Evaluating the Effectiveness of SIM Card Re-Registration as a Cybersecurity Intervention: Evidence from Ghana

Dennis Redeemer Korda
Department of Computing & IT
Bolgatanga Technical University

Obeng Owusu-Boateng
Department of Mathematics & ICT
E. P. College of Education,
Bimbilla, Ghana

Eric Ayintareba Akolgo
Department of Computer Science
Regentropfen University College,
Ghana

Nelson Seidu
Department of Computer Science
Regentropfen University College, Ghana

Kofi Nyame Barnes
ICT Directorate
Dr. Hilla Limann Technical University (DHLTU)

ABSTRACT
SIM card re-registration policies have been widely adopted across developing countries as a strategic intervention to combat cybercrime, strengthen national security and enhance digital identity management systems. In Ghana, the policy was implemented as part of broader efforts to curb the rising incidence of mobile money fraud, identity theft, impersonation and the misuse of anonymous communication channels. By linking SIM cards to verified national identity databases, policymakers anticipated improved traceability of users and increased accountability within the telecommunications ecosystem. Despite high levels of compliance and nationwide enforcement, cybercrime incidents continue to persist, raising concerns about the actual effectiveness of the policy in achieving its intended objectives. This study critically evaluates the impact of SIM card re-registration on cybersecurity outcomes in Ghana. Adopting a qualitative analytical approach, the research draws on empirical evidence, policy documents and secondary data sources to examine both the strengths and limitations of the initiative. The findings reveal that while SIM re-registration significantly enhances user identification, supports law enforcement investigations and strengthens regulatory oversight, it does not sufficiently address the complex and evolving nature of cyber threats. Persistent vulnerabilities such as fraudulent registrations, identity theft, insider threats, weak system integration and the growing use of internet-based communication platforms undermine the effectiveness of the policy. Therefore, the study argues that SIM re-registration should not be viewed as a standalone solution but rather as a complementary measure within a broader cybersecurity strategy. To address these gaps, the paper proposes a multi-layered cybersecurity framework that integrates AI-driven threat detection, robust digital identity management systems, secure communication protocols and continuous user awareness programs. This holistic approach is expected to provide a more resilient and adaptive defense against emerging cyber threats in Ghana and similar developing economies.

Keywords
Cybersecurity, Mobile money, Cyber Security Authority, threats, Authentication.

1. INTRODUCTION
The proliferation of mobile technologies has significantly transformed digital economies, particularly in sub-Saharan Africa. Over the past decade, the region has experienced unprecedented growth in mobile penetration and digital financial services, enabling millions of previously unbanked individuals to access banking, payment and remittance systems [1]. In Ghana, mobile money has emerged as a critical component of the economy, facilitating everyday financial transactions for individuals and businesses alike. According to the [2] mobile money transactions exceeded GHS 1 trillion in 2023, highlighting the deep integration of mobile platforms into Ghana's economic activities.

While these developments have increased financial inclusion, they have simultaneously expanded opportunities for cybercrime. Ghana has witnessed a sharp rise in mobile-based fraud, SIM swap attacks, identity theft and phishing incidents. Data from the Cyber Security Authority [3] indicate that nearly 50% of reported cybercrime cases in Ghana are linked to mobile financial platforms, underscoring the persistent nature of these threats. Financial losses from cybercrime have also increased over recent years, rising from GHS 33 million in 2021 to approximately GHS 56 million in 2022, with mobile money-related scams contributing significantly to these losses [4].

To mitigate these threats, Ghana has implemented SIM card registration and re-registration exercises aimed at improving accountability, enhancing national security and linking mobile subscribers to verified identity systems. The initial SIM registration exercise, introduced in 2010, required mobile network subscribers to provide identification documents to verify their ownership of SIM cards. Subsequent exercises in 2015 and 2019 sought to update subscriber records and address lapses identified during prior registrations [5]. The upcoming SIM re-registration exercise, announced in 2026, aims to further tighten compliance by integrating biometric verification and linking all SIM cards to the National Digital Identity system managed by the National Identification Authority (NIA) [6]. These exercises collectively seek to reduce mobile money fraud, prevent anonymous SIM usage and enable law enforcement agencies to trace criminal activity more effectively.

Despite these measures, cybercrime persists. Investigations show that criminals continue to exploit weaknesses in the registration processes, such as using fake or fraudulently obtained identity documents, purchasing pre-registered SIM

cards and leveraging insider collusion [7]. SIM-based interventions also face challenges related to operational inefficiencies, human errors in data capture and gaps in verifying biometric data against national databases. For example, while millions of SIM cards were re-registered in the 2019 exercise, not all records were accurately authenticated, creating potential loopholes for fraudsters [8].

Furthermore, the scope of cyber threats has evolved beyond SIM-based vulnerabilities. Many attacks now occur via internet-based platforms, encrypted messaging applications and social engineering tactics, which SIM registration alone cannot address [1]. The growing use of mobile applications for financial transactions, peer-to-peer payments and e-commerce has created attack surfaces that are independent of SIM card identity. Therefore, while SIM re-registration improves traceability and strengthens regulatory oversight, it cannot fully mitigate the complex, multi-dimensional nature of contemporary cyber threats.

Research also indicates that user behavior and digital literacy significantly influence vulnerability to cybercrime. In Ghana, surveys show that more than 50% of mobile money users lack awareness of common fraud techniques, leaving them exposed to scams even when SIM registration policies are in place [5]. This highlights that technological interventions alone, such as SIM registration, must be complemented by public education, secure system architectures and proactive monitoring to achieve meaningful cybersecurity outcomes.

Given the persistence of cybercrime despite multiple SIM registration exercises, questions arise regarding the effectiveness of the upcoming 2026 exercise. While linking SIM cards to verified identities remains a foundational step for accountability, the limitations of prior exercises demonstrate that SIM registration should not be treated as a standalone solution. A holistic approach is required, one that integrates secure digital identity management, AI-driven threat detection, robust authentication mechanisms and continuous user education. Such a multi-layered cybersecurity framework can address the systemic, technological and human vulnerabilities that undermine the effectiveness of SIM registration [9]; [1].

This study, therefore, seeks to critically evaluate the effectiveness of SIM card registration and re-registration exercises in Ghana, with particular attention to their impact on mobile money fraud, identity theft and cybercrime mitigation. By analyzing the outcomes of previous exercises (2010, 2015, 2019) and considering the design of the upcoming 2026 exercise, the study aims to identify lessons learned, remaining gaps and recommendations for a more resilient and adaptive cybersecurity strategy. Such analysis is crucial for informing policymakers, telecommunications regulators and law enforcement agencies on the most effective strategies for enhancing digital security in an increasingly mobile-dependent economy.

1.1 Problem Statement

Although SIM re-registration policies are designed to reduce cybercrime by linking mobile subscribers to verified identities, empirical evidence indicates that cyber threats continue to persist in Ghana despite these measures. Reports from the Cyber Security Authority [10] indicate that mobile fraud and identity-based cybercrime account for approximately 45% of all reported cybercrime cases in the country, highlighting the enduring nature of these threats. These figures suggest that while SIM re-registration may improve traceability and accountability in theory, in practice, it has not been sufficient to prevent criminal activity or eliminate fraudulent behavior.

One key factor contributing to this limited effectiveness is the presence of operational and technical weaknesses in the registration process itself. Inconsistent data collection methods, human errors during data entry and inadequacies in system verification mechanisms have all been documented as significant vulnerabilities [7]. For instance, during the 2019 SIM re-registration exercise, millions of SIM cards were registered; however, a substantial portion of biometric data captured was either incomplete or not properly authenticated against national databases, creating opportunities for fraudsters to exploit the system [8]. Moreover, centralized storage of SIM registration data introduces potential security risks, as unauthorized access to these databases could result in large-scale identity compromise. These systemic and operational weaknesses underscore the inherent limitations of relying solely on SIM registration as a cybersecurity measure.

Criminal actors have also demonstrated considerable adaptability in circumventing SIM-based regulations. Fraudulent SIM registration, including the use of pre-registered or stolen SIM cards, continues to be a prevalent method through which cybercriminals bypass identification controls [1]. In addition, identity theft and social engineering attacks remain major avenues for exploiting mobile financial platforms. By manipulating users into divulging sensitive information, attackers can conduct fraudulent transactions without ever needing to compromise SIM registration directly [6]. Beyond SIM-based vulnerabilities, many cybercriminals are shifting operations to internet-based communication channels, such as encrypted messaging applications and social media platforms, where SIM registration mechanisms have limited applicability [5].

These realities indicate that SIM re-registration, while beneficial in enhancing regulatory oversight and traceability, does not fully address the complexity and dynamic nature of modern cyber threats. The evolving landscape of cybercrime in Ghana, characterized by increasing sophistication and multi-channel attack strategies, suggests that a singular focus on SIM registration is insufficient. Effective mitigation requires a multi-layered approach that combines identity verification with advanced technological interventions, such as AI-driven threat detection, secure digital identity management, encryption of communications and ongoing user education [6]; [1]. Only through the integration of these measures can stakeholders hope to comprehensively address the persistence of cybercrime and protect both individual users and broader financial systems.

1.2 Objectives of the Study

This study aims to:

- Evaluate the effectiveness of SIM card re-registration in reducing cybercrime.
- Identify technological, human and systemic limitations of the policy.
- Assess whether SIM re-registration aligns with broader cybersecurity goals.
- Propose a more comprehensive cybersecurity framework.

2. LITERATURE REVIEW

2.1 SIM Registration as a Security Tool

SIM card registration is widely recognized as a regulatory and security mechanism aimed at enhancing national security, improving accountability and supporting law enforcement efforts by linking mobile subscribers to verifiable identities. The fundamental premise of SIM registration is that by associating each SIM card with a unique individual through

validated identification documents such as national ID cards or biometric data authorities can reduce anonymity in telecommunications and improve the traceability of criminal activities [7]. This linkage enables the monitoring and attribution of mobile communications, thereby facilitating the identification of individuals involved in illegal activities such as fraud, terrorism and cybercrime.

From a law enforcement perspective, SIM registration plays a critical role in improving investigative efficiency. By maintaining accurate subscriber records, telecommunications providers and regulatory agencies can assist security agencies in tracking suspicious communications, reconstructing criminal networks and gathering digital evidence. Studies indicate that linking SIM cards to identifiable individuals allows authorities to trace calls, messages and transaction histories back to their source, thereby strengthening the capacity to detect and respond to criminal activities [8]. In contexts where mobile devices are widely used for financial transactions, such as mobile money services, SIM registration also serves as a foundational element of Know-Your-Customer (KYC) compliance frameworks, which are essential for preventing financial fraud and money laundering [9].

In Ghana and other African countries, SIM registration has been implemented as part of broader national security and digital governance strategies. Policymakers argue that eliminating anonymous SIM usage can deter criminal behaviour by increasing the risk of identification and prosecution. For instance, regulatory authorities have emphasized that SIM registration can help curb mobile-related crimes such as phone theft, fraudulent transactions and the dissemination of harmful or illegal communications (Institute of ICT Professionals Ghana [10]. Additionally, the integration of SIM registration with national identity systems particularly through biometric verification has been promoted as a means of strengthening identity management and ensuring the authenticity of subscriber information [11].

Beyond crime prevention, SIM registration also contributes to the development of secure digital ecosystems by enabling access to value-added services such as mobile banking, e-government platforms and digital identity systems. According to [9], registered SIM users are better positioned to access secure digital services that require verified identities, thereby supporting financial inclusion and digital transformation initiatives. In this regard, SIM registration serves not only as a security tool but also as an enabler of trust in digital systems, which is essential for the growth of digital economies.

However, while the theoretical benefits of SIM registration are widely acknowledged, the extent to which these benefits translate into measurable reductions in crime remains a subject of ongoing debate. Some studies suggest that although SIM registration enhances traceability and supports investigations, there is limited empirical evidence demonstrating a direct causal relationship between mandatory SIM registration and a reduction in crime rates [9]; [12]. Nonetheless, its role as a foundational tool for identity verification and regulatory oversight continues to make it a key component of cybersecurity and telecommunications policy frameworks globally.

2.2 Limitations of SIM-Based Security Approaches

Despite the recognized benefits of SIM registration as a mechanism for enhancing traceability and accountability in telecommunications, empirical evidence suggests that it has significant limitations as a standalone cybersecurity strategy. One of the most prominent challenges is the exploitation of weak identity verification systems during the registration process. In many developing countries, including Ghana, SIM registration exercises often rely on documents that may be forged, duplicated, or improperly validated. As noted by [11], weaknesses in identity verification frameworks can enable individuals to register SIM cards using false identities, thereby undermining the objective of linking SIM cards to legitimate users. This creates opportunities for cybercriminals to maintain anonymity despite regulatory measures.

Closely related to this issue is the widespread prevalence of third-party SIM usage across many African countries. SIM cards are frequently registered in the name of one individual but used by another, either due to lack of valid identification, informal market practices, or deliberate intent to evade accountability. Research by [12] highlights that such practices significantly weaken the reliability of subscriber identity data, making it difficult for law enforcement agencies to accurately trace criminal activities. This phenomenon undermines the fundamental premise of SIM registration policies and limits their effectiveness in addressing cybercrime.

Another major limitation is the introduction of new vulnerabilities associated with centralized data storage systems. SIM registration processes typically involve the collection and storage of large volumes of sensitive personal and biometric data in centralized databases. While this facilitates regulatory oversight, it also creates high-value targets for cyberattacks. According to [13], mandatory SIM registration systems can increase risks of data breaches, unauthorized surveillance and misuse of personal information, particularly in contexts where data protection frameworks are weak or inconsistently enforced. In such cases, the very systems designed to enhance security may inadvertently expose users to new forms of risk, including identity theft and large-scale data compromise.

Furthermore, SIM-based security approaches do not adequately address the evolving nature of cyber threats, which increasingly extend beyond traditional telecommunications channels. Cybercriminals are rapidly shifting towards internet-based platforms, including social media, encrypted messaging applications and phishing websites, which are not directly constrained by SIM registration requirements. As highlighted by [14], modern cyber threats are multi-layered and often exploit human vulnerabilities, such as social engineering, rather than relying solely on anonymity provided by unregistered SIM cards. This shift reduces the effectiveness of SIM registration as a comprehensive solution to cybercrime.

These limitations are consistent with broader perspectives in cybersecurity research, which emphasize that no single technological intervention can fully address complex and adaptive cyber threats. Notably, [15], in their work on AI and cybersecurity in developing contexts, argues that effective cyber defense requires integrated, multi-layered approaches that combine technological safeguards, institutional frameworks and user awareness. This reinforces the view that SIM registration should be considered only one component of a broader cybersecurity ecosystem rather than a definitive solution.

While SIM registration contributes to improved identity traceability and regulatory oversight, its effectiveness is constrained by weaknesses in verification systems, widespread third-party usage, data security risks and the evolving nature of cyber threats. Addressing these challenges requires a more

holistic approach that integrates robust identity management systems, decentralized data protection strategies, advanced threat detection mechanisms and continuous public education.

2.3 Cybersecurity Landscape and Systemic Challenges in Ghana

Studies indicate that the cybersecurity framework in Ghana is still evolving, with notable gaps in institutional capacity, technical infrastructure and coordination among key stakeholders. Although the country has made significant progress through the establishment of the Cyber Security Authority and the enactment of the Cybersecurity Act, 2020 (Act 1038), challenges persist in operationalizing these frameworks effectively [15]. These gaps hinder the country's ability to respond comprehensively to the increasing sophistication and frequency of cyber threats.

One of the primary challenges lies in limited institutional capacity. Effective cybersecurity governance requires highly skilled personnel, adequate funding and well-equipped institutions. However, evidence suggests that many public and private sector organizations in Ghana face shortages of cybersecurity professionals and lack the technical expertise needed to detect, prevent and respond to cyber incidents [16]. This capacity gap affects not only national cybersecurity agencies but also telecommunications operators, financial institutions and regulatory bodies that are critical to enforcing SIM registration policies and other digital security measures.

In addition to human capacity constraints, technical infrastructure remains a significant limitation. Robust cybersecurity systems depend on advanced technologies such as intrusion detection systems, real-time monitoring tools and secure data management platforms. While Ghana has made strides in digitalization, many systems remain fragmented and inadequately secured, increasing vulnerability to cyberattacks (World Bank, 2020). For instance, the integration between SIM registration databases, national identity systems and financial platforms is often incomplete or inconsistent, reducing the reliability and effectiveness of identity verification mechanisms.

Another critical issue is the lack of effective coordination among stakeholders. Cybersecurity in a digital economy requires collaboration between government agencies, telecommunications companies, financial institutions, law enforcement and end users. However, studies show that coordination among these actors in Ghana is often limited, leading to fragmented responses to cyber threats and inefficiencies in information sharing [15]. This fragmentation undermines the effectiveness of interventions such as SIM re-registration, which rely heavily on seamless collaboration between multiple institutions to achieve their objectives.

Furthermore, regulatory and enforcement challenges continue to affect the overall cybersecurity posture of the country. Although policies and legal frameworks exist, enforcement mechanisms are sometimes weak and compliance levels vary across sectors. This creates an environment where cybercriminals can exploit regulatory loopholes and inconsistencies in implementation. As noted by the [17], developing countries often face difficulties in translating cybersecurity policies into effective operational practices due to resource constraints and institutional inefficiencies.

These systemic weaknesses significantly limit the impact of isolated interventions such as SIM re-registration. While SIM registration can enhance traceability and accountability, its effectiveness is contingent upon the strength of the broader cybersecurity ecosystem in which it operates. Without robust institutional capacity, secure technical infrastructure and coordinated stakeholder engagement, such interventions are unlikely to produce sustained reductions in cybercrime. According to [15], the complexity of modern cyber threats necessitates a multi-layered approach that combines technological innovation, institutional strengthening and user awareness.

Ghana has made commendable progress in establishing a national cybersecurity framework, significant gaps remain. Addressing these challenges requires sustained investment in capacity building, infrastructure development and inter-agency coordination. Only through such comprehensive efforts can the country enhance the effectiveness of initiatives like SIM re-registration and build a resilient cybersecurity ecosystem capable of addressing evolving threats.

3. METHODOLOGY

This study adopts a qualitative research design to critically evaluate the effectiveness of SIM card re-registration as a cybersecurity intervention in Ghana. A qualitative approach is appropriate for this research because it enables an in-depth exploration of policy implementation, institutional dynamics and systemic challenges that cannot be adequately captured through purely quantitative methods. Qualitative research is particularly useful in cybersecurity and policy studies where contextual understanding, interpretation of practices and identification of underlying patterns are essential [18].

The study employs a multi-method qualitative strategy, combining document analysis, comparative evaluation and thematic analysis to ensure methodological rigor and triangulation of findings. First, document analysis is conducted on a wide range of secondary sources, including government policy documents, reports from the Cyber Security Authority, publications from the National Communications Authority and academic literature on cybersecurity and SIM registration. Document analysis is a systematic procedure for reviewing and interpreting textual data to extract meaning, identify trends and generate empirical insights [19]. This method allows the study to assess policy intentions, implementation strategies and reported outcomes of SIM registration exercises over time.

Second, the study conducts a comparative evaluation of cybersecurity outcomes before and after major SIM registration and re-registration exercises in Ghana, particularly those conducted in 2010, 2015 and 2019, as well as the ongoing reforms leading to the anticipated 2026 exercise. This comparative approach enables the identification of patterns, shifts and inconsistencies in cybercrime trends, including mobile money fraud and identity-related offenses. By examining changes in reported incidents, regulatory responses and institutional performance across these periods, the study assesses whether SIM re-registration has had a measurable impact on cybersecurity outcomes. Comparative analysis is widely used in policy research to evaluate the effectiveness of interventions across different timeframes and contexts [20].

Third, a thematic analysis is employed to systematically identify and analyze recurring themes related to the limitations of SIM-based security approaches. Themes such as weak identity verification systems, third-party SIM usage, data security vulnerabilities and evolving cyber threats are derived from the literature and policy reports. Thematic analysis provides a flexible yet rigorous framework for organizing qualitative data and uncovering patterns that explain complex phenomena [21]. This method is particularly useful for synthesizing diverse sources of information and generating

insights into the structural and operational weaknesses affecting SIM registration policies.

The study relies exclusively on secondary data sources, including government reports, peer-reviewed academic publications, industry reports (e.g., GSMA) and credible cybersecurity studies. Secondary data analysis is appropriate given the availability of extensive documentation on SIM registration policies and cybersecurity trends in Ghana. It also allows for cost-effective and comprehensive analysis while ensuring that the study draws on authoritative and verifiable sources [22].

To enhance validity and reliability, the study adopts a triangulation approach by integrating multiple data sources and analytical methods. This reduces bias and strengthens the credibility of the findings. Additionally, the study aligns with best practices in cybersecurity research, which emphasize the importance of combining policy analysis with empirical evidence to understand complex digital security challenges [15].

Overall, this methodological framework provides a robust basis for evaluating the effectiveness of SIM re-registration policies and identifying gaps that must be addressed through more comprehensive and adaptive cybersecurity strategies.

4. Findings and Discussion

4.1 Centralized Strengths of SIM Re-Registration

The findings of this study indicate that SIM card re-registration in Ghana has yielded several notable benefits, particularly in enhancing accountability and strengthening regulatory oversight within the telecommunications sector. One of the most significant advantages is improved traceability. By linking SIM cards to verified identities through national identification systems, authorities are better positioned to trace communications and investigate criminal activities. This aligns with global evidence suggesting that SIM registration enhances the ability of law enforcement agencies to attribute mobile-based transactions and communications to identifiable individuals [11]. In Ghana, this has been particularly relevant in addressing mobile money fraud and identity-related cybercrimes, where traceability is essential for prosecution and deterrence.

Another key strength is enhanced regulatory control. SIM re-registration has improved the capacity of regulators such as the National Communications Authority to enforce compliance among mobile network operators. By maintaining updated and verified subscriber databases, regulators can better monitor telecommunications activities, ensure adherence to Know-Your-Customer (KYC) requirements and support broader digital governance initiatives. This contributes to a more structured and transparent telecommunications ecosystem, which is critical for national security and economic stability [9].

Additionally, the study finds evidence of a deterrence effect, particularly in reducing opportunistic or low-level cybercrime. The removal of anonymity associated with unregistered SIM cards increases the perceived risk of detection among potential offenders, thereby discouraging certain forms of fraudulent behaviour. Similar observations have been reported in other African contexts, where SIM registration has contributed to a decline in petty mobile-related crimes, although its impact on organized cybercrime remains limited [12].

4.2 Key Limitations

a. Persistence of Cybercrime

Despite the benefits outlined above, the findings reveal that cybercrime remains widespread in Ghana, suggesting that SIM re-registration has had limited impact on addressing the root causes of cyber threats. Reports from the Cyber Security Authority indicate that mobile fraud, phishing and online scams continue to rise, even after multiple SIM registration exercises [3]. This persistence highlights the complexity of cybercrime, which extends beyond issues of anonymity and requires more comprehensive interventions.

b. Identity System Weaknesses

The effectiveness of SIM re-registration is further undermined by weaknesses in identity management systems. Fraudulent registrations, use of forged identification documents and identity theft continue to compromise the integrity of SIM-user linkage. As noted by [7], gaps in verification processes and incomplete integration between SIM registration systems and national identity databases create vulnerabilities that can be exploited by cybercriminals. Consequently, the reliability of subscriber data remains questionable in some cases.

c. Human and Operational Risks

Human and operational factors also present significant risks to the effectiveness of SIM re-registration. The study identifies issues such as human errors during data entry, inconsistent registration procedures across different centers and insider threats as critical vulnerabilities. These challenges can lead to inaccurate or incomplete data records, which in turn weaken the effectiveness of traceability mechanisms. According to [13], large-scale data collection exercises are particularly susceptible to such risks, especially in environments with limited oversight and capacity constraints.

d. Technological Limitations

Another major limitation is that SIM-based security measures do not adequately address the evolving technological landscape of cyber threats. Modern cybercrime increasingly relies on internet-based platforms, including phishing websites, malware distribution channels and encrypted messaging applications that operate independently of SIM registration controls. As highlighted by [9], cyber threats are becoming more sophisticated and multi-dimensional, often exploiting software vulnerabilities and human behavior rather than relying solely on anonymity provided by unregistered SIM cards. This significantly reduces the effectiveness of SIM re-registration as a standalone cybersecurity solution.

e. Centralized Data Risks

Finally, the centralization of SIM registration data introduces significant security and privacy risks. The aggregation of sensitive personal and biometric information into centralized databases creates attractive targets for cyberattacks. In the event of a data breach, large volumes of personal data could be exposed, leading to identity theft and other forms of cybercrime. [13] warns that such centralized systems, if not adequately secured, may inadvertently increase the risk of mass data compromise.

These findings reinforce the argument that while SIM re-registration offers important benefits in terms of traceability and regulatory control, it is insufficient to address the broader and more complex challenges of cybersecurity.

4.3 Proposed Solution: A Multi-Layered Cybersecurity Framework

The findings of this study suggest that SIM card re-registration,

while useful for improving traceability and regulatory oversight, is insufficient as a standalone solution for addressing the complex and evolving nature of cyber threats in Ghana. Consequently, this study proposes a multi-layered cybersecurity framework that integrates technological, institutional and human-centered approaches. Such a framework aligns with global best practices, which emphasize defense-in-depth strategies to mitigate diverse and adaptive cyber risks [23].

4.4 AI-Driven Threat Detection

A key component of the proposed framework is the adoption of artificial intelligence (AI) and machine learning techniques for real-time threat detection and prevention. AI-driven systems can analyze large volumes of transactional and behavioural data to identify anomalous patterns indicative of fraud or cyberattacks. For example, machine learning algorithms can detect unusual mobile money transactions, flag suspicious SIM activity and predict potential fraud attempts before they occur. According to [24], machine learning-based intrusion detection systems significantly enhance the ability to identify previously unknown threats compared to traditional rule-based approaches.

In the Ghanaian context, integrating AI into telecommunications and financial systems can improve proactive threat mitigation, particularly in detecting mobile money fraud and phishing schemes. This approach is consistent with the work of [25], who emphasizes the role of intelligent systems in strengthening cybersecurity resilience in emerging digital ecosystems.

4.5 Strong Digital Identity Systems

Another critical pillar of the framework is the development of robust digital identity systems. Effective identity management goes beyond SIM registration to include biometric verification, multi-factor authentication and continuous identity validation mechanisms. Biometric identifiers such as fingerprints and facial recognition can significantly reduce the risk of identity fraud when properly implemented [26].

Additionally, continuous authentication where user identity is verified throughout a session rather than at a single point can further enhance security by detecting unauthorized access in real time. Integrating SIM registration with secure national identity systems ensures that identity linkage is both accurate and resilient against manipulation. However, such systems must be designed with strong privacy protections to prevent misuse of sensitive data.

4.6 Secure System Architecture

The framework also emphasizes the importance of secure system architecture, particularly through the adoption of end-to-end encryption and zero-trust security models. End-to-end encryption ensures that data transmitted between users and service providers remains confidential and protected from interception. This is especially critical in mobile financial transactions and communication systems [27] ; [28] [29] [30]

Zero-trust architecture, which operates on the principle of "never trust, always verify," requires continuous validation of users, devices and network activities. According to [23], zero-trust models significantly reduce the risk of unauthorized access and lateral movement within systems. Implementing such architectures in Ghana's telecommunications and financial sectors can strengthen defenses against both internal and external threats.

4.7 Public Awareness and Education

Human factors remain one of the most exploited vulnerabilities in cybersecurity. Therefore, public awareness and education are essential components of the proposed framework. Training users to recognize phishing attempts, fraudulent calls and social engineering tactics can significantly reduce the success rate of cyberattacks. Research shows that user education is one of the most effective strategies for mitigating cyber risks, particularly in environments with high levels of digital adoption [28];[31] ;[32]

In Ghana, targeted awareness campaigns especially for mobile money users can help bridge the digital literacy gap and empower individuals to make informed security decisions. This aligns with broader cybersecurity strategies that emphasize the importance of user-centric approaches in reducing risk exposure.

4.8 Regulatory and Institutional Strengthening

Finally, strengthening regulatory and institutional frameworks is critical for sustaining cybersecurity efforts. This includes updating cybersecurity laws, improving enforcement mechanisms and enhancing collaboration among stakeholders such as the Cyber Security Authority, the National Communications Authority, financial institutions and law enforcement agencies.

Effective inter-agency collaboration enables timely information sharing, coordinated responses to cyber incidents and the development of unified security standards. According to the [17], countries with strong institutional coordination frameworks are better positioned to respond to cyber threats and implement effective cybersecurity policies.

The proposed multi-layered framework addresses the limitations of SIM re-registration by integrating advanced technologies, robust identity systems, secure architectures, user education and institutional strengthening. This holistic approach reflects the growing consensus in cybersecurity research that effective threat mitigation requires a combination of complementary strategies rather than reliance on a single intervention.

5. CONCLUSION

SIM card re-registration represents an important regulatory intervention aimed at enhancing identity traceability and strengthening national security in Ghana. By linking mobile subscribers to verified identities, the policy has contributed to improved accountability within the telecommunications sector and has provided law enforcement agencies with a useful tool for investigating cyber-enabled crimes. These benefits underscore the relevance of SIM registration as a foundational component of digital governance and cybersecurity frameworks.

However, the findings of this study clearly demonstrate that SIM re-registration is a necessary but insufficient measure for addressing the broader and more complex challenges of cybersecurity. Despite multiple registration exercises, cybercrime particularly mobile money fraud, phishing and identity-based attacks continues to persist. This indicates that the policy does not adequately address the root causes of cyber threats, which are multi-dimensional and constantly evolving. Weaknesses in identity verification systems, the prevalence of third-party SIM usage, human and operational vulnerabilities and the increasing shift toward internet-based attack vectors all limit the effectiveness of SIM-based controls.

Furthermore, the centralization of sensitive subscriber data introduces additional risks, including potential data breaches and misuse of personal information. These challenges highlight the inherent limitations of relying solely on identity-based regulatory mechanisms in a rapidly evolving digital threat landscape.

Consequently, this study emphasizes the need for a holistic, multi-layered cybersecurity approach that integrates technological, human and institutional solutions. Such an approach should incorporate advanced technologies such as AI-driven threat detection, robust digital identity systems, secure system architectures and continuous user awareness programs. In addition, strengthening regulatory frameworks and enhancing collaboration among key stakeholders including government agencies, telecommunications providers and financial institutions is essential for achieving sustainable cybersecurity outcomes.

In line with contemporary cybersecurity scholarship, this study concludes that effective cyber defense requires integrated and adaptive strategies rather than isolated interventions. Therefore, while SIM re-registration should remain part of Ghana's cybersecurity strategy, it must be complemented by broader systemic reforms to build a resilient and secure digital ecosystem capable of addressing current and emerging cyber threats.

6. REFERENCES

[1] Boateng, O. N., Agyemang, F., & Mensah, J. (2022). A fraud prevention and secure cognitive SIM card registration model. *Journal of Information Security and Applications, 67*, 103124. https://doi.org/10.1016/j.jisa.2022.103124

[2] Bank of Ghana. (2023). An Overview of Bank of Ghana (BoG) Fraud Report: Key Trends and Insights. GAB Research. https://gab.com.gh/assets/images/docs/Overview%20of%20BoG%20Fraud%20Report_UPDATED%20APRIL%202025.pdf

[3] Cyber Security Authority. (2025). *Annual cybersecurity report 2025: Ghana*. Accra, Ghana: CSA. https://www.csa.gov.gh

[4] TechLabari. (2025). Ghanaian biometric data collected for SIM registrations was never authenticated. https://techlabari.com/ghanaian-biometric-data-was-collected-for-sim-registrations-the-data-was-never-authenticated

[5] Modern Ghana. (2025). *Ghana's SIM re-registration: Fixing past flaws or not?*

[6] The Tracker. (2024). *SIM card registration and subscriber data traceability*. https://thetracker.media/12067/tech/elementor-12067/

[7] Minta, D. A. (2022). *Data security and protection during the national SIM card registration exercise in Ghana* (Unpublished doctoral dissertation). University of Cape Coast, Ghana. https://ir.ucc.edu.gh/xmlui/handle/123456789/11321

[8] GhanaWebbers. (2025). The Data-driven truth about Financial scams in Ghana. https://www.ghanawebbers.com/GhanaHomePage/NewsArchive/The-Data-Driven-Truth-about-Financial-Scams-in-Ghana-2029894

[9] GSMA. (2022). *Safety, Privacy and Security across the mobile ecosystem*. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2022/10/Safety-privacy-and-security-across-the-mobile-ecosystem.pdf

[10] Institute of ICT Professionals Ghana (IIPGH). (2017). *SIM registration – Fraud prevention mechanism in mobile communication space in Ghana*. https://iipgh.org/sim-registration-fraud-prevention-mechanism-mobile-communication-space-ghana/

[11] Apau, R. (2020). Digital forensic investigation and cybersecurity in Ghana. *International Journal of Cybersecurity*, 3(2), 45–62. https://www.sciencedirect.com/science/article/pii/S258971X20300619

[12] GSMA. (2016). *Mandatory registration of prepaid SIM cards*. GSM Association. https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

[13] ENACT Africa. (2019). *Will mandatory SIM card registration rid Tanzania of cybercrime?* https://enactafrica.org/enact-observer/will-mandatory-sim-card-registration-rid-tanzania-of-cybercrime

[14] Privacy International. (2019). *SIM card registration: A threat to privacy?* https://privacyinternational.org

[15] Cyber Security Authority (CSA). (2023). *National cybersecurity awareness report*. Accra, Ghana. https://www.csa.gov.gh

[16] Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management, 22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

[17] Korda, D. R., Dapaah, E. O., & Akolgo, E. A. (2024). The role of AI chatbots in education: A review. *AJSE*, *20*(1).

[18] World Bank. (2020). *Cybersecurity capacity review: Ghana*. World Bank Group. https://www.worldbank.org

[19] Creswell, J. W., & Poth, C. N. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications.

[20] Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

[21] Ragin, C. C. (2014). *The comparative method: Moving beyond qualitative and quantitative strategies*. University of California Press.

[22] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

[23] Johnston, M. P. (2017). Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries, 3*(3), 619–626.

[24] National Institute of Standards and Technology (NIST). (2020). *Zero trust architecture (SP 800-207)*. https://doi.org/10.6028/NIST.SP.800-207

[25] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*, 305–

316. https://doi.org/10.1109/SP.2010.25

[26] Feng, S. (2024). Integrating artificial intelligence in financial services: Enhancements, applications and future directions. *Applied and Computational Engineering*, *69*(1), 19-24.

[27] Jain, A. K., Ross, A., & Prabhakar, S. (2016). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), 4–20. https://doi.org/10.1109/TCSVT.2003.818349

[28] Green, M., & Smith, M. (2016). The cryptopals crypto challenges. *Communications of the ACM, 59*(7), 24–26. https://doi.org/10.1145/2948086

[29] Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

[30] Media Foundation for West Africa. (2021). *Internet Freedom Report – Ghana*.

[31] Kuzaga, E. B. (2025). An examination of laws and practices surrounding SIM card registration in Tanzania: A strategy to combat mobile phone-related cybercrime. *East African Journal of Law and Ethics, 8*(1). https://doi.org/10.37284/eajle.8.1.3595