Development and Evaluation of a Cloud Security Framework for Kenyan FinTechs

Omondi Alex Omieno[a*], Dr. James Mwikya Reuben[b], Togdé Ngarenon[c]

[a,b,c] alex.o.omondi@aims-senegal.org, jmwikya@kyu.ac.ke, garenon.togde@aims-senegal.org

[a&c] African Institute for Mathematical Sciences (AIMS), Senegal [b] School of Pure and Applied Sciences, Kirinyaga University, Kenya

Abstract

This study focuses on developing a hands-on security measurement framework index and validating a security measurement framework tailored for Kenyan FinTechs operating in cloud environments. The research objectives were to create a hands-on security measurement framework index combining essential security parameters for cloud security operations and to validate the framework's usefulness for FinTechs in Kenya. Using the Goal-Question-Metric (GQM) methodology, the study developed a framework that integrates security metrics and sub-metrics to assess cloud security performance. The framework was validated against international standards such as COBIT, ITIL, and ISO, and its effectiveness was tested through experimental analysis and questionnaire-based data collection. The target population consisted of all 51 FinTech companies in Kenya registered with the Central Bank of Kenya as of 2024. The results demonstrated that the framework successfully addressed key cloud security challenges, including internal threats, data destruction, and regulatory compliance. The study concludes that the framework provides a practical tool for FinTechs to measure and improve their cloud security performance, ensuring alignment with global standards and local regulatory requirements. Recommendations include the implementation of the framework, continuous monitoring, and collaboration with cloud service providers to enhance security.

Keywords: Cloud Security, Security Measurement Framework, Development, Evaluation, FinTechs

1. Introduction and Background to the Study

Cloud computing has become a cornerstone of innovation and efficiency in the FinTech sector, enabling organizations to scale operations, reduce costs, and enhance service delivery. In Kenya, fintechs' adoption of cloud technologies has been driven by the need to remain competitive in a rapidly evolving financial landscape. However, the benefits of cloud computing come with significant security risks, particularly in developing countries where regulatory frameworks and infrastructure are still evolving (Cybersecurity Ventures 2024).
Kenya's FinTech ecosystem is one of the most vibrant in Africa, with 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, many of which are delivered through cloud-based platforms. Despite these advancements, Kenyan FinTechs face unique challenges in cloud security, including internal threats, data destruction, and compliance with local and international regulations (CBK 2024).

The rapid adoption of cloud technologies by Kenyan FinTechs has exposed these organizations to a range of security risks, including data breaches, unauthorized access, and systemic vulnerabilities. While global security frameworks such as NIST and ISO/IEC 27001 provide broad guidelines, they often fall short in addressing the specific challenges faced by fintechs in emerging markets like Kenya. There is a critical need for a tailored security assessment framework that integrates local regulatory requirements and addresses the unique threat landscape faced by Kenyan FinTechs (T. Jensen 2022). The absence of a standardized security framework has led to the development of ad hoc security measures that may not adequately protect against advanced cyber threats (Cybersecurity Africa Report 2024). This study aims to address this gap by developing and validating a security measurement framework that combines essential security parameters for cloud security operations and aligns with global standards and local regulatory requirements.

Specific Objectives of the study are:

- To develop a security measurement framework index that combines essential security parameters for cloud security operations.
- To evaluate and validate the effectiveness of the developed security assessment framework in addressing cloud security challenges for FinTech companies in Kenya.

2. Literature Review

2.1 Cloud Security Frameworks

Several cloud security frameworks have been developed to guide organizations in securing their cloud environments. These frameworks include COBIT, NIST, ISO/IEC 27017, and the AWS Well-Architected Framework. While these frameworks provide comprehensive guidelines, they often require customization to address the specific needs of FinTechs in emerging markets.

COBIT 5: This framework provides governance and management guidelines for IT activities, emphasizing risk management and performance measurement. However, it lacks specific technology advice and requires significant customization for cloud environments (Wallarm. 2024).

NIST SP 800-144: This framework offers focused guidance on cloud security threats and vulnerabilities, providing practical recommendations for risk mitigation. However, it is primarily focused on government organizations and may not fully address the needs of fintechs (NIST 2011).

ISO/IEC 27017: This international standard provides specialized instructions for cloud security control practices, addressing data classification, encryption, and access protocols. However, its implementation can be complex and resource-intensive, particularly for smaller organizations (IT Governance. Iso-27017 and iso-27018.).

AWS Well-Architected Framework: This framework provides a structured approach to building secure and efficient cloud infrastructures, focusing on operational excellence, security, reliability, performance efficiency, and cost optimization. However, it is heavily dependent on AWS services, which may limit its applicability to other cloud platforms (Tutorials Dojo. Aws, 2024).

2.2 Security Metrics and Measurement

Security metrics are essential for assessing the effectiveness of cloud security measures. These metrics enable organizations to track and evaluate the security and privacy levels of their cloud operations, improving data clarity and supporting strategic decision-making. The Goal-Question-Metric (GQM) methodology is a widely used approach for developing security metrics and aligning them with organizational goals and objectives.

3. Research Methodology

3.1 Design and Methodology

The research design employed a mixed-method approach, integrating 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.

Scientists implemented experimental research methods to understand technical issues in cloud computing. An investigation using a private cloud service platform called OwnCloud in a FinTech environment detected vulnerabilities that users might face during operation.
The research used the Goal-Question-Metric (GQM) approach to build an assessment system designed for cloud security measurements. This methodology allowed scientists to build an assessment framework that measured security strengths across cloud systems. Given the absence of universally recognized cloud security metrics, the framework underwent customizing to address FinTech business requirements through goal-oriented metric alignment.

3.2 Framework Building Through Metrics

The framework was developed using the GQM methodology, which 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): A 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.
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 (D.M. Mwaura 2023).

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 (J.M. Njoroge 2024). 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 FinTechs.

4. Results and Discussion

4.1 Framework Development

The framework was developed to address the specific cloud security challenges faced by Kenyan FinTechs. It consists of five primary domains: Identify, Protect, Detect, Respond, and Recover. Each domain includes specific metrics and sub-metrics designed to measure the effectiveness of cloud security measures.

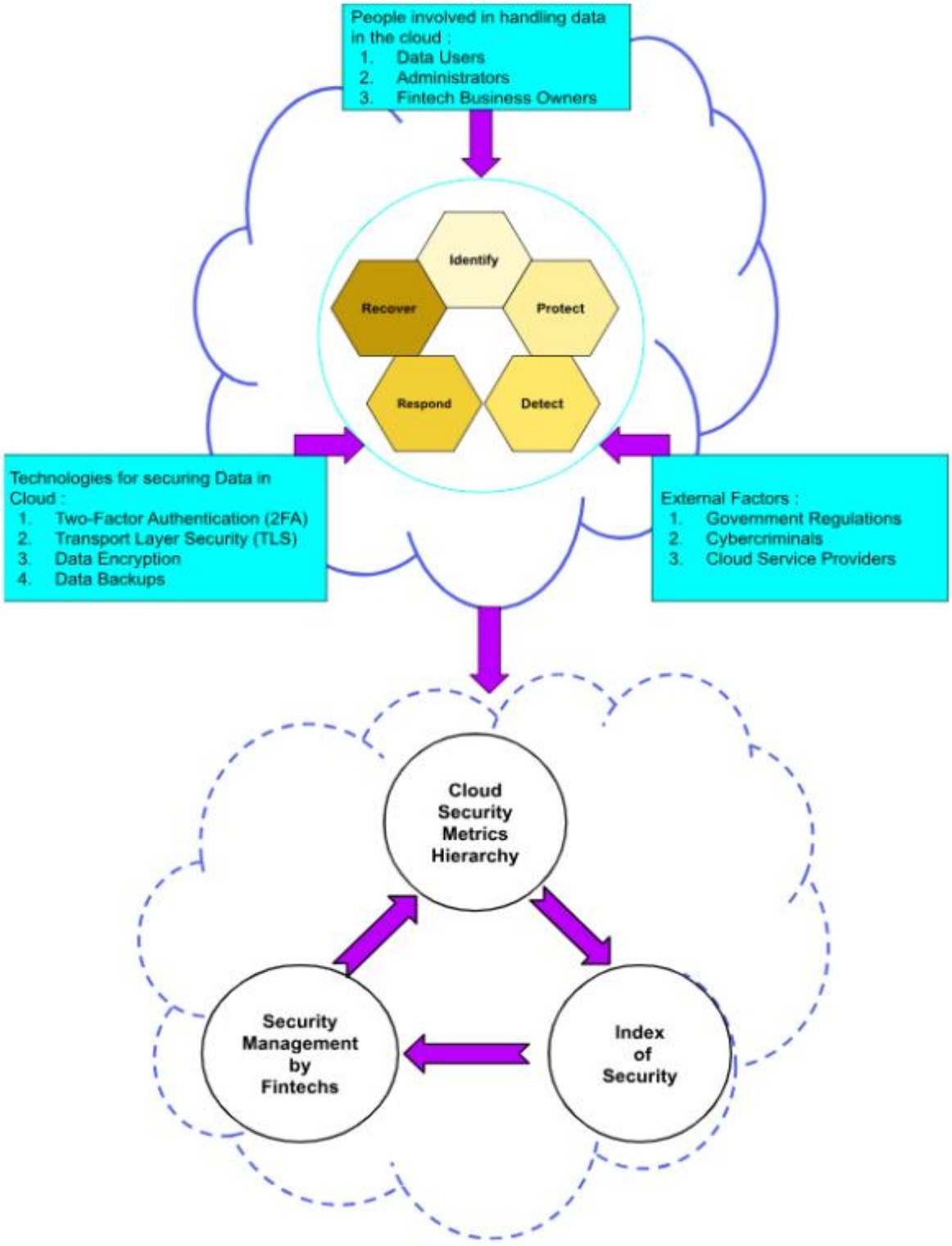

Figure 1: Framework for Enhancing Cloud Computing Security.
Source: Authors (2025)

4.1.1 Security Metrics Hierarchy

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, depicted in Figure 2, is a new method for visualizing security-related information gathered from the cloud environments utilized by the FinTech sector.

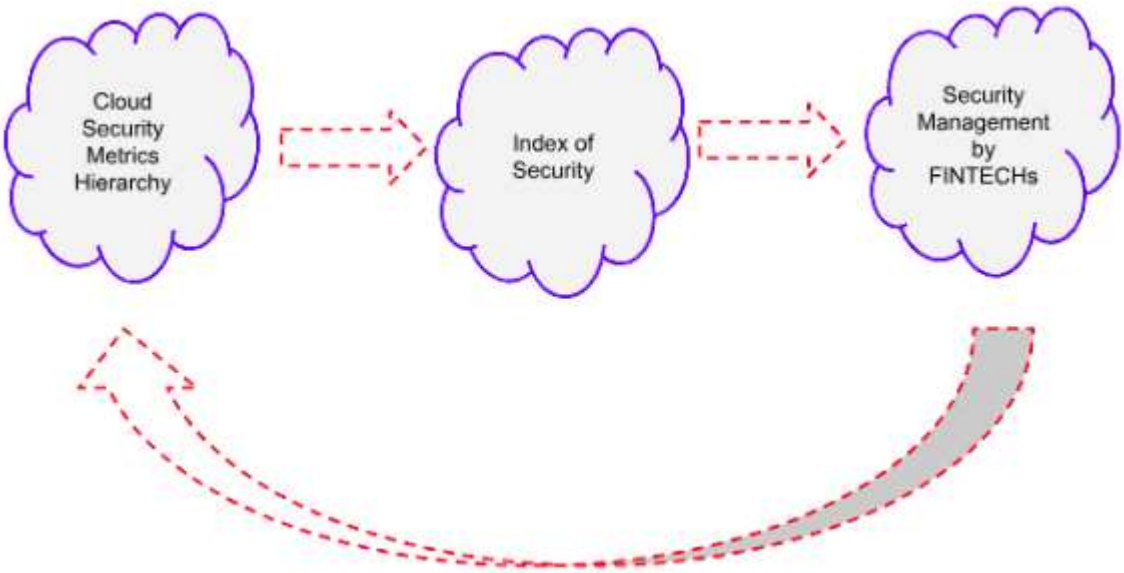

Figure 2: Life Cycle of Security Management.
Source: Authors (2025)

4.1.2 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 1 shows the components organized into specific areas of security that need to be focused on.

Table 1: 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: Authors (2025)

The initial thing to establish proper governance and security begins with proper identification and management of IT assets. Even though it is crucial these challenges 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 remain 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 and 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 own environments, such as data centers, office equipment, IoT devices, and mobile workforce tools.

It's important for cloud providers 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.

4.1.3 Framework Validation

The framework was validated against global security standards, including COBIT, ITIL, and ISO frameworks. The validation process involved assessing the framework's alignment with these standards and testing its effectiveness through experimental analysis and questionnaire-based data collection.

4.2 Experimental Analysis

The experimental analysis focused on identifying vulnerabilities and threats in cloud environments using the OwnCloud platform. The results revealed several key security challenges, including internal threats, data destruction issues, and compliance with regulatory requirements.

4.2.1 Internal Threats

The study identified internal threats as a significant security challenge. Rogue administrators pose a major risk to cloud security, and the ability of administrators to reset user passwords without exposing password visibility was identified as a critical vulnerability.

4.2.2 Data Destruction

The study also highlighted data destruction as a key security challenge, with deleted files remaining accessible in the cloud for up to 30 days. This poses significant privacy and security risks, particularly in environments where sensitive financial data is stored.

4.3 Framework Implementation

This developed framework outlines a lifecycle-based approach for managing cybersecurity from both technical and organizational perspectives. The framework has levels; group metrics, individual metrics, and sub-metrics. The group metrics; are Identify, Protect, Detect, Respond, and then Recover. This represents the primary domains to focus on for effectively securing cloud-based data. For each group metric, detailed subcategories and associated technologies are specified to guide the implementation of specific measures.

Priority levels are introduced to help organizations prioritize the sub-metrics that need immediate attention for reducing risk while balancing the effort required for their implementation. These priorities aim is:

- Simplify the identification of critical submatrices that need high priority.
- Support organizations to carry out risk analysis and management processes with ease.

High-priority levels for sub-metrics are assigned based on two key Conditions;

- Cyber Risk Reduction: This considers factors such as exposure to threats (probability of a threat occurring), occurrence probability, and the potential damage caused by a threat.
- Ease of Implementation: This evaluates the technical and organizational maturity required to implement specific measures.

The framework defines a three-tier priority scale for sub-metrics:

- High Priority: Actions that significantly reduce one or more key risk factors therefore must be executed regardless of complexity.
- Medium Priority: Reduce a risk factor and are relatively easy to implement.
- Low Priority: Actions that reduce a risk factor but are more challenging to implement, often requiring substantial organizational or infrastructural changes.

The framework uses well-known security standards from around the world, including COBIT5, NIST (National Institute of Standards and Technology), ISO (International Organization for Standardization), CSA (Cloud Security Alliance) STAR, and AWS (Amazon Web Services) well-architected framework. to validate the sub-metrics and their alignment with best practices. The classification of sub-metrics provides clear guidance on responsibilities and procedures, ensuring proper management of IT assets and resources.

Table 2 below (Developed Framework 2025) details the framework structure, including the priority levels, validation references, applicable group metrics, and classification. The research introduces a scoring mechanism, assigning one (1) point for ”yes” and zero (0) for ”no” responses. Using the GQM (Goal Question Metric) formula, the total score can indicate the level of security achieved for cloud-based data by a FinTech.

Table 2: Framework Component Subdivision/ Details

Level	Description	Priority	Validation References	Classification	Type	Metric
1	**IDENTIFY RISKS IN CLOUD**				Group	*Met1*
1.1	**Asset Management (1.1):** The resources, personnel, infrastructure, equipment, and services that support the Fintech's business processes are identified and managed in alignment with their significance to business goals and the organization's risk strategy.				Metric	*M et1.1*
1.1.1	ID.AM-1: Are all physical IT equipment (computers, laptops, BYOD) within the Fintech inventoried?	HIGH	COBIT 5 BAI09.01, BAI09.02 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8	Fintech Administratiors need to comply.	Sub-Metric	*M et1.1.1*
1.1.2	ID.AM-2: Is there a complete inventory of all system and application software within the Fintech?	HIGH	COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8	Fintech Administratiors need to comply.	Sub-Metric	*M et1.1.2*
1.1.3	ID.AM-3: Do cloud providers enable the Fintech to specify where their content is stored, ensure its security during transit and at rest, and manage it effectively?	LOW	COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9,PL-8	Cloud providers need to provide the information.	Sub-Metric	*M et1.1.3*
1.1.4	ID.AM-4: Does the Fintech ensure that external information system service providers comply with the Fintech's information security requirements, including applicable laws, policies, regulations, standards, and guidelines?	HIGH	COBIT 5 APO02.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9	Fintech Administratiors need to comply.	Sub-Metric	*M et1.1.4*
1.1.5	ID.AM-5: Does the cloud provider define the resilience measures in place to support the delivery of critical services across all operating states (e.g., during normal operations, under duress or attack, and during recovery)?	Medi…	ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 COBIT 5 APO03.03,APO03.04, BAI09.02	Cloud providers need to provide the information.	Sub-Metric	*M et1.1.5*

4.3.1 Evaluating the Framework’s Functionality

The Security Index (SecIndex) is determined by selecting the highest value from a set of security metrics:
SecIndex = max(Metric 1, M etric2, Metric 3, Metric 4, Metric 5)
Example:
SecIndex = max(Metric 1, M etric2, Metric 3, Metric 4, Metric 5) = max(0, 1, 0, 1, 0) = 0

Hence, **SecIndex = 0**, Which implies that the cloud environment is not secure.

Example:

SecIndex = max(Metric 1, M etric2, Metric 3, Metric 4, Metric 5) = max(0, 0, 1, 1, 1) = 1

Here, **SecIndex = 1**, which implies the cloud environment is secure.

At every level in the hierarchy, the max function is used to propagate the highest measured value upward, ensuring that only the most significant metric is passed to the next level.

The value of a **Metric Group (Metric x)** is defined as the maximum value among its constituent metrics;

$$Metric_x = \max(Metric_{x.1}, Metric_{x.2}, \ldots, Metric_{x.n})$$

E.g ;

$$Metric_1 = \max(Metric_{1.1}, Metric_{1.2}, Metric_{1.3})$$

Best-Case Scenario

$$Metric_1 = \max(Metric_{1.1}, Metric_{1.2}, Metric_{1.3}) = \max(1, 1, 1) = 1$$

$$Metric_2 = \max(Metric_{2.1}, Metric_{2.2}, Metric_{2.3}, Metric_{2.4}, Metric_{2.5}) = \max(1, 1, 1, 1, 1) = 1$$

Similarly:

$$Metric_3 = 1, \quad Metric_4 = 1, \quad Metric_5 = 1$$

Non-Secure Scenario

$$Metric_1 = \max(Metric_{1.1}, Metric_{1.2}, Metric_{1.3}) = \max(1, 0, 0) = 0$$

$$Metric_2 = \max(Metric_{2.1}, Metric_{2.2}, Metric_{2.3}, Metric_{2.4}, Metric_{2.5}) = \max(1, 1, 0, 0, 0) = 0$$

Similarly:

$$Metric_3 = 0, \quad Metric_4 = 0, \quad Metric_5 = 0$$

The value of a **Sub-Metric (Metric_x.y)** is calculated as the maximum among its sub-components:

$$Metric_{x.y} = \max(Metric_{x.y.1}, Metric_{x.y.2}, \ldots, Metric_{x.y.n})$$

E.g ;

$$Metric_{2.2} = \max(Metric_{2.2.1}, Metric_{2.2.2}, Metric_{2.2.3}, Metric_{2.2.4}, Metric_{2.2.5})$$

Best-Case Sub-Metric Example

$$Metric_{4.1} = \max(Metric_{4.1.1}, Metric_{4.1.2}, Metric_{4.1.3}, Metric_{4.1.4}, Metric_{4.1.5}) = \max(1, 1, 1, 1, 1) = 1$$

$$Metric_{3.3} = \max(Metric_{3.3.1}, Metric_{3.3.2}, Metric_{3.3.3}, Metric_{3.3.4}) = \max(1, 1, 1, 1) = 1$$

$$Metric_{4.1} = 1$$

Non-Secure Sub-Metric Example

$$Metric_{1.1} = \max(Metric_{1.1.1}, Metric_{1.1.2}, Metric_{1.1.3}, Metric_{1.1.4}, Metric_{1.1.5}) = \max(1, 0, 0, 0, 1) = 0$$
$$Metric_{1.2} = \max(Metric_{1.2.1}, Metric_{1.2.2}, Metric_{1.2.3}, Metric_{1.2.4}) = \max(0, 0, 0, 1) = 0$$
$$Metric_{1.3} = 0$$

Each **Sub-Metric** ($Metric_{x.y.n}$) evaluates to either 1 (for "Yes") or 0 (for "No"). For example:

- Is data encrypted during transit (upload/download from the cloud)? If **Yes**, $Metric_{2.3.2} = 1$ If **No**, $Metric_{2.3.2} = 0$

Using these metrics, the Security Index for a FinTech organization can be calculated, yielding a result of either Secure or Not Secure.

If the above metrics are used to compute the security index of a FinTech organization X, the result will indicate whether the organization is secure (1) or not secure (0). A typical scenario is illustrated in Figure 3.

Level	Description	Metric	Sec Index
1	IDENTIFY RISKS IN CLOUD	Met1	
1.1	**Asset Management (1.1):** The resources, personnel, infrastructure, equipment, and services that support the Fintech's business processes are identified and managed in alignment with their significance to business goals and the organization's risk strategy.	M et1.1	
1.1.1	ID.AM-1: Are all physical IT equipment (computers, laptops, BYOD) within the Fintech inventoried?	M et1.1.1	0
1.1.2	ID.AM-2: Is there a complete inventory of all system and application software within the Fintech?	M et1.1.2	0
1.1.3	ID.AM-3: Do cloud providers enable the Fintech to specify where their content is stored, ensure its security during transit and at rest, and manage it effectively?	M et1.1.3	1
1.1.4	ID.AM-4: Does the Fintech ensure that external information system service providers comply with the Fintech's information security requirements, including applicable laws, policies, regulations, standards, and guidelines?	M et1.1.4	0
1.1.5	ID.AM-5: Does the cloud provider define the resilience measures in place to support the delivery of critical services across all operating states (e.g., during normal operations, under duress or attack, and during recovery)?	M et1.1.5	1
Secure ?			0

Figure 3: Illustration of a typical security index computation scenario
Source: Framework

The framework was rigorously validated against industry standards and thoroughly tested to confirm its functionality and effectiveness in enhancing security in cloud systems used by FinTechs.

5. Conclusion and Recommendations

5.1 Using the Framework

FinTech organizations can execute the framework implementation through a five-step process depicted below in Figure 4.

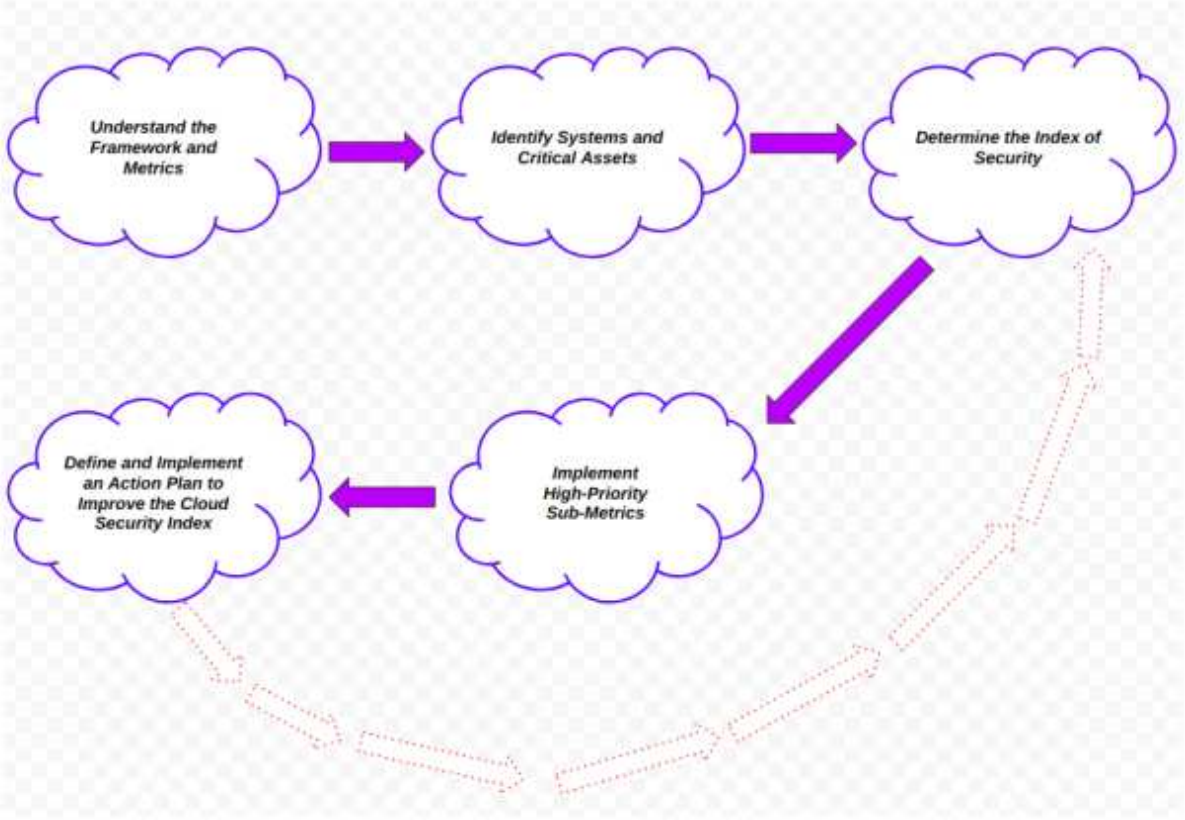

Figure 4: Steps for Using the Framework
Source: Authors (2025)

- Understand the Framework and Metrics: FinTech companies need to deeply understand both the framework structure and its individual elements before applying them according to their business requirements.
  The practice begins by referring to public documentation about the framework. Organizations must examine public descriptions of cloud security operations and then customize them to meet unique organizational requirements. The metrics feature straightforward evaluation through structured yes/no questions.

- Identify Systems and Critical Assets: Organizations need to identify their essential IT infrastructure systems before they continue. systems and information assets are essential for operations. The assessment requires this step to move forward effectively. The assessment process requires systems and critical assets identification for conducting impact evaluations and protection requirements. The final responsibility for putting each sub-metric into practice ensures that FinTech organizations stay accountable.

- Determine the Index of Security: Analysis of sub-metric questions produces their respective answers. Service evaluation uses the GQM methodology to compute an Index of Security that determines system stability. The organization's security status can be determined with this Index of Security calculation.

- Implement High-Priority Sub-Metrics: Organizations must now establish their priorities and take corresponding action. Enhanced preparedness with better cloud security awareness becomes possible through this phase. Organizations must apply risk assessment along with gap detection to measure the distance from their existing security level toward an ideal secure condition.

- Define and Implement an Action Plan to Improve the Cloud Security Index: Finally, organizations develop an action plan outlining necessary activities to achieve a secure security index. This plan includes a timeline based on identified risks and specific operational conditions. Continuous improvement should be a priority even after achieving the target profile, ensuring the framework evolves alongside new risks and technologies.

Clearly, it is preferable to have a continuous evolution of the Framework implementation, even after achieving the target profile, in line with periodic risk assessments and ongoing improvement actions.

5.2 Conclusion

The study successfully developed and validated a security measurement framework for cloud computing in Kenyan FinTechs. The framework provides a practical tool for FinTechs to measure and improve their cloud security performance, ensuring alignment with global standards and local regulatory requirements. The framework's effectiveness was demonstrated through experimental analysis and questionnaire-based data collection, with the results highlighting its ability to address key cloud security challenges, including internal threats, data destruction, and regulatory compliance.

5.3 Recommendations

Based on the findings, the following recommendations are proposed:

- Implementation of the Framework: FinTechs should implement the developed framework to measure and improve their cloud security performance. The framework provides a structured approach to identifying and mitigating security risks, ensuring alignment with global standards and local regulatory requirements.

- Continuous Monitoring: FinTechs should establish continuous monitoring processes to track and evaluate the effectiveness of their cloud security measures. This will enable organizations to identify and address emerging security threats on time.

- Collaboration with Cloud Providers: FinTechs should collaborate with cloud service providers to enhance transparency and improve security measures. This includes developing data retention formats, deletion methodologies, and recovery protocols that align with organizational requirements.

- Training and Awareness: FinTechs should invest in training and awareness programs to educate employees and stakeholders about cloud security risks and best practices. This will help to minimize the risk of internal threats and ensure compliance with regulatory requirements.

References

Central Bank of Kenya. (2024). *Annual report on the state of financial services in Kenya.* Central Bank of Kenya.

Cybersecurity Ventures. (2024). *Cybercrime incidents in East Africa: Report on rising cyber threats in East Africa.*

Cybersecurity Africa Report. (2024). *Trends and predictions in East African cyber threats.* Cybersecurity Africa.

Jensen, T. (2022). Challenges in implementing international cybersecurity standards in the African FinTech sector. *Journal of Cyber Policy, 7*(1), 58–72.

Wallarm. (2024). *COBIT 5 for cloud security.*

National Institute of Standards and Technology (NIST). (2011). *NIST US government cloud computing technology roadmap, release 1.0 (draft).* NIST.

IT Governance. (2023). *ISO-27017 and ISO-27018.* Retrieved from https://www.itgovernance.co.uk/

Tutorials Dojo. (2024). *AWS.*

Mwaura, D. M., & Mugo, R. (2023). Exploring the cloud security challenges in the Kenyan financial technology sector. *Journal of Cloud Computing and Security, 12*(2), 45–63.

Njoroge, J. M., & Njenga, A. (2024). Systematic approaches to sampling in cloud security research. *Computing Research Review, 16*(1), 78–92.

Business Daily Africa. (2023). Kenya's FinTechs confront cyber threats as incidents rise. *Business Daily Africa.*

Intelligent CIO Africa. (2023). Kenya's mobile-first strategies make FinTechs vulnerable to cyber attacks. *Intelligent CIO Africa.*

Cloud Security Alliance. (2022). *Blockchain for secure cloud transactions in FinTech: Enhancing transparency and reducing fraud.*

Cloud Security Alliance. (2022). *User authentication technologies in FinTech cloud security: An evaluation of biometric and multi-factor authentication.*

CrowdStrike. (2024). *Cloud security issues: Risks, threats, and challenges.*

European Union Agency for Cybersecurity (ENISA). (2021). *Data protection in cloud computing.*

Finextra. (2023). *Future of FinTech in Africa: Cloud will open new doors for the African FinTech industry.*

European Union Agency for Network and Information Security (ENISA). (2024). *Cloud computing security risks and benefits: Comprehensive analysis of cloud risks and operational benefits.*

Forrester's. (2024). *Cloud computing deployment models.*

ISO/IEC. (2015). *ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls for cloud services.*

Obura, J. O., & James, R. (2021). Security threats, mitigation, and framework for cloud computing applications: A theoretical review. *Conference Paper,* 24.

Microsoft. (2024). *What is cloud computing? Azure.*

European Network and Information Security Agency (ENISA). (2018). *Security and resilience in cloud computing: Strategies and challenges. ENISA Publications.*