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

APPLICABILITY OF CLOUD SECURITY FRAMEWORKS AND MODELS IN THE KENYAN-BANKING SECTOR: A REVIEW

[1*]Ouma Geofrey, [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: May 2024

ABSTRACT

The years from 2007 has seen the Banking industry in Kenya has experience growth and transformation when it comes to technology and this is mostly attributed to the integration of cloud computing. A comprehensive literature review that goes through the multifaceted landscape of cloud security within the Kenyan banking sector has been provided in this article. By Conducting through Framework and model analysis that include KLDAP-RBAC,SRA(Security Reference Architecture), Integrated Intrusion Detection and Prevention System (IDPS), Multifactor authentication and Multi-Cloud Databases (MCDB), this review gives a comprehensive assessment of their strengths, their weaknesses and their ways of application. Cloud security governance concept is examined by using the shared security responsibility model. Mobile cloud computing security integration further characterizes augments of the discussion, addressing the challenges faced by the mobile banking sector. This review is as a foundational resource for banks and stakeholders who have the aim to strengthen their cloud security setup in the dynamic and fast-evolving Kenyan banking setting. Drawing upon these insights, the banking industry can come up with a secure and resilient path toward continued innovation and customer-centric services.

Keywords: *Cloud security, Data Security, Security Frameworks, Security Reference Architecture, Banks, KCB, Kenya*

1. Introduction

Cloud computing can be defined as [1] an internet-based application that provides businesses access to shared resources that include the hardware and software resources, data storage and adaptable business applications when they are needed. One thing about the Kenyan banking industry is that it is considered to be the most mature, largest and fast growing than any other in East Africa. It has seen significant transformations in technological innovations since the year 2007. Significantly one of the most banking sector advancements in the banking sector incorporates cloud computing. These advancements in the sector have seen benefits that include cost savings, scalability and flexibility [2]. Just like any sector, these advancements also present challenges that include but not limited to data loss, illegal system access and denial of service attacks. One good question to ask is why adopt cloud computing as a country? This need is attributed by the need to cut the costs of operations, increase productivity and also to improve customer experience [3]. Cloud computing is being used by various banks in the country to provide a variety of services such as mobile banking, internet banking and ATM banking to its users.

The Kenyan banking industry has witnessed a huge technological transition wich was marked by the introduction of mobile money payment platform locally known as M-Pesa.[4] The vision 2030 economic development strategy describes a subsequent advancement hinged on the widespread use of Information and Communication Technology in Kenya. Technological innovations like mobile money, agency banking, ATMs, and Internet banking, cash transactions and payments are now even faster [5] as a result. These developments cleared the way for the use of cloud computing in the banking industry, which has several advantages including improved operational effectiveness, lower costs, and higher client service quality [6].

[6] contends that using the cloud enables banks to quickly develop their IT systems at a fraction of the cost by using service procurement to obtain infrastructure, development platforms, and application software and avoiding large one-time investments and drawn-out, risky implementation processes. Furthermore, compared to conventional central data warehousing architectures, it considerably improves data processing capabilities, enabling quick storage, processing, and analysis, strengthening the bank's data management skills [6]. Nevertheless, strict information security precautions are required due to the reliance on technology for financial services. Fraud can come about due to lack of security, which would compromise public trust in electronic payment systems and bring about doubt against these technologies. As a result, their acceptance of banking services can be affected [5]. When Integrating cloud computing into the banking industry, security hurdles come up that include problems with data and network security and this must be acknowledged [6].

2 Background

Many benefits, such as lower costs, more flexibility and scalability, and a faster time to market, is growing cloud computing and increasing popularity in the banking sector. One of the largest barriers to widespread use continues to be concerns about security [7]. The benefits of cloud computing remain susceptible and lack credibility without reliable and consistent security procedures. [8] noted that banks are relying on cloud computing to transform their daily operations. The use of IT and business model transformation to outrun the competition is now essential for banks to achieve growth and innovation. However, a lot of people have struggled with security due to concerns with data privacy, proprietary vendor platforms, and a lack of strong policies [9].

The cloud continues to be hampered by important security challenges, such as availability, integrity, and confidentiality [10]. Additionally, due to the multi-tenancy of virtualized resources, architectural complexity creates new security concerns such as breaches of data, virtualization vulnerabilities, and hypervisor vulnerabilities [11]. Several additional urgent problems, such as transmission security, hostile insiders, external attacks, service interruptions, data protection, disaster recovery, and business continuity has complicated the security environment is further [11].

Data security within this dynamic technological landscape, remains a paramount concern for customers and organizations especially in financial institutions like banks [12]. Confidentiality gaps may compromise security systems, while ambiguity in data security regulation exposes a challenge due to limited knowledge of emerging cloud technologies [13]. Tampering of programs and data can lead to significant financial and operational losses, with insider threats and eavesdropping representing additional, yet unexplored, potential threats [14].

Cloud computing gives access to universal data and applications whereas banking institutions continually struggle with the details of privacy and security frameworks. They must present a strict regulatory and compliance framework to safeguard data privacy and system security [15]. Cloud computing does bring out opportunities for mobile applications, innovation testing, and micro-banking services wich has created trust and security. This has been a requirement for full organizational acceptance of these platforms [16]. Therefore, the adoption of cloud reference architecture is becoming weighty for financial institutions, setting the stage for enhanced business agility, growth, and business model evolution [17].

3 Methodology

Twenty six papers that were reviewed and each paper contributed to unique insights and models in cloud computing security. [18] introduced the KLDAP framework, wich is a tough Kerberos Authentication with Role-Based Access Control (KLDAP) system made for cloud computing applications. The aim of this framework tends to strengthen cloud security, DDOS attacks weak, and ultimately promoting client satisfaction through by not allowing direct access. [19] proposed a Wireless-Kerberos (W-Kerberos) framework, focusing on a security architecture for Wireless LANs to cater to both security and mobility needs. The Kerberos Authentication with Cloud Computing Access Control presented by [20], particularly the Kerberos Authentication with Role-Based Access Control (KARBAC) framework. This framework serves as a trusted intermediary between cloud servers and clients, ensuring secure access. [21] extensively evaluated the KARBAC system, underscoring its efficiency in user creation, role assignment, and security management within cloud computing environments. [21] further delved into the development of a Security Reference Architecture (SRA) for cloud systems, concluding that security measures should be integrated throughout the system lifecycle for an effectively secure cloud system.

[22] proposed a SRA (Security Reference Architecture) for Blockchains wich is a standardized model that helps designers that use the platform keeping in place the considerations of vulnerabilities, threats and defenses. Furthermore, [23] advocated for

a Security Reference Architecture (SRA) tailored for Big Data, emphasizing its implementation within a Cloud Computing environment. Additionally, A meta-model by [24], along with security and misuse patterns to construct a Security Reference Architecture (SRA) for cloud systems. This model excels in stopping attacks, not just through identifying or reporting them. Vaishali B. K. (2016) provided an overview of Intrusion Detection System (IDS) models in Cloud Computing, emphasizing their role in protecting cloud environments. [25] examines various Intrusion Detection and Prevention System (IDPS) technologies, emphasizing the benefits of using numerous types for full threat detection. [26] provided a fresh viewpoint on network intrusion detection research, highlighting the significance of necessary, complete, and mutually exclusive intrusion detection types. [27] described the working principles of a cloud-based multi-factor authentication system for the banking industry, demonstrating its efficiency in preventing credential theft and malware. Section 4 discusses selected frameworks that require additional evaluation.

4 Existing cloud security frameworks

According to [28] protecting the cloud ecosystem against vulnerabilities is a challenging and shared obligation between cloud providers and users. The security challenges that cloud providers must recognize and address, the countermeasures that must be put in place, and the controls that must be in place must be at least as effective as the security safeguards that banks would have in place if they weren't using the cloud [29] Understanding the difficulties and investigating current models and frameworks are necessary to create a cloud security framework that is successful. These well-established paradigms can be examined to get insights into optimal practices. It is also possible to determine their relevance and a route to a banking industry cloud computing environment that is more secure [28]. The objective of this inquiry is to equip consumers and service providers with the information and tools they need to safeguard their vital assets and business operations in the dynamic digital era. The following sections examine five cloud security frameworks. The next section reviews five cloud security frameworks.

4.1 KLDAP-RBAC Framework

According to [30], the Lightweight Directory Access Protocol (LDAP) is a widely used standard for providing access to directory servers, which includes authentication and authorization services. [18] designed the Kerberos Authentication with Role Based Access Control (KLDAP) framework for cloud computing applications. This framework works by providing cloud computing customers a policy, permission and role specification module for the access control on their resources. Permissions of the LDAP-RBAC policy are then stored and used to provide access control decisions by the Kerberos authorization server component. For user authentication performed by the Kerberos, user permissions are stored in LDAP by using the KLDAP framework and tickets are used by the secure authentication system to check and verify the identities of users and services [18]. LDAP is used as a lightweight directory to manage and store user data.

KLDAP-RBAC framework has a structured difference in the policy specification module provides a solution for enhancing cloud security. This enables clients by using precision and clarity to have control over access control policies [31]. The overall security is strengthened by ensuring that access rights explicitly outlined and enforced. Framework temporal hierarchy incorporations and separation of duty constraints equips it to function effectively even in resource constrained scenarios making this adaptability a significant asset as it ensures that security measures remain robust not regarding the operational environment [32]. Kerberos is recognized for its robustness and framework’s overall security capabilities through providing a secure foundation for verifying client identities. Incorporation of strong cryptography in the Kerberos protocol facilitates the encryption of communications that guarantees privacy and data integrity even in potentially insecure network connections [33].

Limitations of the KLDAP-RBAC Framework

Limitations of the KLDAP-RBAC majorly arises from its main focus of protocol’s authentication where it’s not quite good at verifying the clients identity and approving subsequent access[34].This can leave a potential gap in the security enforcement process that might bring up additional measures for vigorous access control [18]. The structure also assumes the existence of a dependable administrator who oversees all customers and system responsibilities. This presumption might not hold in the world of reality and particularly in complex systems that has many users. It might be impractical and possibly lead to vulnerabilities to rely solely on one administrator to manage the security and access control of the entire system [35]. KLDAP framework was focused on the secure cloud framework and defined a methodology for the cloud that will protect users' data and highly important information from malicious insider as well as outsider attacks by using Kerberos and LDAP identification. However, the Kerberos protocol can only authenticate a client's identity and it cannot authorize the access of users once they get a ticket to access services from the cloud.

4.2 Security Reference Architecture (SRA)

The security reference architecture (SRA) proposed by [36] utilizes security patterns and Unified Modeling Language (UML) models to ensure the integrity of a cloud computing architecture. It serves as conceptual architecture without implementation information, providing a prototype model of security for cloud computing environment. The SRA is versatile, finding applications in applying security to cloud systems, defining service level agreement (SLAs) evaluating specific cloud systems' security, and various other purposes [36].

Strengths

[36] developed a Reference Architecture (RA) as the foundation of the Security Reference Architecture (SRA), offering a precise view of cloud systems. This standardized, generic architecture provides a high-level abstraction of the system, valid for a specific domain, without implementation details [36]. The SRA enriches this RA by strategically incorporating security mechanisms, effectively fortifying the architecture's overall security [24].

Moreover, SRA uses security patterns which adds precision and clarity to its design. This UML representation and usage of patterns will offer a more precise portrayal of the architecture as compared to traditional models found in its literature. This enhanced precision is essential for addressing security concerns in a comprehensive manner [36]. SRA controls misuse of patterns to address specific security threats further contributing to its robustness [36].

Weaknesses

One limitation of the SRA is in its coverage of security aspects. [36] acknowledges, while their model is significant, it doesn't provide a detailed guide on how to construct them. A complete SRA would require a larger investment of time, and some components will be repeat themselves. Therefore, complete coverage, is not aimed at. This coverage could also be a potential disadvantage for certain applications (Fernandez & Monge, 2014). SRA may require adjustments ensuring its application ability to cloud environments and developing a specific security patterns that is custom-made to cloud computing. This development will indicate a need for further refinement [36].

Security Reference Architecture is a good step towards making a concept that will have an effect cloud security. Utilizing Reference Architecture (RA) and integrating security patterns, it does provide precision and structured approach towards fortifying cloud systems against potential threats [37]. It is important however to acknowledge its limitations in covering and highlighting the need for currently ongoing refinement and development of specific security patterns, for cloud environments.

4.3 Multi-Factor Authentication Model

[38] has proposed a strong multi-factor authentication model, made for remote access to banking applications. This has been done by recognizing the weaknesses and vulnerabilities of single-factor authentication methods. This has been done by advocating for a layered security approach that is aimed at protecting against malware attacks and unauthorized access.

Strengths

The proposed triple-stage verification process has introduced an extra layer of security that establishes identity and mitigates potential malware threats during access to banking applications from remote locations [39]. This is done through incorporating multiple factors, including something that the user knows like his/her username and password, something the user has like the biometric fingerprint authentication, and a transaction code or one-time code. A triple-stage model creates a strong defense and a good prevention measure against un-authorized access [40].

Multifactor authentication (MFA) is seen as a more secure alternative to single-factor authentication (SFA) [41]. Using MFA creates many independent credentials, making it more difficult for attackers to go through all phases. This layered strategy improves security but lowers the possibility of security infractions [41]. Adding biometric fingerprint authentication allows the model to make use of the user's unique physical identity property for verification, this offers an extra degree of security because biometric data is difficult to copy or fabricate [42]. Furthermore, the usage of Secure Sockets Layer (SSL) services and virtual private network (VPN) connectivity improves browsing security by protecting against malware and credential theft [43].

Weaknesses

The proposed model does offer strong security measure and this possibly will introduce some complex and additional steps for its users. There will arise a need for multiple authentication factors, wich include biometric data, transaction passwords and one-time passwords. All that requires additional effort and that potentially leads to undesired user inconveniences [38].

Effectiveness of the model relies on the proper implementation and maintenance of biometric authentication hardware and software. Any weaknesses or vulnerabilities in the biometric authentication process potentially undermines the security of the system [44].

4.4 Multi-Cloud Databases (MCDB) Model

[45] Multi-Cloud Databases (MCDB) security paradigm concept is a complicated technique that combines many cloud services providers in order to improve security and privacy. It is divided into the three Layers that include management, application and presentation. The primary goal of the paradigm is protecting against data intrusion assuring service availability and maintaining data integrity [45]. It successfully protects user data by dispersing data over various clouds and using secret sharing algorithm.

Strengths

The MCDB adopts a multi-cloud approach wich disperses data redundantly and this reduces the risk of unauthorized access or malicious manipulation [47] and thus making it have the ability to get rid of security risks associated with data compromission. Application of the secret sharing algorithm ensures that even if one cloud is compromised, an attacker would not have access to complete data sets thus providing a layer of security [45]. The risk that this model effectively addresses is associated with malicious insiders in the could environment by making use of numerous clouds. A multipurpose and diverse set of database queries provided by the MCDB paradigm ensures that consumers have the tools needed to interact with their data efficiently [48].

Weaknesses

Coordinating and maintaining data across clouds may need more resources and skills [45] and this contributes to a considerable complexity in its implementation. While the approach tackles security issues about data intrusion and integrity, it is critical to ensure the DBMS and communication lines between clouds are safe. Any flaws in these components could jeopardize the security provided by MCDB [45]. The approach performs particularly well in minimizing risks related with insider threats. To fully benefit from the MCDB paradigm, it is critical to guarantee that the underlying components, such as the DBMS and communication channels, are safe [49]. Comparisons with different multi-cloud models may provide more insights into its efficacy.

4.5 Shared Security Responsibility Model

The shared security responsibility framework model shows the security framework of cloud service providers and clients. This shows who is responsible for making certain sections of the cloud environment safe [50]. The approach highlights that, while the cloud computer provider is responsible for the underlying infrastructure, users are responsible for the security of their data, applications, and cloud computing setups [15].

Strengths

a) *Clear Accountability*

Responsibilities of this model are clearly shown through reducing ambiguity and ensuring that both the cloud provider and the customer know their respective roles in cloud security. This transparency is necessary for successful security management [52].

b) *Collaborative security efforts*

Cloud provide and the customer have a role in security. Recognizing this encourages a collaborative approach to cloud resource security. This shared duty promotes communication and coordination among stakeholders, resulting in a stronger security posture [53].

c) *Customizable security measures*

Customers can implement security controls and configurations that match with their specific use cases and compliance standards [54]. The concept enables enterprises to develop security measures that are relevant to their needs and requirements.

Weaknesses

a) *Misinterpretation*

Misinterpretations and misconceptions about the specific distribution of tasks can arise due to the varying shared security responsibility approach. It is critical for enterprises to completely understand the model defined by their chosen supplier [52].

b) *Challenges in Enforcing Customer Compliance*

Ensuring that clients follow their commitments and have followed the proper security measures under a shared security paradigm is quite the challenge for cloud providers [55]. The Shared Security Responsibility Model is a fundamental paradigm for creating accountability in cloud security and a shared Security Responsibility model promotes collaboration and effectiveness in security by clearly identifying the obligations of both cloud providers and customers [56]. Understanding the model's precise details as described by the cloud provider is fundamental for the Enterprises to keep in mind and customers must proactively deploy security measures within their areas of responsibility in order to fully benefit from the shared security model [57].

4.6 Summary of the existing frameworks

Table 1 provides a summary of existing cloud security frameworks and their purpose and contribution to the cloud computing industry.

Table 1: Existing frameworks

Author (s)	**Purpose**	**Framework/ Model/Algorithm**	**Findings/Results/Contribution**
[18]	To design the Kerberos Authentication with Role-Based Access Control (KLDAP) framework for cloud computing applications	KLDAP framework	The solutions proposed here can be implemented in the future to prevent the cloud from direct access, and DDOS attacks and to produce satisfactory improvements in cloud security. This will help to enhance the client's interest and satisfaction.
[19]	A Kerberos-Based Authentication Architecture for Wireless LAN	W-Kerberos Framework/ Architecture	Proposed security architecture trying to satisfy both security and mobility needs
[32]	Kerberos Authentication with Cloud Computing Access Control.	Kerberos Authentication with Role-Based Access Control (KARBAC) framework	Model acts as a trust third party between cloud computing servers and clients to allow secure access to cloud computing services
[36]	Security Reference Architecture (SRA) for cloud systems	SRA security patterns	Concluded that security must be applied throughout the complete lifecycle and that working only with architectures is not enough to build secure systems.
[23]	The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses	The Security Reference Architecture (SRA) model	Presented a security-oriented methodology for designers of block-chains platforms and applications, respecting the proposed SRA
[24]	Towards a Security Reference Architecture for Big Data	Unified Modeling Language (UML) models	SRA emphasizes the idea of a Big Data ecosystem by implementing the system using a Cloud Computing environment.
[25]	Building a security reference architecture (SRA) for cloud systems	UML models	Present a meta-model as well as security and misuse patterns

Author (s)	Purpose	Framework/ Model/Algorithm	Findings/Results/Contribution
[26]	Intrusion Detection and Prevention System: Technologies and Challenges	IDPS technologies	Using multiple types of IDPS technologies can achieve more comprehensive and accurate detection and prevention of malicious activity
[28]	Explaining the workings principle of cloud-based multi-factor authentication architecture in banking sectors	MFA Model	Established a secure VPN connectivity, where browsers are fully protected from malware and hinder credential theft.
[58]	Review: Authentication in Cloud Computing	Surveyed the existing popular security models of cloud computing	The authentication method is the main factor in preserving the security and privacy of each communication in cloud computing.
[41]	Multi-Factor Authentication System	MFA model	The results show that users quickly digested the system, and the probability of a successful brute-force attack is less than6.72 E-25 for the first and second stages combined if you only select 8 items out of 36, which is the total number of items, or 2.7E-17 in the specific case of our implementation
[45]	Multi-Cloud Data Management using Shamir's Secret Sharing and Quantum Byzantine Agreement Schemes	MCDB Model	It has been shown that the multi-cloud model is superior to the single-cloud model in addressing the security issues in cloud computing
[59]	Factors Affecting the Adoption of Cloud Computing in the Government Sector	Model	Contributed to existing knowledge by proposing a novel model for the adoption of cloud technology by the government. This model was tested and verified, and in addition, the study revealed new findings and conclusions.
[60]	The State of Cloud Computing in Nigeria	Model	Issues about data security and privacy on the cloud need to be squarely addressed to engender acceptance of cloud computing

Author (s)	**Purpose**	**Framework/ Model/Algorithm**	**Findings/Results/Contribution**
			technology by businesses and organizations nationwide.
[61]	Cloud Computing Features, Issues and Challenges: A Big Picture.	Discussion on cloud computing architecture, security issues, and platforms for cloud	exhibited scientific classification of issues and the methodologies in which these issues have been handled, concentrating on an operational level, client level, service level, and application level, security and context-awareness
[62]	Cloud computing research: A review of research themes, frameworks, methods, and future research directions	Meta-analysis of 285 articles from 67 information systems	Findings indicate that extant cloud computing literature tends to skew towards the technological dimension to the detriment of other under-researched dimensions such as business, conceptualization, and application domain
[63]	An Empirical Study of Factors that Influence the Adoption of Cloud Computing Applications by Students in Saudi Arabian Universities	Technology Acceptance Model 3 (TAM3)	Identifying and examining the critical factors that influence the students' intention to adopt cloud computing applications in Saudi Arabian universities using the modified TAM3 model.
[64]	Cloud Computing Issues for Higher Education: Theory of Acceptance Model	Theory of Acceptance Model and structured equation modeling	Findings revealed that perceived ease of use affected the intention to use the technology in the future, and intention to use was demonstrated in the teachers' actual use
[65]	Cloud Computing and its Challenges and Benefits in the Bank System	analysis of the security system (strengths and weaknesses)	highlight the current situation of Cloud Computing systems
[66]	Implementation of a Cloud in the Banking Sector	Hybrid Mode analysis	Continued advancement of cloud computing within the banking sector will require vendors and banks to overcome its challenges together

Author (s)	**Purpose**	**Framework/ Model/Algorithm**	**Findings/Results/Contribution**
[67]	A New Conceptual Framework Modelling for Cloud Computing Risk Management in Banking Organizations	Conceptual Framework Modeling for cloud computing Risk management	Successful framework modeling for cloud computing risk management will greatly improve the probability of cloud computing success in banking organizations.
[68]	Data Security Model for Cloud Computing. Journal of Communication and Computer	Data security model	In the authentication phase in the proposed data security model, OTP is used as two-factor authentication software
[69]	Security Model for Preserving Privacy over Encrypted Cloud Computing	Secure Model for Preserving Privacy Over Encrypted Cloud Computing (SPEC)	Reveal that the model can be of better performance than previous ones and will have a good security level as well.
[70]	A Framework for Security Transparency in Cloud Computing	framework that enables a detailed analysis of security transparency for cloud-based systems	The framework allows users to identify their needs for transparency based on a cloud migration strategy and checks how these needs can be satisfied through the cloud service provider’s offerings
[71]	Cloud Computing Security	Encryption framework	Framework ensures secured advancement of data at the client and server end.
[72]	Data Security Model in Cloud Computing	novel data security model	The model ensures data traversing in a cloud computing environment
[73]	Security Framework for Secure Cloud Computing Environments	Multi-dimensional Mean Failure Cost (M2FC)	Envision control of the M2FC by analyzing the cost of various countermeasures that one can deploy in Cloud Computing systems to improve security, and match these costs against the benefits
[74]	Current Issues in Cloud Computing Security and Management	security monitoring tool	shows it is possible to build solutions to cloud security a system based on previous work

Author (s)	Purpose	Framework/ Model/Algorithm	Findings/Results/Contribution
[75]	Investigating the Security Factors in Cloud Computing Adoption: Towards Developing an Integrated Framework	Framework	Towards Developing an Integrated Framework

5 Cloud Security Frameworks for the Kenyan Banking Industry

Kenya's banking sector has seen great significant technical developments in recent years and factors such as increased internet penetration and expanding mobile phone user base have contributed to these technical developments. All these advancements have increased digital banking services that entail mobile and online payments resulting towards protecting sensitive financial data. Adoption of the cloud-based technology comes with the challenges of contenting with the need to comply with regulatory requirements set forth by the Central Bank of Kenya (CBK) that ensures that cloud-based systems meet stringent security standards. The banking sector must address concerns surrounding data privacy, especially in light of recent cyber threats and incidents affecting financial institutions globally. Given the rapid pace of technological adoption in Kenya's banking industry, cloud security frameworks play a critical role in fortifying the sector's resilience against evolving cyber threats. The frameworks under consideration offer potential solutions to secure cloud environments, thereby safeguarding critical financial data and ensuring uninterrupted access to banking services. Evaluating these frameworks within the specific context of Kenya's banking industry is imperative for building a robust security infrastructure that aligns with the sector's unique challenges and regulatory landscape

6 Conclusion

A variety of techniques addressing the challenges of cloud security have been provided by evaluated cloud security frameworks. The KLDP-RBAC framework offers a solid solution that makes formal policy descriptions a priority while admitting potential limits in administrator dependency. Security Reference Architecture (SRA) presents a conceptual model filled with security patterns that demonstrates precision and clarity in design and this may require further refining for specific cloud environments. The Integrated Intrusion Detection and Prevention System (IDPS) provides a unified tool with extensive attack identification and prevention capabilities though its real-world usefulness has yet to be confirmed. The multi-factor authentication architecture developed by Bose, Chakraborty, and Roy provides a strong defense against illegal access and malware threats, but it adds complexity for users. A multi-cloud strategy and secret sharing mechanism is kept in place to reduce data intrusion across many clouds. Finally, the shared security model establishes a core structure for responsibility in cloud security by clearly defining duties and allowing for configurable security measures. Various misinterpretations and the risk of disregarding customer responsibilities highlight the importance of thoroughly understanding this shared model. Each framework has distinct strengths and considerations, emphasizing the significance of customized security solutions in the evolving landscape of cloud computing.

7 References

[1] F. Thabit, S. A. H. Alhomdy and S. B. Jagtap, "Toward a model for cloud computing banking in Yemen," *International Journal of Research in Advanced Engineering and Technology,* vol. 5, no. 4, pp. 14-18., 2019.

[2] K. M. Kituku, *Adoption of cloud computing in Kenya by firms listed in the Nairobi Stock Exchange).,* 2012.

[3] R. Mugyenyi, *Adoption of cloud computing services for sustainable development of commercial banks in Uganda.,* 2018.

[4] S. Musau, S. Muathe, and L. Mwangi, "Financial inclusion, bank competitiveness and credit risk of commercial banks in Kenya," *International Journal of Financial Research,* vol. 9, no. 1, pp. 203-218, 2018.

[5] J. Koori, N. Wanjiku and G. Atheru, "Technological Banking Innovations and Financial Inclusion by Commercial Banks in Nairobi County, Kenya.," *International Journal of Current Aspects in Finance, Banking and Accounting,* vol. 2, no. 1, pp. 1-27, 2020.

[6] G. Yan, "Application of Cloud Computing in Banking: Advantages and Challenges.," *In 2017 2nd International Conference on Politics, Economics and Law (ICPEL 2017),* 2017.

[7] S. Singh, Y. S. Jeong and J. H. Park, "Singh, S., Jeong, Y. S., & Park, J. H. (2016). A survey on cloud computing security: Issues, threats, and solutions.," *Journal of Network and Computer Applications,* pp. 200-222., 2016.

[8] Y. Alghofaili, A. Albattah, N. Alrajeh, and B. A. S. Al-Rimy, "Secure cloud infrastructure: A survey on issues, current solutions, and open challenges," *Applied Sciences,* vol. 11, no. 19, 2021.

[9] N. Akhtar, B. Kerim, Y. Perwej and A. P. Tiwari, "A Comprehensive Overview of Privacy and Data Security for Cloud Storage.," *International Journal of Scientific Research in Science Engineering and Technology.,* 2021.

[10] P. A. F. Vitti, D. R. dos Santos, C. Westphall, C. M. Westphall and K. M. Vieira, "Current issues in cloud computing security and management.," *SECURWARE,* 2014.

[11] I. Senarathna, C. Wilkin, M. Warren, and W. Yeoh, "Factors that influence the adoption of cloud computing: An empirical study of Australian SMEs.," *Australasian Journal of Information Systems,* 2018.

[12] D. B. Balanagalakshmi and D. S. K. Bullard, "Cloud computing technology-security issues in banks-an overview.," *European Journal of Molecular & Clinical Medicine,* vol. 7, no. 2, pp. 5299-5304, 2020.

[13] B. Alouffi, M. Hasnain, A. Alharbi and W. Alosaimi, "A systematic literature review on cloud computing security: threats and mitigation strategies.," *IEEE Access,* pp. 57792-57807., 2021.

[14] E. O. Ekong, "Impact of Cyber-Security on Financial Fraud in Commercial Banks in Nigeria: A Case Study of Zenith Banks in Abuja," *Doctoral dissertation, AUST,* 2023.

[15] A. Mahalle, J. Yong, X. Tao, and J. Shen, "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*, 2018.

[16] F. Ghane, S. Gilaninia and M. Homayounfar, "The effect of cloud computing on the effectiveness of customer relation management in the electronic banking industry: a case study of Eghtesad novel bank.," in *Arabian Journal of Business and M*, 2016.

[17] F. A. Kamoun, "Rethinking the role of enterprise architecture during times of economic downturn: a dynamic capabilities approach," *Journal of Information Technology Management*, vol. 24, no. 1, 2013.

[18] N. I. Eltayb and O. A. Rayis, "Cloud Computing Security Framework Privacy Security., 6(2), " *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 6, no. 2, pp. 78-83, 2018.

[19] M. A. Kâafar, L. Benazzouz, F. Kamoun, and D. Males, "A Kerberos-based authentication architecture for Wireless Lans.," in *In Networking 2004: Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Third International IFIP-TC6 Networking Conference Athens, Greece, May 9–14, 2004, Proceedings 3*, 2004.

[20] S. Khamitkar, Y. F. Al-Dubai, P. Bhalchandra, and P. Wasnik, "Kerberos authentication with cloud computing access control.," *International Journal of Advanced Computational Engineering and Networking*, pp. 2320-2106., 2015.

[21] Y. F. Al-Dubai and S. D. Khamitkar, "Kerberos: secure single sign-on authentication protocol framework for cloud access control," *Global Journal of Computer Science and Technology: B Cloud and Distributed*, 2014.

[22] E. B. Fernandez and R. Monge, "A security reference architecture for cloud systems.," in *In Proceedings of the WICSA 2014 Companion*, 2014.

[23] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski, "The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses.," *EEE Communications Surveys & Tutorials*, 2020.

[24] J. Moreno, M. A. Serrano, E. Fernandez-Medina and E. B. Fernandez, "Towards a Security Reference Architecture for Big Data." in *In DOLAP.*, 2018.

[25] E. B. Fernandez, R. Monge, and K. Hashizume, "Building a security reference architecture for cloud systems.," *Requirements Engineering*, vol. 21, pp. 225-249, 2016.

[26] M. Azhagiri, A. Rajesh and S. Karthik, "Intrusion detection and prevention system: technologies and challenges," *International Journal of Applied Engineering Research*, vol. 10, no. 87, pp. 1-12, 2015.

[27] B. S. Kumar, T. C. Raju, M. Ratnakar, and N. Sudhakar, "Intrusion detection system-types and prevention," *International Journal of Computer Science and Information Technologies*, vol. 4, no. 1, pp. 77-82, 2013.

[28] R. Bose, S. Chakraborty, and S. Roy, "Explaining the workings principle of cloud-based multi-factor authentication architecture on banking sectors.," *In 2019 Amity International Conference on Artificial Intelligence (AICAI)*, 2019.

[29] V. Maheshwari, S. Sahana, S. Das, I. Das and A. Ghosh, "Factors Influencing Security Issues in Cloud Computing.," in *International Conference on Advanced Communication and Intelligent Systems*, 2022.

[30] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions.," *The Journal of supercomputing*, vol. 76, no. 12, pp. 9493-9532, 2020.

[31] K. V. Raipurkar and A. V. Deorankar, "Improve data security in a cloud environment by using LDAP and two-way encryption algorithm.," *In 2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016.

[32] S. Khamitkar, Y. Al-Dubai, P. Bhalchandra, and P. Wasnik, "Kerberos authentication with cloud computing access control.," *International Journal of Advanced Computational Engineering and Networking*, pp. 2320-2106, 2015.

[33] T. Muhammad, M. T. Munir, M. Z. Munir, and M. W. Zafar, "Elevating Business Operations: The Transformative Power of Cloud Computing.," *International Journal of Computer Science and Technology*, vol. 2, no. 1, pp. 1-21, 2018.

[34] A. Moralis, V. Pouli, S. Papavassiliou, and V. Maglaris, "A Kerberos security architecture for web services based instrumentation grids.," *Future Generation Computer Systems*, vol. 25, no. 7, pp. 804-818, 2009.

[35] M. C. Libicki, L. Ablon, and T. Webb, "The defender’s dilemma: Charting a course toward cybersecurity.," *Rand Corporation*, 2015.

[36] E. Fernandez and R. Monge, "A security reference architecture for cloud systems.," *In Proceedings of the WICSA 2014 Companion*, pp. 1-5, 2014.

[37] A. Rath, B. Spasic, N. Boucart and P. Thiran, "Security pattern for cloud saas: From system and data security to privacy case study in AWS and azure," *Computers*, vol. 8, no. 2, 2019.

[38] R. Bose, S. Chakraborty, and S. Roy, "Explaining the workings principle of cloud-based multi-factor authentication architecture on banking sectors.," in *Amity International Conference on Artificial Intelligence (AICAI)*, 2019.

[39] S. Chakraborty, R. Bose, S. Roy, and D. Sarddar, "Auditing deployed software licenses on the cloud using a secure loopback protocol," *Int. J. Recent. Technol. Eng*, vol. 8, no. 3, pp. 1-5, 2019.

[40] A. I. Newaz, A. K. Sikder, M. A. Rahman and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses.," *ACM Transactions on Computing for Healthcare*, vol. 2, no. 3, pp. 1-44, 2021.

[41] M. Aldwairi and S. Aldhanhani, "Multi-factor authentication system," in *In The 2017 International Conference on Research and Innovation in Computer Engineering and Computer Sciences (RICCES’2017). Malaysia Technical Scientist Association.*, 2017.

[42] V. Kakkad, M. Patel and M. Shah, "Biometric authentication and image encryption for image security in cloud framework.," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, pp. 233-248, 2019.

[43] T. Campbell, "Protection of systems.," *Practical Information Security Management: A Complete Guide to Planning and Implementation*, pp. 155-177, 2016.

[44] A. Sarkar and B. K. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems.," *Multimedia Tools and Applications*, vol. 79, pp. 27721-27776., 2020.

[45] M. A. AlZain, B. Soh, and E. Pardede, "TMR-MCDB: Enhancing security in a multi-cloud model through the improvement of service dependability," *International Journal of cloud computing and services science (IJ-CLOSER)*, vol. 3, no. 3, pp. 133-144, 2014.

[46] M. Ahmed, A. Litchfield and C. Sharma, "A distributed security model for cloud computing.," in *Proceedings of the Americas Conference on Information Systems.*, 2016.

[47] M. A. Alzain and E. Pardede, "Using multi shares for ensuring privacy in database-as-a-service.," in *In 2011 44th Hawaii international conference on System Sciences*, 2011.

[48] S. Gupta, R. C. Poonia, V. Singh and L. Raja, "Tier application in multi-cloud databases to improve security and service availability.," in *In Handbook of Research on cloud computing and Big Data Applications in IoT*, 2019.

[49] M. S. Kiraz, "A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing," *Journal of Ambient Intelligence and Humanized Computing*, pp. 731-760, 2016.

[50] A. Sunyaev and A. Sunyaev, "Cloud computing.," *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, pp. 195-236, 2020.

[51] C. Gurkok, "Securing cloud computing systems.," *In Computer and Information Security Handbook*, Morgan Kaufmann., 2017, pp. 897-922.

[52] M. A. Al Moteri, "Decision Support for Shared Responsibility of Cloud Security Metrics.," 2017.

[53] R. Yeluri and E. Castro-Leon, "Building the Infrastructure for Cloud Security: A Solutions View," *Springer Nature.*, 2014.

[54] D. Blum, "Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment," *Springer Nature.*, 2020.

[55] R. P. Padhy, M. R. Patra and S. C. Satapathy, "Cloud computing: security issues and research challenges.," *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, pp. 136-146, 2011.

[56] J. Becker and E. Bailey, "A comparison of IT governance & control frameworks in cloud computing.," 2014.

[57] C. Tang and J. Liu, "Selecting a trusted cloud service provider for your SaaS program.," *Computers & Security*, pp. 60-73, 2015.

[58] K. Purohit and M. A. Rana, "AUTHENTICATION IN CLOUD COMPUTING.," 2016.

[59] M. Alsanea, J. Barth and R. Griffith, "Factors affecting the adoption of cloud computing in the government sector: a case study of Saudi Arabia.," *International Journal of Cloud Computing and Service Science*, vol. 36, pp. 1-16, 2014.

[60] U. C. Iwuchukwu, E. E. Atimati, C. I. Ndukwe, and O. C. Iwuamadi, "The state of cloud computing in Nigeria.," *IOSR Journal of Electrical and Electronics Engineering*, pp. 84-93, 2017.

[61] D. Puthal, B. P. Sahoo, S. Mishra and S. Swain, "Cloud computing features, issues, and challenges: a big picture." in *In 2015 International Conference on computational intelligence and Networks*, 2015.

[62] P. K. Senyo, E. Addae, and R. Boateng, "Cloud computing research: A review of research themes, frameworks, methods, and future research directions.," *International Journal of Information Management*, vol. 38, no. 1, pp. 128-139, 2018.

[63] A. A. Almazroi, *An empirical study of factors that influence the adoption of cloud computing applications by students in Saudi Arabian Universities*, Doctoral dissertation, Flinders University, School of Computer Science, Engineering and Mathematics, 2017.

[64] Z. Shana and E. S. Abulibdeh, *Cloud computing issues for higher education: Theory of acceptance model.*, 2017.

[65] B. Nedelcu, M. E. Stefanet, I. F. Tamasescu, S. E. Tintoiu, and A. Vezeanu, "Cloud Computing and its Challenges and Benefits in the Bank System.," *Database Systems Journal*, vol. 6, no. 1, 2015.

[66] C. Agre, "Implementation of a cloud in the banking sector.," *International Journal of Computer Science and Information Technology*, vol. 3, no. 2, pp. 1168-1174., 2015.

[67] A. Elzamly, B. Hussin, S. Abu Naser, and K. Khanfar, "A new conceptual framework modeling for cloud computing risk management in banking organizations.," *International Journal of Grid and Distributed Computing*, 2016.

[68] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Data security model for cloud computing," *Journal of Communication and Computer*, vol. 10, no. 8, pp. 1047-1062., 2013.

[69] J. R. Mlgheit, E. H. Houssein, and H. H. Zayed, "Security Model for Preserving Privacy over Encrypted Cloud Computing.," *Journal of Computer and Communications*, vol. 5, no. 6, 2017.

[70] U. M. Ismail, S. Islam, M. Ouedraogo, and E. Weippl, "A framework for security transparency in cloud computing.," *Future Internet*, 2016.

[71] M. A. Albahr, "Cloud Computing Security.," 2015.

[72] P. Shamsolmoali and M. Zareapoor, "DATA SECURITY MODEL IN CLOUD COMPUTING.," 2016.

[73] M. Jouini and L. B. Rabai, "A security framework for secure cloud computing environments.," in *Cloud Security: Concepts, methodologies, tools, and applications*, 2019, pp. 249-263.

[74] P. A. Vitti, D. R. dos Santos, C. Westphall and K. M. Vieira, "Current issues in cloud computing security and management.," *SECURWARE*, 2014.

[75] M. Alassafi, A. Alharthi, A. Alenezi, R. Walters and G. Wills, "Investigating the security factors in cloud computing adoption: Towards developing an integrated framework," *Journal of Internet Technology and Secured Transactions (JITST)*, vol. 5, no. 2.