

# Cloud Security Challenges and Framework Development for Kenyan Fintechs

Omondi Alex Omieno<sup>1\*</sup>, Dr. James Mwikya Reuben<sup>2</sup>, Togdé Ngarenon<sup>3</sup>

<sup>1,3</sup>African Institute for Mathematical Sciences (AIMS), Senegal

<sup>2</sup>School of Pure and Applied Sciences, Kirinyaga University, Kenya

DOI: <https://doi.org/10.51584/IJRIAS.2025.10020037>

Received: 10 February 2025; Accepted: 14 February 2025; Published: 13 March 2025

## ABSTRACT

The rapid adoption of cloud computing by FINTECHs in Kenya has brought significant operational advantages, but it has also exposed these organizations to serious security challenges. This study addresses the critical security issues faced by Kenyan FINTECHs, focusing on internal threats and data destruction. The research objectives were to investigate the cloud security challenges Kenyan FINTECHs faced and develop a security assessment framework to address these challenges. Using a mixed-method approach, the study collected data through questionnaires and experimental analysis of the OwnCloud platform. The findings revealed that internal threats, such as rogue administrators, and data destruction issues, such as incomplete deletion, are major concerns. A security assessment framework was developed and validated against international standards like NIST CSF 2.0, COBIT, ITIL, and ISO. The framework provides a structured approach to identifying and mitigating cloud security risks, offering a practical tool for FINTECHs to enhance their cloud security infrastructure. The study recommends increased awareness and training for employees, improved collaboration with cloud providers, and the implementation of robust security policies to address these challenges.

**Keywords:** Cloud Security, Security Framework, FINTECHs, Standards

## INTRODUCTION AND BACKGROUND TO THE STUDY

Integrating cloud computing in financial services has catalyzed innovation and efficiency in the fintech sector globally. In Kenya, a pioneer in mobile money and digital financial solutions, adopting cloud technologies is critical for sustaining growth and competitiveness. However, the benefits of cloud computing come with many security risks that must be carefully managed to protect sensitive financial data and maintain consumer trust (S. Garg, 2020).

Kenya's fintech ecosystem is among the most vibrant in Africa, driven by widespread mobile penetration and a robust regulatory framework. The Central Bank of Kenya reports that over 80% of the adult population has access to financial services, with a significant portion of these services delivered through mobile devices and increasingly through cloud-based platforms. This widespread adoption underscores the importance of robust cybersecurity measures (CBK, 2024).

Despite these advancements, Kenyan fintech companies face unique challenges in cloud computing security. The regulatory landscape in Kenya, although progressive, still struggles to ensure that digital financial services are both inclusive and secure. The Data Protection Act of 2019 marked a significant step towards aligning Kenya's data protection policies with global standards, yet its implementation continues to evolve, especially concerning cloud services (Kenya Data Protection Act 2020).

### Problem Statement

As fintech companies in Kenya increasingly turn to cloud computing to drive innovation and enhance service delivery, they encounter a complex array of security challenges that threaten the integrity and reliability of financial services. The rapid adoption of cloud technologies has exposed these companies to more risks, including data breaches, unauthorized access, and systemic vulnerabilities that could potentially lead to significant financial and reputational damage. Despite the critical nature of these risks, there is a notable absence

of a standardized security assessment framework tailored to the specific conditions and regulatory environment of the Kenyan fintech sector (J. Smith, 2023).

Current global security frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 provide broad guidelines applicable across industries and regions. However, these standards often fall short of addressing the unique challenges faced by fintech companies in emerging markets, particularly those operating under rapidly evolving regulatory landscapes like Kenya (T. Jensen, 2022). These international standards may not fully include local regulatory requirements, such as those outlined in Kenya's Data Protection Act of 2019, nor are they always aligned with the operational realities of Kenyan fintech companies, such as mobile money platforms that dominate the financial landscape (Republic of Kenya, 2020).

The implementation of security standards faces problems because organizations lack money and a basic understanding of security while also using old network equipment. Current security approaches and business methods in the area vary. Targeted cyberattacks have grown rapidly into major threats across the region, thus specialized security measures are required to defend East Africa against its rising cyber threats (Cybersecurity Africa Report, 2024).

Because there is no regional framework, companies create random security systems that might not protect against today's advanced threats as these methods are inadequate to protect against present-day cyber attacks. There is a critical need for a robust, scalable, and regulatory-compliant security framework that not only aligns with global best practices but also integrates local market dynamics and regulatory specifics. Therefore, it is essential to have a comprehensive, end-to-end standardized security framework based on industry standards, but tailored to the specific requirements of the fintech sector in Kenya.

## Objectives

The primary foundation of this research consists of developing an industry-tailored standardized Cloud Computing Security Assessment Framework for Kenyan fintech companies. The research established a specialized security assessment Framework for the Kenyan fintech industry. This framework aims to help FinTech companies assess their cloud security systems to detect security threats and strengthen their security framework within Kenyan regulations. The security standards of organizations improve through this framework operating within Kenya's business environment.

## Specific Objectives

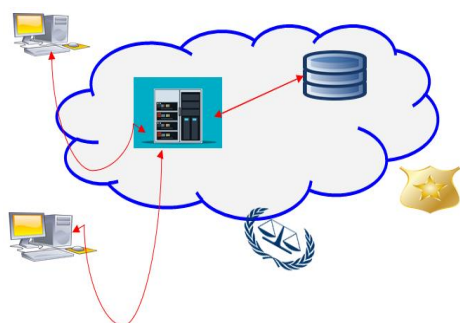
- The study aims to investigate the cloud security challenges that Kenyan fintech companies currently face.
- The development of a security assessment framework for assessments of cloud security problems that exist in Kenyan fintech companies.

## LITERATURE REVIEW

### Cloud Computing Security Analysis

The Trusted Computing Group (TCG 2020) found six main defense zones that must have strong security controls, which they recommend implementing to win against threats. These areas are:

Figure 1: Areas of concern in cloud security



Source: Trusted Computing Group's (2020)

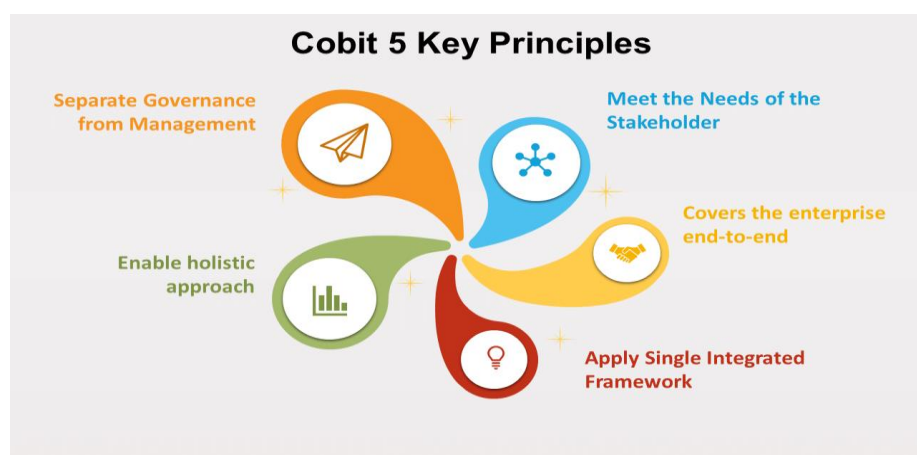
- Data security at rest: Applying encryption technology to data that sleep on cloud servers to keep unauthorized individuals away.
- Transit security: Protecting data as it moves from one point to another using secure encryption.
- Authentication: Using passwords, multi-factor authentication, and biometric security measures to protect against unauthorized data access.
- Data isolation: Employing virtual machine technology to safely manage different customer data.
- Compliance: Ensuring that customers follow laws and rules when using cloud services.
- Incident response: Having an effective incident response plan to fix security problems and system breakdowns.

## Cloud Security Frameworks

Cloud technology provides many advantages, especially through scalable performance at reduced costs while remaining flexible and efficient. The more organizations use cloud services to run their operations, the more important it becomes to protect their data. To stay secure, you must put strong security systems in place. Cloud security frameworks drive organizational security requirements in all cloud environments. These frameworks assist companies in creating security rules that work best for their unique cloud setups. By following these security frameworks, organizations can learn how to analyze their data protection risks plus choose and put in place their security features. The security framework includes regular safe checks plus a security monitoring team with a plan for incidents and schedule updates for protection.

COBIT 5 for Cloud Computing:

Figure 2. COBIT5 Principles.



Source: Wallarm (2024)

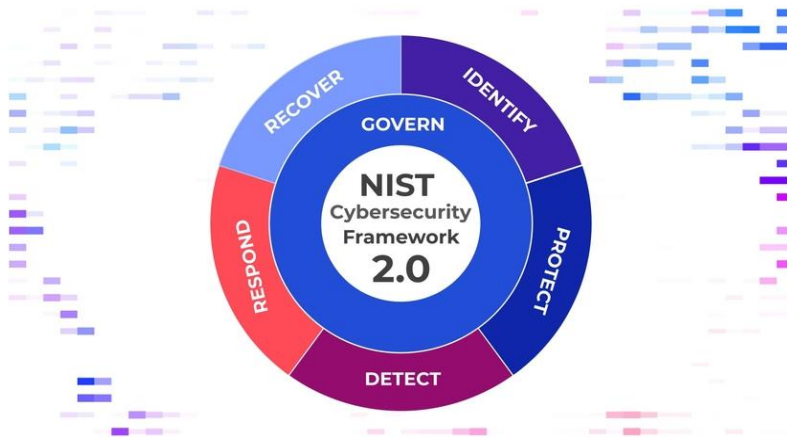
The COBIT 5 for Cloud Computing framework delivers governance and management guidelines. IT's activities benefit from the strategic alignment that enables them to follow business objectives. It emphasizes the importance of risk management alongside performance measurement techniques and process improvement practices for cloud systems. This framework delivers direction to establish roles with corresponding responsibilities together with essential control systems, organizations need assessments to adopt cloud safely and achieve their desired business outcomes (Wallarm 2024).

## NIST CSF 2.0:

The specialized publication NIST CSF 2.0 delivers focused guidance about cloud security by examining cloud-based security threats along with vulnerabilities and risk factors. It provides comprehensive knowledge about threats, vulnerabilities, and risks that are exclusive to cloud environments. It offers both a thorough examination of security issues involved with cloud services and practical guidelines for their mitigation. The publication

provides uniform guidelines together with practical recommendations for risk minimization strategies. This framework is widely used by the cybersecurity community as an official reference (ResearchGate 2024).

Figure 3. NIST Core Functions.

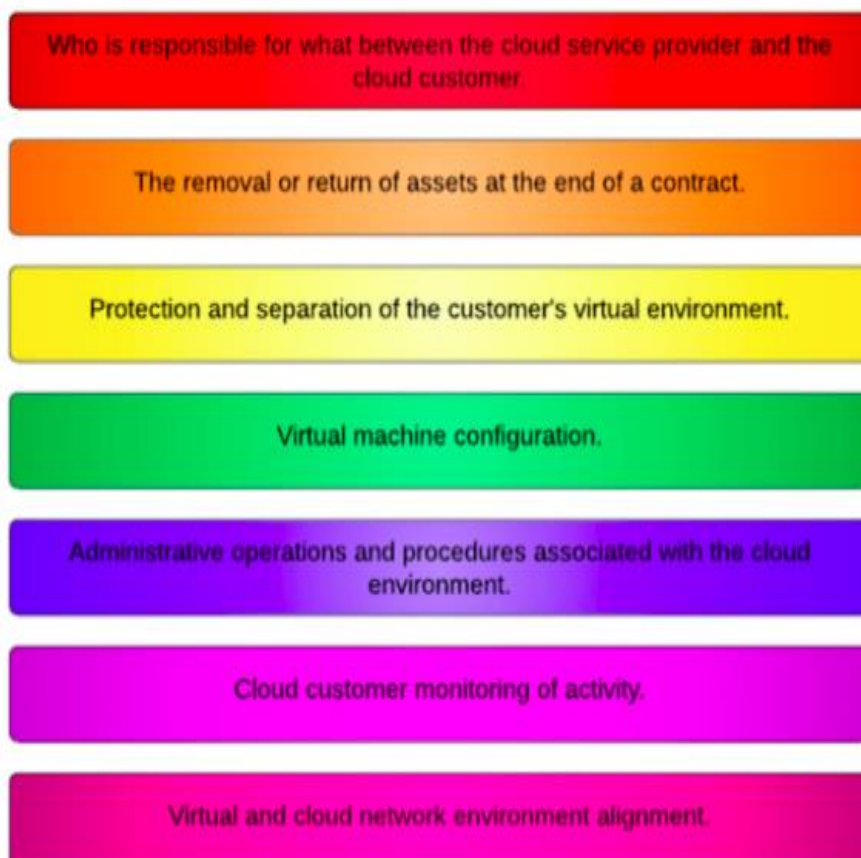


Source: ResearchGate (2024)

## ISO 27017

ISO 27017 is an international standard that specifically addresses cloud security controls. It provides guidance on implementing effective security measures for cloud services, covering areas such as data classification, encryption, access management, and incident response. This standard ensures that cloud service providers and users have a common set of security controls to build upon (ResearchGate 2024).

Figure 4. Standards of ISO/IEC 27017.



Source: ResearchGate (2024)



## AWS Well-Architected Framework:

Figure 5.Six Pillars of AWS



Source: Tutorials Dojo (2024)

Delivers an organized procedure for creating secure and efficient infrastructure throughout Amazon Web Services (AWS). It encompasses five pillars: operational excellence, security, reliability, performance efficiency, and cost optimization. The structured system provides organizations with tools to ensure proper cloud setups (Tutorials Dojo 2024).

## Related Studies

A theoretical review by James Reuben and Johnmark Obura Ouma (2021) analyzed computing security in Sub-Saharan Africa with specific attention to insider attacks data leakage and denial of service vulnerabilities. The authors suggested encryption together with intrusion detection systems as security measures. The authors identified the need for better legal structures to regulate cloud adoption in developing nations although they recognized their value in supplementing intrusion detection systems. According to the author, additional research on AI-driven security solutions for future development remains a necessary task. This study builds upon their previous effort by creating an operational security framework for Kenya's financial technology domain.

Atuah and David Sanka Laar (2023) researched cloud security compliance challenges confronting SMEs in Ghana's Bolgatanga Municipality. The research team implemented Design Science Research Methodology (DSRM) to build a straightforward cloud adoption framework that lowers costs while advancing agility and market expansion. The authors recognized that the framework had constrained applicability to quick shifts in technological environments. This research builds upon their work by examining fintech operations in Kenya while focusing on specific compliance requirements of local conditions.

Mayur Rahul (2023) developed a trust-focused approach for cloud security assessment through cloud provider trust score evaluation. This innovative model offers limited support toward dealing with the unique issues that fintech companies face such as regulatory requirements. This research introduces trust metrics along with compliance elements into a specially designed framework for security evaluation within Kenya's fintech sector.

The authors Togesh Awashi, Tendai Musunda, and Timothy Makambwa (2024) introduced their research cloud migration framework that focused on data security and compliance frameworks appropriately designed for educational institutions alongside optimization plans. The framework by Togesh et al provides strong academic guidelines yet fails to address digital finance platforms' distinctive regulatory requirements and security needs. This research applied their methodology with modifications to address unique aspects found in the Kenyan fintech industry.

## Conceptual Framework

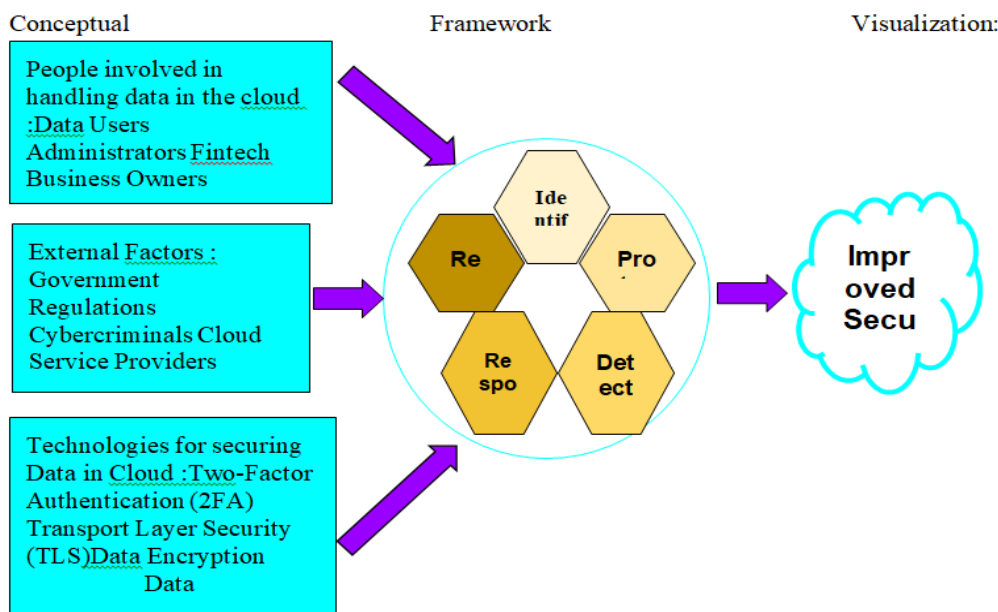
Conceptual Framework Building Blocks:

Table 1: Building Blocks

Independent Variables	Intervening Variables	Overall Dependent Variable
People  Technology  External Factors	Identify Risks  Protect Data  Detect Incidents  Respond to Threats  Recover from Breaches	Security in Cloud Computing for Fintech

Source: Authors (2025)

Figure 6: Building the Framework



Source: Authors (2025)

## RESEARCH METHODOLOGY

### Design and Methodology

Research design constitutes a systematic framework that defines procedures for collecting data while performing analytic procedures to address research questions efficiently. The study results acquire accuracy and dependability through this essential component (Zhang 2022).

The research design employed a mixed-method approach which integrated descriptive research with experimental designs. The information gathered from participants for this descriptive research enabled better comprehension of cloud security challenges that affect Kenyan FinTech organizations. Research data collection was achieved through questionnaires that reached employees from the involved fintech organizations.

Researchers employed a descriptive survey type because it let them collect mass-scale assessments about cloud security matters from survey participants. The study's output enabled researchers to extend their conclusions about cloud security practices to the fintech sector operating within Kenya. The mixed-method approach enhanced problem analysis by merging both quantitative numerical data and qualitative human perspective data (Petrenko 2021).

### **Population of the study**

Scientists study entire collections of subjects known as populations from which they choose sample groups to obtain measurements and data. For this study, the target population consisted of all 51 Fintech companies in Kenya registered with the Central Bank of Kenya as

of 2024. These companies were included in the research because they handle sensitive and critical data that necessitates secure and private storage, and they heavily rely on IT resources for infrastructure growth. Every organization stands within one of two categories: leveraging existing cloud infrastructure or preparing to incorporate it for their infrastructure needs.

The participants in the study were selected from five different departments within the Fintech companies, with one individual from each department providing insights through questionnaires. Each selected participant shared their perspectives on cloud computing security practices based on their role.

### **Technique and Sample Size**

This research employed a census approach. All 51 Fintech companies registered by the Central Bank of Kenya (CBK) was included in this study. One representative from each company was chosen from five key departments, resulting in a total sample size of 255 participants (51 companies  $\times$  5 departments). This approach ensured comprehensive coverage of the sector, allowing for in-depth data collection from all Fintech firms that utilize cloud computing for data storage and operations. This ensured valuable insights into cloud computing security practices and the specific challenges faced by the industry.

### **Instrumentation**

Given the challenge of accessing backend cloud security threats directly, the study simulated a private cloud environment using OwnCloud, a widely accepted SaaS platform for cloud computing.

### **Data Analysis**

Analysis took place across two distinct phases of the research study. This study presents simulation results from OwnCloud-based cloud security tests that led to experimental outcomes. A descriptive statistics approach analyzed all gathered participant data obtained through questionnaire surveys during phase two of the analysis. The researchers demonstrated the results through textual and numeric representations, including graphs and tables alongside charts along with frequencies and percentages. GQM techniques led to the development of the framework that generated crucial information about the FINTECH sector cloud security status.

### **Framework Building Through Metrics**

Measurement tools labeled security metrics enable Kenyan Fintechs to track and evaluate the security and privacy level their cloud operations achieve. Metric systems serve to improve data clarity and better strategic decisions and predictive analytics and help organizations formulate proactive security strategies. Each metric consists of measurable qualities along with designated assessment measurement systems.

The established procedural rules that govern metric collection enable results interpretation with accuracy. During measurement operations sub-elements referred to as primitive metrics or sub-metrics receive specified constraints. Metrics can be expressed in one of the following

Ways:

- Number - #: The study team received authorization for a single representative from Executive Management, Finance, Information Technology, Data Management, and Operations to complete survey questionnaires. Managers understood their critical role in the research as their input would help deepen our understanding of business challenges.
- Percentage - %: The research maintained complete privacy of responses while neither the staff nor the administration required participation. Participants received notification they could end their participation whenever they felt unsure about the research.
- Logic value: Response data took the form of either "Yes" or "No" to indicate whether specific events occurred.

Security management in cloud computing follows this proposal-based cycle;

- Cloud security metrics hierarchy.
- Index of Security (IndSec).
- Security Management by Finthechs.

The security metrics hierarchy is derived from the GQM methodology, and the Index of Security(IndSec) is computed using this hierarchy. Fintechs then use the security index as a reference to improve their cloud security measures. The security management lifecycle serves as a new method for visualizing security-related information gathered from the cloud environments utilized by the Fintech sector.

Security metrics hierarchy relies on GQM methodology and utilizes this framework to determine the Index of Security (IndSec). Fintech companies use the security index assessment to improve their cloud security measures.

The original GQM approach developed by Caldiera and Rombach during the 1970s enabled this study to utilize a quantitative assessment for cloud security testing. The GQM methodology structured the measurement model across three levels:

- Conceptual level (goal): Each object at this level receives its goal definition according to multiple cloud security models through which Fintech sector professionals view their work.
- Operational level (question): The operational level consists of questions that create models for evaluating the subject under analysis. This evaluation methodology determines the level of achievement regarding set goals.
- Quantitative level (metric): EA set of established metrics connects to every questionnaire to measure quantifiable answers.

The research utilized GQM techniques to establish direct security metrics hierarchy linkage by pairing security features to relevant metrics addressing system objectives.

## RESULTS AND DISCUSSION

### Experimental Analysis of Cloud Security

The research objective examined data file operations in cloud environments while identifying security threats from cloud providers. The experiment was conducted using OwnCloud version 10.15. A desktop machine had OwnCloud set up for the exploration. The software required users to create new accounts. Different individuals received separate user accounts to use the OwnCloud client software version 5.3.1. Users stored their dummy data through the OwnCloud client software version and used a web browser when accessing the application.

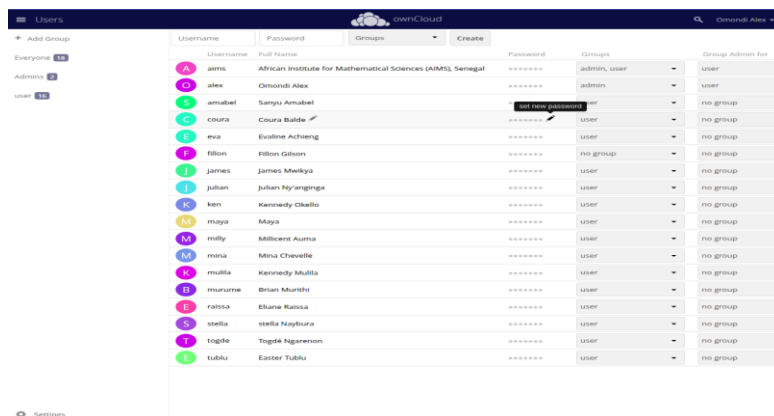


## The Insider Threat Challenge

Cloud security faces serious threats because internal misbehaving employees and system administrators exploit their access privileges to sensitive information. Three types of stakeholders exist who pose an insider threat: cloud provider employees as well as their clients and independent partners who work within cloud operations. Because these individuals manage authorized access to cloud services and customer data along with related infrastructure, they can take advantage of their position to breach security.

OwnCloud allows administrators to reset user passwords without exposing password visibility to themselves. Internal personnel access remains the main security risk this scenario demonstrates. The ability to reset a user password by an administrator allows their entry into affected systems as that user while giving them unrestricted access to data and system security vulnerability potential.

Figure 7: User List and Password Change



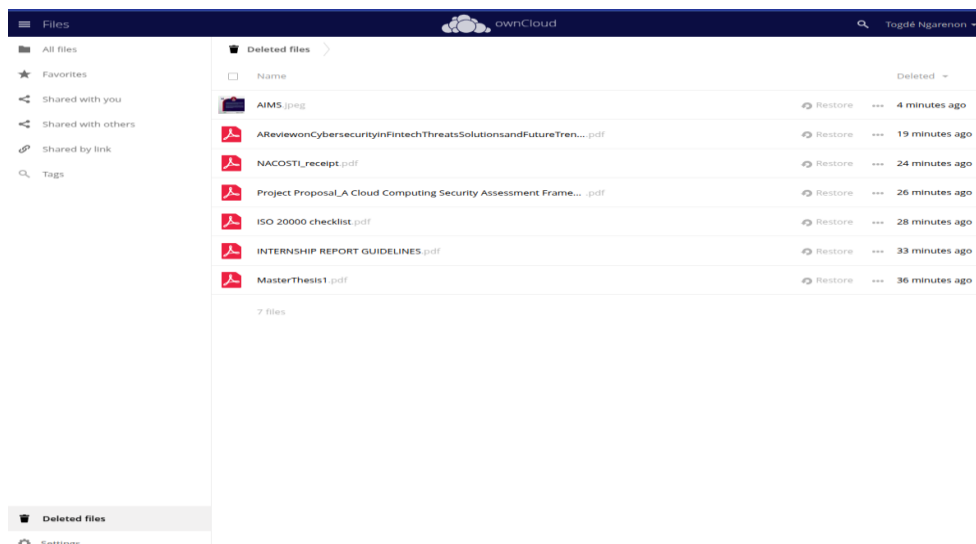
Username	Full Name	Password	Groups	Group Admin for
admins	African Institute for Mathematical Sciences (AIMS), Senegal	*****	admin, user	user
alex	Omondi Alex	*****	admin	user
amabel	Sanyu Amabel	*****	no group	no group
coura	Coura Bulde	*****	user	no group
eva	Evaline Acheng	*****	user	no group
filion	Filion Gilsen	*****	no group	no group
james	James Mwika	*****	user	no group
julian	Julian Nyanganga	*****	user	no group
ken	Kennedy Okello	*****	user	no group
maya	Maya	*****	user	no group
milly	Millicent Auma	*****	user	no group
mina	Mina Chevelle	*****	user	no group
mulia	Kennedy Mulia	*****	user	no group
munume	Brian Murithi	*****	user	no group
ratosa	Eliane Ratosa	*****	user	no group
stella	Stella Noybura	*****	user	no group
togde	Togde Ngarenon	*****	user	no group
tutulu	Easter Tutulu	*****	user	no group

Source: Authors (2025)

## Deleted Data Challenge

Users received immediate loss of files following their cloud upload and deletion process on their local computer, but those files still existed in the cloud storage for another 30 days. Cloud-based files became visible in the cloud storage for thirty days until complete deletion occurred. Security and privacy risks develop because files stay inside the cloud system accessible to unauthorized users during the thirty-day catchment period.

Figure 8: Deleted Documents in the Cloud



Name	Deleted
AIMS.jpeg	4 minutes ago
AReviewonCybersecurityinFintechThreatsSolutionsandFutureTren... .pdf	19 minutes ago
NACOST_receipt.pdf	24 minutes ago
Project Proposal_A Cloud Computing Security Assessment Frame... .pdf	26 minutes ago
ISO 20000 checklist.pdf	28 minutes ago
INTERNSHIP REPORT GUIDELINES.pdf	33 minutes ago
MasterThesis1.pdf	36 minutes ago

Source: Authors (2025)

## Respondent Demographics

The research presented key demographic findings from survey participants about their age range while separating responders into gender categories along with education status and professional background.

## Questionnaire Response Rate

Table 2 presents questionnaire response rates which demonstrate enough respondent participation for this research.

Table 2: Return Rate for Questionnaire

Respondents	Questionnaires administered	Questionnaires returned	Return rate (%)
FinTech Staff	255	189	74.2

source: Survey data (2025)

The research distributed 255 questionnaires which were sent to employees from each of the 51 FinTech organizations validated by the Central Bank of Kenya by 2024. Table 2 shows that out of the distributed questionnaires, 74.2% (189) were filled up and returned for assessment. According to Oluqbenga Asaolu, research findings with a 50% response rate qualify as adequate, while a 60% response rate scores as good, and exceeding 70% response rate stands as very good. Based on established standards, this research's response rate of 74.2% achieves a very good outcome. The study attained an elevated response rate through successful research methods which combined early study announcements with convenient self-reporting questionnaires and dedicated follow-up communications for participant concerns and prompt response submissions.

## Key Cloud Security Challenges Encountered

The key security problems confronting Fintechs in Kenya through SaaS cloud adoption undergo evaluation in this section. The researcher used questionnaires to collect data about multiple safety issues along with security practices and cloud computing obstacles.

## Deployment Models Security Challenges

A study on Kenyan fintech companies reveals significant cloud security challenges, with participants highlighting major concerns such as data accessibility risks due to internet outages, unauthorized access by malicious cloud administrators, and insufficient password security measures, emphasizing the need for multi-factor authentication and advanced protection techniques. Respondents also expressed unease over cloud vendors' uncontrolled data management practices, lack of transparency in data deletion, and inadequate incident response responsibilities, underscoring the necessity for stronger vendor supervision, compliance measures, and improved security defenses. The findings stress that addressing these issues is critical to safeguarding financial trust and maintaining service integrity as the fintech sector grows.

The research findings align with recent cybersecurity reports highlighting threats in Kenya's fintech industry, including over 860 million cyberattacks reported in the past year and vulnerabilities in public and private entities like Kenya Power and Kenya Railways. Kenya's mobile-first development approach, while enabling rapid application construction, often lacks robust cybersecurity safeguards, leaving fintech companies exposed to phishing, ransomware, and data breaches. A key challenge is the disconnect between application development and cybersecurity teams, necessitating integrated strategies like the "3C's" (Convergence, Consolidation, and Context) to combat evolving threats. Globally, cybercrime is escalating, with projected losses reaching \$9.5 trillion by 2024, driven by state-backed and financial hackers targeting mobile and smart devices. To mitigate risks, organizations must adopt zero-trust architectures, multi-factor authentication, and continuous cloud system supervision, alongside employee cybersecurity training. The study underscores the urgent need for

comprehensive and collaborative security measures to ensure the resilience and integrity of Kenya's growing fintech sector.

Table 3: Respondents' Views on Security Issues

Statement	Mean	Std. Deviation
SI_1_Data or information stored in the cloud may experience significant availability issues due to internet downtime	4.70	.756
SI_2_A cloud administrator poses a substantial risk if they become rogue and attempt to access data stored in the cloud	4.67	.778
SI_8_Relying solely on password protection is insufficient to prevent unauthorized access in the cloud	4.64	.713
SI_5_In the SaaS model, hackers can exploit vulnerabilities in the data security framework to gain unauthorized access to data or applications.	4.59	.874
SI_7_Multi-tenancy in the cloud poses a significant concern for clients due to the risk of a hacker exploiting the shared host	4.59	.757
SI_4_Since the data owner lacks control over the cloud vendor's data handling practices, there is no reliable way to ensure that the data is being managed lawfully	4.57	.924
SI_3_When a data owner issues a command to delete a cloud resource, there is no definitive way to confirm that the data has been completely erased	4.46	1.079
SI_6_Cloud computing can lead to a lack of accountability for providers in the event of security incidents	4.45	.991

source: Survey data (2025)

### Security Protocols Implemented by the Cloud Service Provider

The research highlights significant cloud security challenges faced by Kenyan fintech organizations, with respondents emphasizing the importance of complete security monitoring logs (mean score 4.78, SD 0.663) and regular audits to mitigate risks. However, concerns were raised about the adequacy of security measures for data in transit and at rest, reflected in low mean scores (2.61 and 2.60, respectively) and high standard deviations (1.094 and 1.099), indicating a need for improvement. Respondents also expressed skepticism about the strength of authentication platforms (mean 2.55, SD 1.122) and user access control policies (mean 2.54, SD 1.160), underscoring the necessity for stronger enforcement and communication of security measures. Additionally, doubts about data retention, deletion policies (mean 2.50, SD 1.080), and incident management preparedness (mean 2.10, SD 1.225) highlight the need for better cloud provider education and transparency. Addressing these vulnerabilities is crucial for building trust and ensuring the integrity of Kenya's rapidly growing fintech sector.

Table 4: Respondents' Views on Security Measures

Statement	Mean	Std. Deviation
CPA_1 Cloud computing suppliers should maintain thorough security monitoring logs of all access to your data and documents, conducting routine audits, random	4.78	.663

checks, or investigations of suspicious activity based on their established scripts and operation		
CPA_3 In SaaS, applications are multi-tenant and hosted by third parties, which can lead to a variety of complex security issues	4.65	.816
CPA_5 Cloud computing providers offer adequate security for data in transit (data being transferred between the cloud and user devices).	2.61	1.094
CPA_4 Cloud computing providers offer adequate security for data at rest (data stored in the cloud).	2.60	1.099
CPA_6 Cloud computing providers offer a robust authentication platform for users to access the cloud.	2.55	1.122
CPA_2 User access control rules, security policies, and enforcement measures are provided to customers in a clear and informative manner	2.54	1.160
CPA_7 Cloud providers have adequate and credible policies and practices in place, particularly regarding data retention, deletion, and security.	2.50	1.080
CPA_8 Customers are aware of how incidents and disasters may impact their data and, as a result, have appropriate recovery procedures in place	2.10	1.225

source: Survey data (2025)

SASRA's new regulatory requirements for third-party financial system integrators aim to prevent cyber-attacks by mandating IT audits, incident response plans, and clear data retention and deletion guidelines to safeguard sensitive financial data. This aligns with the Communications Authority of Kenya's reports on rising cyber threats, emphasizing the need for fintech organizations to adopt robust security protocols. To address cloud security challenges, Kenyan fintech businesses must implement comprehensive security frameworks, advanced monitoring systems, strong authentication solutions, and clear data management policies to mitigate risks and ensure resilience against evolving cyber threats.

### Issues in Cloud Computing Related to Deployment Models

Survey participants in Kenya's fintech sector expressed strong agreement on critical cloud security concerns, with service and data accessibility being the top priority (mean score 4.87, SD 0.448), as downtime could severely disrupt operations and customer services. High levels of concern were also noted for data confidentiality (mean 4.86), privacy (mean 4.85), and data integrity (mean 4.85), emphasizing the need for robust encryption and protection against unauthorized access to prevent financial and reputational damage. Respondents highlighted reduced control over data management (mean 4.75) and a lack of provider accountability during security incidents (mean 4.69), calling for stricter contractual obligations. Additionally, challenges like vendor lock-in (mean 4.58) and transnational legal inconsistencies (mean 4.56) were identified as significant barriers, underscoring the complexity of compliance and security in cloud computing. These findings stress the necessity for enhanced security measures and provider accountability to address the sector's vulnerabilities.

Table 5: Concerns on Cloud Computing

Statement	Mean	Std. Deviation
PC_2 Availability of services and/or data	4.87	.448
PC_4 Confidentiality of corporate data	4.86	.522
PC_1 Privacy	4.85	.525

PC_3 Integrity of services and/or data	4.85	.577
PC_5 Loss of control over services and/or data	4.75	.666
PC_6 Lack of accountability of providers in the event of security incidents	4.69	.813
PC_8 Intra-cloud (vendor lock-in) migration	4.58	.813
PC_7 Inconsistency among transnational laws and regulations	4.56	.865

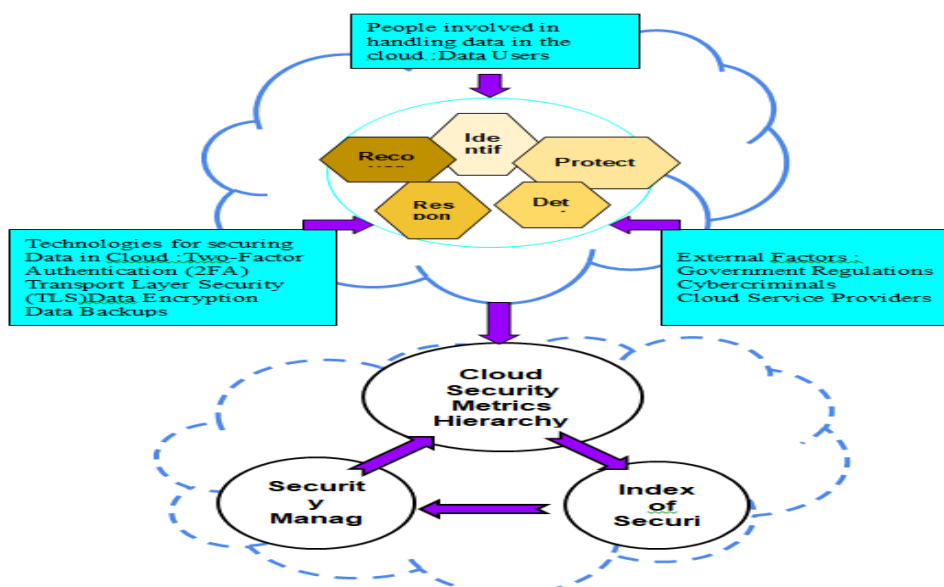
source: Survey data (2025)

These findings align with Kumar’s emphasis on availability, confidentiality, and data integrity as foundational pillars of cloud security, highlighting concerns such as unauthorized access and service availability during internet outages, which mirror challenges in the fintech sector. Kumar recommends robust security protocols and strict SLAs to mitigate these risks. Similarly, Ghimire and Thapa stress that unclear accountability and low provider transparency erode trust in financial technology, advocating for mandatory compliance frameworks and continuous monitoring to address security gaps. Bhorat adds that global cloud service frameworks often conflict with local data regulations, creating compliance issues for fintech companies, and calls for standardized international regulations to ensure clarity and security across borders. The consensus across studies underscores the need for enhanced defensive systems, precise legal oversight, and adherence to the CIA (Confidentiality, Integrity, Availability) triad in cloud security frameworks to overcome technical and security obstacles, enabling fintechs to fully leverage cloud computing benefits.

## Framework Developed

The combination of previous research findings alongside essential reviews together with empirical data establishes security as a fundamental issue that Fintechs encounter while using cloud technologies. The proposed chapter solves this problem through a structured framework that allows organizations to deploy cloud technology while prioritizing complete system security capabilities. Organizations must transfer their cloud data and applications in ways that establish stronger security than the systems maintained at their facilities. The framework, shown in Figure 9 is a research-driven framework established by the author and is organized into eight sequences creating two major categories. Written from the researcher’s work it provides a structure that divides sections logically.

Figure 9: Framework for Enhancing Cloud Computing Security



Source: Authors (2025)



The first section includes five stages that include Identify, Protect, Detect, Respond, and Recover. The Framework includes a Metric Hierarchy followed by an Index of Security and ends with the Implementation of a Secure Cloud. The developed framework gathers insights from analysis outcomes as well as established frameworks in combination with research findings. The data analysis revealed that Fintechs need a security framework that addresses three key factors contributing to security vulnerabilities: human errors, inadequate technologies, and external threats. This framework draws its basis from important references between CSA security guidance and threat analysis together with ENISA security assessment reports and the NIST cloud computing definitions.

## Framework Components

The framework's levels are discussed in this section, which Fintechs can utilize to align their operations with core security requirements for achieving robust cloud security. Table 6 shows the components organized into specific areas of security that need to be focused on.

Table 6: Framework Component Subdivision

Identify	Protect	Detect	Respond	Recover
Asset management	Access Control	Anomalies and Events	Response planning	Recovery Planning
Business environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Mitigation	Communications
Risk Assessment	Information Protection Processes and Procedures		Improvements	
Risk Assessment Strategy	Maintenance		Analysis	
Supply Chain Risk Management	Protective Technology			

source: Survey data (2025)

The initial thing to establish proper governance and security begins with proper identification and management of IT assets. Even though these challenges must continue to persist in managing IT assets. Assets inventory is the most important thing for creating reliable security over computing systems. The identification and operational management of physical and logical IT assets remains a difficult endeavor for companies ranging across all sizes. Multiple elements prevent inventory solutions from reaching their full potential. The inventory program faces multiple obstacles such as restricted network visibility substandard endpoint agent implementation and incompatible system integration among diverse technologies. Untracked assets introduce substantial security risks because they remain updated and supported inadequately and therefore become easy targets for malware attacks. Asset management dynamics undergo fundamental transformations whenever organizations move towards cloud infrastructure. Cloud providers maintain total control over managing infrastructure hardware assets as the principal operator within these cloud systems. This shift can ease the burden of physical asset management for customers, particularly for workloads hosted in the cloud. However, Fintechs still need to maintain inventories of physical assets within their environments, such as data centers, office equipment, IoT devices, and mobile workforce tools. Cloud providers need to maintain and share inventory information relevant to Fintech's specific cloud infrastructure. This collaboration ensures that both parties effectively manage and secure their respective assets.

## CONCLUSION AND RECOMMENDATIONS

### Conclusion

The implementation of cloud computing provides Fintech organizations with substantial advantages to both develop innovative approaches and achieve market expansion. However, past implementations show that the many advantages Fintechs gain require managing serious security challenges. Fintech organizations require methods to address numerous operational challenges. Data security requirements need critical evaluation by Fintechs before they adopt industry standards to build up robust security policies to safeguard their operations. The research provides Fintechs with a definitive methodology to implement secure cloud services that emphasize stages necessary for optimization and security enhancement. The research adjusts the method into distinct steps that optimize and protect cloud facilities. By implementing the structured framework developed in this research, Fintechs can create trusted cloud platform operations. Their data security will improve, and their compliance level with Service Level Agreements (SLAs) and Quality of Service (QoS) benchmarks will increase.

### Recommendations

Based on the findings, the following recommendations are proposed:

- **Awareness and Training:** The development of an organization-wide security awareness must become a pivotal decision for Fintech organizations. Employees, stakeholders, and users need to grasp the security dangers that accompany cloud computing. Also, employees and stakeholders of Fintech companies need comprehensive education about cloud technologies and must understand their role in minimizing those challenges.
- **Collaboration with Providers:** Cloud service providers need to increase their transparency measures through improved collaboration with their Fintech clients. Fintech clients receive support from providers when creating data retention formats and deletion methodologies while developing recovery protocols. Client access to limited auditing abilities would enable security concerns to be resolved while preserving operational integrity.

## REFERENCES

1. Business Daily Africa. (2023). Kenya's fintechs confront cyber threats as incidents rise. Business Daily Africa.
2. Intelligent CIO Africa. (2023). Kenya's mobile-first strategies make fintechs vulnerable to cyber attacks. Intelligent CIO Africa.
3. Cloud Security Alliance. (2024). Compliance and governance in fintech cloud security: Navigating regulatory standards.
4. Cheng, L., Zhang, X., & Li, W. (2022). A survey on cloud computing security issues and challenges. *Future Generation Computer Systems*, 117, 185–207.
5. CrowdStrike. (2024). Cloud security issues: Risks, threats, and challenges.
6. Tutorials Dojo. (2024). AWS.
7. Finextra. (2023). Future of FinTech in Africa: Cloud will open new doors for the African FinTech industry.
8. European Union Agency for Network and Information Security (ENISA). (2024). Cloud computing security risks and benefits: Comprehensive analysis of cloud risks and operational benefits.
9. Forrester's. (2024). Cloud computing deployment models.
10. IT Governance. (2023). ISO-27017 and ISO-27018. Retrieved from <https://www.itgovernance.co.uk/iso-27017-and-iso-27018>
11. Trusted Computing Group. (2020). Cloud security: A comprehensive analysis.
12. ISO/IEC. (2015). ISO/IEC 27017: Security techniques for cloud services. International Organization for Standardization.
13. ISO/IEC. (2015). ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls for cloud services.

14. Obura, J. O., & James, R. (2021). Security threats, mitigation, and framework for cloud computing applications: A theoretical review. Conference Paper, 24.
15. Central Bank of Kenya. (2024). Annual report on the state of financial services in Kenya. Central Bank of Kenya.
16. Communications Authority of Kenya. (2024). Kenya's fintechs face growing cyber threats as incidents rise. Business Daily Africa.
17. Government of Kenya. (2019). Data Protection Act, 2019. Official Kenyan Government Publications.
18. Republic of Kenya. (2019). The Data Protection Act, 2019. Government Printer, Nairobi.
19. National Institute of Standards and Technology (NIST). (2012). NIST SP 800-144: Cloud security guidelines. U.S. Department of Commerce.
20. Petrenko, S., Smith, J., & Sun, Y. (2021). Adapting international cybersecurity standards for developing countries: A case study approach. *International Journal of Information Security*, 20(2), 207–219.
21. Rahul, M. (2023). A trust-based framework for the assessment of security in cloud computing environments. Paper, 134.
22. Cybersecurity Africa Report. (2024). Trends and predictions in East African cyber threats. Cybersecurity Africa.
23. ResearchGate. (2024). NIST CSF 2.0.
24. Amazon Web Services. (2023). AWS Well-Architected Framework: Best practices for building secure, scalable cloud infrastructures.
25. Smith, J., & Adeyemi, B. (2023). Adapting cybersecurity frameworks to fit the African fintech landscape. *African Journal of Information Systems*, 15(3), 204–223.
26. United Nations. (2015). Sustainable development goals.
27. Cybersecurity Ventures. (2024). Cybercrime incidents in East Africa: Report on rising cyber threats in East Africa.
28. Wallarm. (2024). COBIT 5 for cloud security.