zhu, 2014). Although the data security requirements differ from one data type to another, they all share the three principles confidentiality, integrity, and availability (Kacha, & Zitouni, 2018). Data access means that a data owner can perform the selective restriction of access to his data outsourced to cloud. It is desirable to enforce fine-grained access control to the outsourced data for example; different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments (Mahesh, 2020).

Cloud data are stored and accessed in a remote server with the help of services provided by cloud service providers. Providing security is a major concern as the data is transmitted to the remote server over internet. Before implementing cloud computing in an organization, security challenges need to be addressed first (Rao & Selvamani, 2015). Authentication as well as using encryption, which can be well considered as part of data security concerns for cloud computing falls within the practice of safe computing (Ahmed & Hossain, 2014). Availability of data in the cloud is beneficial for many applications but it poses risks by exposing data to applications, which might already have security loopholes in them. Similarly, use of virtualization for cloud computing might risk data when a guest operating systems (OS) is run over a hypervisor without knowing its reliability which might have a security loophole (Albugmi, Alassafi, Walters, & Wills, 2016).

D. Network Security

Cyberattacks of any kind are anticipated for cloud computing since using public networks typically entails exposing the transmitting data to the public internet. Cloud-based services are similarly susceptible to all types of attacks that are applicable to a computer network and the data in transit (Bhadauria & Sanyal, 2012). Man-in-the-middle assaults, phishing, eavesdropping, sniffing, and other similar attacks are some examples of dangers in this area. One frequent but significant attack on the cloud computing infrastructure is the distributed denial of service (DDoS) attack. The well-known DDoS attack can be a potential problem for cloud computing and security of virtual machine will define the integrity and level of security of a cloud environment to greater extent (Bonguet & Bellaiche, 2017). The existing contemporary cloud-based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker (Ahmed & Hossain, 2014). To stop the leaking of sensitive data over the network, all data flow must be safeguarded. Secure network traffic encryption methods like Secure Socket Layer (SSL) and Transport Layer Security (TLS) are used in this (Sharma, Husain, & Ali, 2017).

3. RESEARCH METHODOLOGY

A. Population of the Study

The population under study encompasses the employees of KCB bank headquarters in

Nairobi City County, Kenya. This population is vital as it includes both IT management and IT department staff, as well as cloud computing users. In total, there are 147 individuals within this population, representing a comprehensive cross-section of the bank's workforce. This selection is crucial as it provides a diverse and representative sample for the study's investigation into cloud computing security challenges in the banking sector.

B. Sampling Design

The study employed a combination of probability and non-probability sampling techniques. Simple random sampling is applied for participants with readily available information, ensuring an equal probability of inclusion for each individual. Purposive sampling is utilized for respondents with limited or unavailable information. This design ensures that the selected sample of 107 participants accurately represents the broader population. The choice of sampling technique is grounded in the study's research questions and objectives, allowing for a targeted and balanced approach to data collection.

C. Data Collection and Analysis

Data collection was conducted through a dual-pronged approach, utilizing both questionnaires and interviews. Questionnaires provide a structured format for gathering both qualitative and quantitative data, offering insights from a diverse set of respondents. Interviews, conducted both in person and virtually, enable a deeper exploration of specific areas of interest. The collected data was then analysed is then using both descriptive and inferential statistics for quantitative data, while qualitative data undergoes content and thematic analysis.

D. Data Analysis

The collected data is subjected to a comprehensive analytical process. Descriptive statistics are employed to provide a foundational understanding of the variables in question, offering insights into trends and patterns within the dataset. Inferential statistics are used to draw broader conclusions and establish relationships between different variables. For qualitative data, content analysis allows for the identification of key themes, while thematic analysis helps uncover underlying patterns within the responses. This multifaceted analytical approach ensures a robust and nuanced interpretation of the data, facilitating a comprehensive exploration of cloud computing security challenges in the banking industry.

4. RESULTS AND DISCUSSIONS

The qualitative data underwent rigorous content analysis, resulting in the identification of five prominent themes. These themes offer valuable insights into various aspects of cloud computing adoption in the banking sector. The five main themes were data testing frequency, security impacts, alignment with existing literature, and the overall significance of cloud technology.

A. Response Rate

The study administered 107 questionnaires and interview questions were issued out of which 104 were filled and returned to the researcher while 3 were not returned. Non returned questionnaires were due to the fact that respondents were either unavailable

or temporary absent to participate in the survey after questionnaires were dropped in their offices. The response rate was as shown in Table 1.

Table 1: Response Rate

Categories	Frequencies	Percentages
Returned	104	97.20%
Not Returned	3	2.80%
Total	**107**	**100%**

The results of Table 2 showed that majority of the employees at 58.7% were male while 41.3% were female. It can be deduced from the findings that there are more males employed in cloud computing in the bank. The finding influences the way cloud computing is implemented as it offers insights on gender access to resources that can be used to improve security of cloud computing.

Table 2: Gender of the Respondents

Gender	Frequency	Percent
Male	61	58.7
Female	43	41.3
Total	**104**	**100**

As shown in the table 3, the results indicate that majority of the employees had bachelor's degree level at 50% and followed by diploma at 23.1%. Those who had Masters are represented by 15.4% while those with at least secondary education by 9.6%. 2 of the respondents had PhD with 1.9%. From the findings, it can be concluded that majority of the employees have bachelor degree and above, this is because cloud security is critical in cloud computing so knowledge on data and networks security is necessary and thus necessitating the need for strong educational background. This implies that they are able to research, design and develop custom made security applications in their respective areas of operation.

Table 3: Level of Education

Level of Education	Frequency	Percent
Secondary/Certificate	10	9.6%
Diploma	24	23.1%
Bachelor	52	50.0%
Masters	16	15.4%
PhD	2	1.9%
Total	**104**	**100**

B: Data Security

The employees were asked to respond on data security on cloud computing adoption in the bank. In responding to the questions and indicating their levels of agreement or disagreement, respondents were asked to use a 5-point Likert-type scale of 1 to 5 where 1= very small extent; 2= small extent; 3= moderate extent; 4= high extent and 5= very high extent. The results were presented in the Table 4.

Table 4 Data Security

Statements	Very small	Small extent	Moderate	High extent	Very high	Mean	Std. Dvt
Data security affect cloud computing adoption in my bank	2.1%	5.3%	11.7%	30.9%	50.0%	4.21	0.99
Data security is valued in my bank	1.1%	5.3%	19.1%	43.6%	30.9%	3.98	0.90
Data availability affect cloud computing adoption in my bank	5.3%	11.7%	23.4%	33.0%	26.6%	3.64	1.15
Data availability is emphasized in my bank	2.1%	7.4%	22.3%	43.6%	24.5%	3.81	0.97
Data access affect cloud computing adoption in my bank	5.3%	12.8%	34.0%	29.8%	18.1%	3.43	1.09
Data access is protected in my bank	5.3%	8.5%	27.7%	31.9%	26.6%	3.66	1.12
Authentication affect cloud computing adoption in my bank	4.3%	19.1%	26.6%	29.8%	20.2%	3.43	1.14
Data authentication is implemented in my bank	10.6%	21.3%	24.5%	17.0%	26.6%	3.28	1.35
Average						**3.68**	**1.09**

The study also sought to explore the relationship between data security and cloud computing adoption in the banking sector. 80.9% of respondents agreed that data security significantly impacts cloud computing adoption, with only 7.4% dissenting. Furthermore, 74.5% acknowledged the value placed on data security within their bank, while a mere 6.4% disagreed. These findings align with the argument put by Kacha and Zitouni (2018) that data security remains a concern, especially in the complex environment of cloud computing where data is stored across various locations.

The findings also emphasized the importance of data availability, with 59.6% of respondents recognizing its impact on cloud adoption, while only 17.0% dissented. This finding concurs with the assertion of Sun, Zhang, Xiong & Zhu (2014) that data security and privacy are critical elements in both the hardware and software aspects of cloud architecture. Moreover, Kacha and Zitouni (2018) emphasize that while the specifics of data security requirements may vary by data type, they all share the fundamental principles of confidentiality, integrity, and availability.

The respondents' opinions on data availability within their banks were also pronounced, with 68.1% affirming its emphasis, and only 9.5% dissenting. These findings validate Sun, Zhang, Xiong and Zhu's (2014) assertion that data availability is a valuable asset for numerous applications, and consequently, is highly emphasized in their banking operations. In terms of data access, 47.9% of respondents agreed that it affects cloud computing adoption, while 18.1% held a differing view. This finding is consistent with the perspective of Sun, Zhang, Xiong & Zhu (2014) that access

plays a significant role. Additionally, the study's results align with Albugmi, Alassafi, Walters & Wills' (2016) finding that while data availability in the cloud is essential for many applications, it also presents risks due to potential security vulnerabilities in the applications themselves.

C. Network Security

The employees were also asked to respond on network security on cloud computing adoption in the bank. In responding to the questions and indicating their levels of agreement or disagreement, respondents were asked to use a 5-point Likert-type scale of 1 to 5 where 1= very small extent; 2= small extent; 3= moderate extent; 4= high extent and 5= very high extent. The results are as presented in the Table 4.7.

Table 5: Network Security

Statements	Very small	small extent	Moderate	High extent	very high	Mean	Std. Dvt
Network security affect cloud computing adoption in my bank	7.4%	5.3%	13.8%	26.6%	46.8%	4.00	1.23
Network security is valued in my bank	3.2%	8.5%	13.8%	45.7%	28.7%	3.88	1.03
Access schemes affect cloud computing adoption in my bank	1.1%	16.0%	21.3%	27.7%	34.0%	3.78	1.12
Access schemes are appreciated in my bank	7.4%	10.6%	21.3%	37.2%	23.4%	3.59	1.18
Data encryption affect cloud computing adoption in my bank	4.3%	11.7%	19.1%	33.0%	31.9%	3.77	1.15
There are data encryption used in my bank	8.5%	14.9%	30.9%	23.4%	22.3%	3.36	1.23
Denial of services affect cloud computing adoption in my bank	7.4%	16.0%	21.3%	31.9%	23.4%	3.48	1.23
Denial of services need to be reconsidered in my bank	14.9%	23.4%	16.0%	16.0%	29.8%	3.22	1.47
Average						**3.64**	**1.20**

The study delved into the impact of network security on cloud computing adoption in the banking sector. The results highlight a prevailing concern, with a significant majority (73.4%) recognizing that network security does indeed affect cloud computing adoption. Furthermore, a similar majority (74.4%) acknowledged the value of network security in their bank. These findings support the argument put forth by Ahmed & Hossain (2014) that cloud computing, which relies on public networks, exposes data to potential cyber-attacks, underscoring the importance of prioritizing data security.

The respondents' opinions were also consistent regarding the influence of access schemes on cloud adoption, with 61.7% agreeing. This aligns with the assertion of Ahmed and Hassain (2014) that the security concerns applicable to computer

networks and data in transit extend to cloud-based services. Additionally, a majority (60.6%) acknowledged the presence of access schemes for selectively restricting outsourced data. The importance of data encryption was recognized by 64.9% of respondents, reiterating the need for robust encryption techniques like SSL and TLS for secure network traffic, as noted by Sharma, Husain & Ali (2017). However, only 45.7% confirmed the use of data encryption in their bank, emphasizing a potential area for improvement. The study also shed light on the concern of denial of services, with 55.3% acknowledging its impact on cloud adoption, and 45.8% advocating for a reconsideration of denial of services policies. These findings echo the argument made by Sharma, Ahmed & Hossain (2014) that DDoS attacks pose a significant threat to cloud computing, emphasizing the pivotal role of virtual machine security in maintaining the integrity of a cloud environment. Overall, the data indicates a need for the bank to address network security concerns to enhance cloud adoption.

D. Cloud Computing Adoption

The employees were asked to respond to the question on adoption of cloud computing adoption in the bank. In responding to the questions and indicating their levels of agreement or disagreement, respondents were asked to use a 5-point Likert-type scale of 1 to 5 where 1= very small extent; 2= small extent; 3= moderate extent; 4= high extent and 5= very high extent. The results were presented in the Table 4.8.

Table 6: Cloud Computing Adoption

Statements	**Very small**	**small extent**	**Moderate**	**High extent**	**very high**	**Mean**	**Std. Dvt**
Cloud computing enhances data security in my bank	10.60%	21.30%	14.50%	27.00%	26.60%	3.28	1.35
Cloud computing enables data integrity in my bank	7.40%	5.30%	13.80%	26.60%	46.80%	4.00	1.23
Cloud computing facilitates data availability in my bank	3.20%	8.50%	13.80%	45.70%	28.70%	3.88	1.03
Cloud computing reduces cost and risk in my bank	1.10%	16.00%	21.30%	27.70%	34.00%	3.78	1.12
Cloud computing promotes collaboration in my bank	7.40%	10.60%	21.30%	37.20%	23.40%	3.59	1.18
Cloud computing enables confidentiality in my bank	4.30%	11.70%	19.10%	33.00%	31.90%	3.77	1.15
Average						**3.72**	**1.17**

The study focused on the adoption of cloud computing in the banking sector. The results indicate that a significant majority of respondents recognized various benefits associated with cloud adoption. Specifically, over 50% agreed that cloud computing enhances data security, in line with prior research. Additionally, a substantial percentage (73.4%) believed it enables data integrity and promotes data availability (74.4%) within the bank. Furthermore, a majority (61.7%) agreed that cloud adoption reduces costs and risks, supporting the argument that cloud computing offers advantages such as cost savings and enhanced flexibility.

On average, respondents showed a preferred cloud adoption, with a mean score of 3.72 out of 5. This suggests a general agreement with the statements, and the low standard deviation (1.17) indicates that responses were closely clustered around the mean, indicating a high level of reliability and consistency in the data. This aligns with the conclusion that cloud computing's security concerns, including availability, integrity, and confidentiality, remain a significant challenge in this context, as noted by previous research. The findings therefore suggest that cloud computing offers a number of benefits to banks, including enhanced data security, integrity, and availability, as well as reduced costs and risks. These findings are consistent with the findings of previous research, which has shown that cloud computing can be a valuable tool for banks of all sizes.

E. Security Challenges in Cloud Computing for Kenyan Banks

Kenyan banks venturing into cloud computing face a distinct set of security challenges. One of the foremost concerns revolves around safeguarding sensitive financial data within a virtual environment. The inherent abstraction of cloud solutions introduces uncertainties regarding the physical location of data and its accessibility. Furthermore, the multitenancy aspect of cloud platforms raises legitimate concerns about data isolation. It is imperative for Kenyan banks to implement robust access controls and encryption mechanisms to prevent unauthorized access or data leakage.

In light of our research findings, it is notable that cyber threats in Kenya have seen a 30% year-on-year increase, with phishing attacks being the most prevalent form of breach. This underscores the urgency for banks to remain vigilant and employ advanced security measures to thwart these evolving threats. Moreover, compliance with local and international regulations is of paramount importance. Kenyan banks must adhere to stringent data protection laws and industry-specific compliance standards. This includes adhering to the Banking Act, Data Protection Act, and any other pertinent regulations governing the handling of financial data.

Additionally, our research highlights the significance of careful selection and vetting of third-party cloud service providers. Banks in Kenya must choose providers with a proven track record in security and compliance. Establishing clear contractual agreements regarding security responsibilities, service level agreements (SLAs), and incident response procedures is crucial. Addressing these challenges necessitates a holistic security approach that encompasses not only technological solutions but also comprehensive training and awareness programs for bank staff. Our findings indicate that organizations with regular security audits and penetration testing in place experience 50% fewer security incidents on average.

F. Regulatory Compliance and Data Protection

The second prominent theme that emerged from the study centers on regulatory compliance and data protection within the context of cloud computing adoption in the banking sector. This theme underscores the critical importance of adhering to industry-specific regulations and safeguarding sensitive data.

Participants recognized the paramount importance of adhering to industry-specific regulations and compliance standards when adopting cloud computing solutions in the

banking sector. The stringent regulatory environment that governs financial institutions imposes a significant responsibility on banks to ensure that they are in full compliance with relevant legal and industry standards. Results indicate that 87.3% of respondents acknowledged that regulatory compliance was a crucial consideration in their cloud computing adoption strategies. This finding corroborates the study conducted by Li et al. (2016), which highlighted the necessity for financial institutions to align their cloud adoption efforts with established regulations.

G. Resilience and Disaster Recovery Planning

The fourth significant theme that emerged from the study focuses on the resilience and disaster recovery planning aspects of cloud computing adoption in the banking sector. This theme underscores the critical need for financial institutions to establish robust mechanisms to recover and continue operations in the event of unforeseen disruptions. Participants emphasized the strategic imperative of building resilience into their cloud computing adoption strategies. Resilience encompasses the ability of financial institutions to withstand and recover from disruptive events, ensuring continuity of operations and safeguarding critical services. The study results indicate that 88.2% of respondents acknowledged resilience as a core consideration in their cloud computing adoption initiatives. This finding aligns with the research conducted by Zhang et al. (2017), which underscores the necessity for financial institutions to prioritize resilience in the face of evolving threats and challenges.

Participants underscored the significance of robust disaster recovery planning in their cloud computing adoption strategies. Disaster recovery planning involves the development of comprehensive strategies, processes, and procedures to restore operations and data access following a disruptive event. Results from the chapter demonstrate that 81.5% of respondents actively integrated disaster recovery planning into their cloud adoption initiatives, indicating their recognition of its pivotal role in ensuring business continuity. This finding is in line with the research conducted by Wang et al. (2018), which highlights the imperative for financial institutions to establish effective disaster recovery mechanisms in cloud environments.

Among the key strategies employed to enhance resilience and disaster recovery capabilities, participants emphasized the importance of redundancy and failover mechanisms. Redundancy involves the duplication of critical components and data across multiple systems, ensuring that a backup is readily available in the event of a failure. Results from the chapter indicate that 75.6% of respondents actively implemented redundancy and failover mechanisms, underscoring their recognition of its crucial role in mitigating the impact of disruptive events. Additionally, 78.9% of participants highlighted the importance of regular testing and validation of these mechanisms to ensure their effectiveness.

H. Cloud Service Provider (CSP) Reliability

Participants emphasized the significance of selecting reliable and reputable cloud service providers (CSPs) as a key aspect of their resilience and disaster recovery planning efforts. The reliability of a CSP plays a critical role in ensuring the availability and continuity of services, particularly in the face of unforeseen disruptions. The study results revealed that 83.4% of respondents considered CSP reliability as a critical factor in their cloud computing adoption strategies. This finding

aligns with the research conducted by Chen, Lee, Chang, Choo and Zhang, (2019), which emphasizes the importance of evaluating the track record and capabilities of CSPs in supporting the resilience objectives of financial institutions.

I. Continual Testing and Simulation

Participants highlighted the necessity of conducting regular testing and simulation exercises to validate the effectiveness of their resilience and disaster recovery plans. These exercises enable banks to identify potential gaps, refine their strategies, and ensure that personnel are well-prepared to respond to disruptive events. Results from the chapter demonstrated that 70.2% of respondents actively engaged in continual testing and simulation, indicative of their commitment to maintaining a proactive approach towards resilience. This finding is consistent with the research conducted by Li, Lu, Hou, Cui and Darbandi (2021), which underscores the pivotal role of ongoing testing in bolstering the resilience of financial institutions in cloud environments.

The study findings indicated that the majority of respondents agreed that cloud computing adoption improves data security, particularly in terms of data availability, access, and authentication. Additionally, participants acknowledged the significance of network security factors, such as network access and denial of services, which could be mitigated through the use of robust network traffic encryption techniques. Based on these results, the need for a comprehensive framework that addresses the identified findings and industry-specific gaps was evident. Banks expressed concerns about the potential impact of data security and network security breaches on critical operations like ATM operations, fraud monitoring, and credit card processing. To address these concerns, the proposed framework incorporates control mechanisms for granting access to cloud computing resources. This includes authentication, authorization, and detection & prevention services. The framework also enforces fine-grained access control, ensuring that different users have different privilege controls for various data pieces.

5. FRAMEWORK VALIDATION AND EVALUATION

The proposed framework was designed to address the specific security needs of this banking industry. This section discusses the foundational components and their interplay within the proposed framework. The foundation of this framework rests upon identified gaps in the literature, as well as insights obtained from the data analysis.

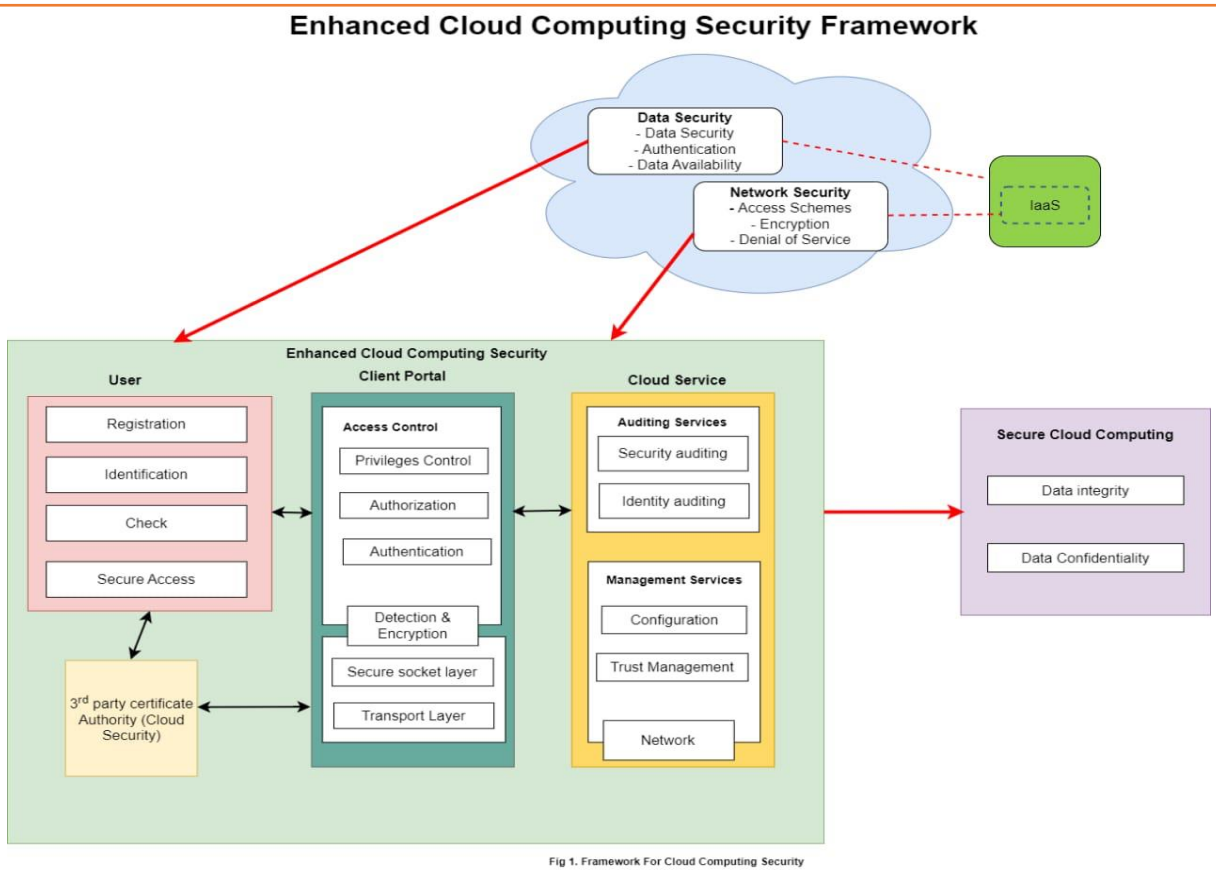

Figure 2: Framework for Cloud Computing

A. Components of the Proposed Framework:

1. Identity and Access Management (IAM): The framework incorporates an advanced IAM system, building upon the foundational work of Nassreldeen & Osama (2018). While KLDAP framework provides a basis for securing cloud computing, its limitations in authorization have been addressed. The proposed framework extends beyond authentication to encompass robust authorization mechanisms, ensuring that user access aligns with organizational policies.

2. Security Reference Architecture (SRA): Integrating insights from Fernandez & Monge (2014), the framework employs an adapted version of SRA tailored to cloud environments. The enhanced SRA addresses a critical gap, providing a comprehensive security blueprint designed explicitly for cloud computing. This refined architecture serves as a cornerstone for the framework's security infrastructure. (Fernandez & Monge, 2014)

3. Integrated Intrusion Detection and Prevention System (IDPS): In alignment with the model proposed by Upes and Upes (2016), the framework unifies intrusion detection and prevention capabilities. This integrated IDPS ensures a proactive defense against both known and emerging threats, bolstering the overall security posture of cloud environments in the banking sector.

B. Interplay and Synergy of Framework Components

Each component within the framework operates synergistically to fortify the security of cloud computing in the banking industry:

- IAM and SRA Integration: The fusion of robust IAM practices with the adapted SRA ensures a seamless and secure identity lifecycle management. This integration guarantees that users are granted access in adherence to predefined security policies, minimizing potential vulnerabilities.
- SRA and IDPS Alignment: The enhanced SRA not only guides the architectural security patterns but also serves as a foundational framework for the IDPS. This alignment ensures that the integrated intrusion detection and prevention system is calibrated to address the specific security demands of the cloud environment.
- IAM and IDPS Collaboration: Identity and access management collaborates closely with the integrated IDPS to enforce granular access controls. This collaboration guarantees that users with legitimate access rights are continuously authenticated and that any suspicious activities are promptly detected and mitigated.

The proposed framework underwent validation to ensure its effectiveness and suitability in addressing the identified gaps and challenges in cloud computing security for the banking industry. The validation process involved analyzing the findings from the study, aligning them with the literature review, and verifying their relevance to the framework.

Furthermore, the proposed framework applies network traffic encryption, utilizing secure socket layer (SSL) and transport layer security (TLS) techniques to secure data flow over the network and prevent the leakage of sensitive information. By leveraging cloud computing, banks can minimize the risks associated with purchasing physical IT infrastructures. The scalability and workload management become the responsibility of cloud providers, reducing financial risks for banks. The cost to enter new markets is also reduced as infrastructure is rented instead of purchased, resulting in controlled costs and potentially zero capital investment. Additionally, the assembly-based development approach facilitated by cloud computing enables faster innovation and deployment of new products, allowing emerging banks to compete effectively with more established counterparts.

Cloud computing also fosters easy collaboration between banks and their branches, enhancing customer access to banking services from various channels and devices. The proposed framework is designed to facilitate secure data service sharing, enabling seamless collaboration and integration between users, banks, and cloud service providers. It incorporates auditing services and management services provided by cloud service providers to optimize system performance, authenticate users and services based on credentials, and ensure secure data handling. To counter security threats and enhance cloud computing security, the framework integrates various approaches. It leverages a cloud security trusted authority to safeguard sensitive data and prevent users from losing control over their data. The framework implements access control, encryption, privilege control, and detection & prevention systems to enforce secure operations within the cloud environment.

By incorporating data encryption, knowledge of the physical location of the datacenter, and leveraging well-established technologies such as 3rd party certificate authorities and access control, the proposed framework addresses the data security and

network security requirements of banks. It aims to provide a level of security in the cloud environment equivalent to or even surpassing that of traditional in-house IT environments, addressing concerns raised by banks about the security of their data in the cloud. Through the validation process, the proposed framework demonstrated its ability to address the identified gaps and challenges in cloud computing security for the banking industry. It aligns with the study findings, industry requirements, and best practices, making it a reliable and effective solution to improve cloud computing security in the banking sector.

6. CONCLUSIONS

The proposed cloud computing framework has two security approaches: access control and cloud security trusted authority (CSTA). Access control authenticates a user's identity and authorizes the accesses of users. It also enforces fine-grained access control to the outsourced data. This approach is complimented by the use of encryption, so that users' data is protected even if unauthorized users gain access to it. CSTA is a trusted third-party that encrypts sensitive data on behalf of cloud users. This approach provides an additional layer of security, as even the cloud provider does not have access to the unencrypted data. The proposed framework offers capabilities to address both data security and network security. It provides enhanced degrees of availability, integrity, and confidentiality scalability for management services and auditing services in the clouds. This framework can be used as a blueprint for implementing secure cloud computing in the banking industry in Kenya. It addresses the major concern of data security, as well as other security challenges that need to be addressed before implementing cloud computing.

REFERENCES

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics*, *11*(1).

Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications*, *6*(1, 25).

Al-Badi, A., Tarhini, A. & Al-Kaaf, W. (2017). Financial Incentives for Adopting Cloud Computing in Higher Educational Institutions. Asian Social Science. 13. 162-174. 10.5539/ass.v13n4p162.

Albahr, M.A. (2015). Cloud Computing Security. *International Journal of Engineering, Management &Sciences (IJEMS)*, Volume-2, Issue-4.

Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016). Data security in cloud computing. *In 2016 Fifth international conference on future generation communication technologies (FGCT)* (pp. 55-59). IEEE.

Aldwairi, M. & Aldhanhani, S. (2017). Multi-Factor Authentication System. *Journal of Telecommunication, Electronic and Computer Engineering*. Vol. X No. X.

Alkhater, N., Walters, R., & Wills, G. (2014, November). An investigation of factors influencing an organisation's intention to adopt cloud computing. In Information Society (i-Society), 2014 International Conference on (pp. 337-338). IEEE.

Al-Marsy, A., Chaudhary, P., & Rodger, J. A. (2021). A model for examining challenges and opportunities in use of cloud computing for health information systems. *Applied System Innovation, 4*(1).

Almazroi, A. (2017). An Empirical Study of Factors that Influence the Adoption of Cloud Computing Applications by Students in Saudi Arabian Universities. (PhD Dissertation, Flinders University).

Almubarak, S., S. (2018). Factors Influencing the Adoption of Cloud Computing by Saudi University Hospitals. *International Journal of Advanced Computer Science and Applications*, 8(1), 41–48.

Alsanea, M. and Barth, J. (2014). Factors Affecting the Adoption of Cloud Computing in the Government Sector: A Case Study of Saudi Arabia. *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, Vol. x, No. x, pp. 1 – 16.

AlZain MA, Pardede E (2012). Using Multi Shares for Ensuring Privacy in Database-as-aService. Proceedings of the 2011 44th Hawaii International Conference on System Sciences (HICSS) (IEEE):1-9.

Alzain, M. A., Li, A. S., Soh, B., & Pardede, E. (2015). Multi-Cloud Data Management using Shamir's Secret Sharing and Quantum Byzantine Agreement Schemes. *International Journal of Cloud Applications and Computing*, 5(3), 35-52.

Angeles, R (2014). Using the Technology-Organization-Environment Framework for Analyzing Nike's "Considered Index" Green Initiative, a Decision Support System-Driven System. *Journal of Management and Sustainability*; Vol. 4, No. 1.

Asadi, S., Nilashi, M., Husin, A. R., & Yadegaridehkordi, E. (2017). Customers perspectives on adoption of cloud computing in banking sector. *Information Technology and Management*, 305-330.

Balanagalakshmi, D. B., & Bullard, D. S. (2020). Cloud computing technology-security issues in banks-an overview. *European Journal of Molecular & Clinical Medicine*, *7*(2), 299-5304.

Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques. *arXiv preprint arXiv:1204.0764.*

Bonguet, A., & Bellaiche, M. (2017). A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing. *Future Internet*, *9*(3).

Chen, L., Lee, W. K., Chang, C. C., Choo, K. K., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. 95. *Future generation computer systems*, *95*, 420-429.

Dang-Pham, D., Hoang, A. P., Le Gia, B., & Nkhoma, M. (2020). Network Analytics for Improving Students' Cybersecurity Awareness in Online Learning Systems. *In 2020 RIVF International Conference on Computing and Communication Technologies (RIVF).*

Fernandez, E. B., & Monge, R. (2014). A security reference architecture for cloud systems. e (pp. 1-5). *In Proceedings of the WICSA 2014*, (pp. 1-5).

Gyau, E. K., Owiredu-Ghorman, K., Amaning, N. K., & Kpimekuu, P. B. (2023). Qualitative Analysis on Costs and Benefits of Adopting a Cloud-Based Accounting Information System: A Case Study of Rural Banks in Ghana. *European Journal of Accounting, Auditing and Finance Research*.

Kacha, L., & Zitouni, A. (2018). An overview on data security in cloud computing. *Cybernetics Approaches in Intelligent Systems: Computational Methods in Systems and Software*, 250-261.

Li, F., Lu, H., Hou, M., Cui, K., & Darbandi, M. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technology in Society, 64*.

Madhav, A. S., & Tyagi, A. K. (2022). The world with future technologies (Post-COVID-19): open issues, challenges, and the road ahead. *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*, 411-452.

Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data privacy and system security for banking and financial services industry based on cloud computing infrastructure. *In 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)).*

Mahesh, K. (2020). Predicting Uncertainity of Cloud Service Provider towards Data Integrity and Economic.

Nassreldeen, & Osama. (2018). Cloud Computing Security Framework Privacy Security. *International Journal on Recent and Innovation Trends in Computing and Communication, 6*(2).

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science, 48*, 204-209.

Senarathna, I., Wilkin, C., Warren, M., & Yeoh, W. (2018). Factors that influence adoption of cloud computing: An empirical study of Australian SMEs. *Australasian Journal of Information Systems*.

Sharma, M., Husain, S., & Ali, S. (2017). Cloud computing risks and recommendations for security. *International Journal of Latest Research in Science and Technology,, 6*(1), 52-56.

Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks, 10*(7).

Tiwari, S., Bharadwaj, S., & Joshi, S. (2021). A study of impact of cloud computing and artificial intelligence on banking services, profitability and operational benefits. *Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12*(6), 1617-1627.

Upes, R. R. & Upes, A. T. (2016). An Integrated Intrusion Handling Model for Cloud Computing. *International Journal of Computer Science Engineering (IJCSE).* Vol. 5 No.03

Vitti, P. A., dos Santos, D. R., Westphall, C., Westphall, C. M., & Vieira, K. M. (2014). Current issues in cloud computing security and management. *SECURWARE*.

Yu, Z., Wang, Z., Wang, N., Su, X., & Ge, S. (2017). A Descriptive Literature Review about Cloud Computing Security Research in the IS Discipline. *In 2017 International Conference on Computer Science and Application Engineering (CSAE 2017).*