IAA Journal of Scientific Research 13(1):28-31, 2026. www.iaajournals.org

©IAAJOURNALS ISSN: 2636-7319

https://doi.org/10.59298/IAAJSR/2026/1312831 IAAJSR:1311

Cybersecurity Challenges and Solutions for Mobile Money Platforms in East Africa

Arionget Jemima

Department of Pharmacoepidemeology Kampala International University Uganda
Email: jemima.arionget@studwc.kiu.ac.ug

ABSTRACT

Mobile money platforms have revolutionized financial inclusion in East Africa, enabling millions of previously unbanked individuals to access digital financial services. Platforms such as M-Pesa, MTN Mobile Money, and Tigo Pesa have facilitated financial transactions, promoted entrepreneurship, and strengthened the region's digital economy. However, the rapid adoption of these services has also introduced significant cybersecurity challenges, including social engineering attacks, agent-driven fraud, and fragmented regulatory frameworks. These threats compromise user trust, financial integrity, and the sustainability of mobile money ecosystems. This review examines the key cybersecurity risks affecting mobile money platforms in East Africa and evaluates potential mitigation strategies. Proposed solutions include enhanced authentication mechanisms, multi-factor verification frameworks, user education and awareness programs, and strengthened regulatory policies. By integrating technological, educational, and policy interventions, stakeholders can enhance the security and resilience of mobile financial services. The study underscores the importance of collaborative efforts among telecom operators, financial institutions, regulators, and users to ensure safe, trustworthy, and sustainable mobile money platforms across the region.

Keywords: Mobile money, cybersecurity, East Africa, social engineering, agent fraud, financial inclusion.

INTRODUCTION

Over the past decade, East Africa has emerged as a global leader in mobile financial innovations, with mobile money platforms revolutionizing financial inclusion and transforming the region's socio-economic landscape. Countries such as Kenya, Uganda, Tanzania, and Rwanda have witnessed an unprecedented expansion in mobile-based financial services, enabling millions of previously unbanked citizens to access digital financial tools [1]. Mobile money platforms like M-Pesa (Kenya), MTN Mobile Money (Uganda), and Tigo Pesa (Tanzania) have not only facilitated financial transactions but also promoted entrepreneurship, enhanced remittance services, and supported small-scale business operations. These platforms have become a cornerstone of East Africa's digital economy, bridging the gap between traditional banking systems and the informal sector [2]. However, as the use of mobile money services has grown exponentially, so have the associated cybersecurity challenges. With billions of transactions processed monthly, mobile money platforms have become prime targets for cybercriminals seeking to exploit vulnerabilities in the systems and among users. While these platforms promise convenience and financial empowerment, they are also susceptible to fraud, data breaches, system manipulation, and social engineering attacks, which threaten user trust and the overall sustainability of digital financial ecosystems in the region [3].

The proliferation of mobile money in East Africa can be attributed to the region's rapid mobile phone penetration and limited access to conventional banking infrastructure. According to the GSMA (Global System for Mobile Communications Association), East Africa accounts for over 50% of global mobile money transactions, with Kenya alone contributing a significant share. This growth has played a crucial role in achieving financial inclusion goals outlined in regional development frameworks, particularly those aligned with the United Nations Sustainable Development Goals (SDG 1 and SDG 9), which emphasize poverty reduction and the promotion of innovation and infrastructure [4]. Despite these advancements, the security of mobile money platforms remains a growing concern. Cyber threats are evolving in complexity and frequency, targeting both system vulnerabilities and human behavior. Recent studies indicate that a significant proportion of users have experienced or been exposed to fraudulent schemes such as phishing (fraudulent emails or SMS seeking personal information), vishing (voice call scams), and smishing (SMS-based fraud). For instance, one study reported that 33.4% of users strongly agreed that PIN sharing posed a major security challenge, highlighting the importance of addressing user awareness and behavioral risks [5].

Furthermore, agent-driven fraud, where mobile money agents engage in unethical practices such as overcharging, fake reversals, or account manipulation, has also become a persistent issue. Approximately 22.3% of respondents in recent surveys identified agent-related fraud as a major threat to the credibility of mobile money services. Additionally, the absence of robust regulatory frameworks and the uneven enforcement of cybersecurity standards across East African nations have created loopholes for criminal exploitation, including money laundering and terrorist financing. These challenges call for a comprehensive evaluation of cybersecurity measures in the mobile money sector [6]. The protection of user data, financial integrity, and institutional credibility is not only a technical issue but also a developmental imperative, as cyber insecurity undermines financial inclusion and erodes public confidence in digital innovations.

While mobile money platforms have significantly contributed to economic growth and financial inclusion in East Africa, their increasing integration into everyday financial transactions has exposed users and service providers to serious cybersecurity threats. Cybercriminals continue to exploit technological weaknesses, human error, and regulatory loopholes to perpetrate fraudulent activities. The lack of adequate user education on cybersecurity best practices has made many individuals vulnerable to deception, particularly through social engineering tactics such as phishing and smishing [7]. Moreover, existing cybersecurity frameworks in East Africa are fragmented, with varying levels of enforcement and coordination among governments, telecommunication companies, and financial regulators. This inconsistency leaves room for cross-border cybercrimes, which are difficult to detect and prosecute. As mobile money systems increasingly handle sensitive financial and personal data, the risks associated with unauthorized access, identity theft, and financial losses are magnified. Therefore, the problem lies not only in the sophistication of cyber threats but also in the limited capacity of stakeholders to implement, harmonize, and enforce effective cybersecurity policies and technological safeguards. Without coordinated interventions that combine regulatory reform, technological innovation, and user awareness, the region's mobile money ecosystem faces significant sustainability challenges [8].

The primary aim of this study is to investigate the cybersecurity challenges and potential solutions for mobile money platforms in East Africa, a rapidly growing segment of the region's financial ecosystem. Specifically, the study seeks to identify and analyze the major cybersecurity threats affecting mobile money services, including social engineering attacks and agent-driven fraud, which undermine user trust and the overall sustainability of these platforms. It also examines the causes and consequences of these cyber threats, evaluates the adequacy of existing regulatory frameworks governing mobile financial services, and explores both technological and policy-based interventions to enhance system security and resilience. Furthermore, the research aims to propose strategic recommendations for improving user education, fostering stakeholder collaboration, and strengthening policy enforcement to mitigate cybersecurity risks. By addressing these objectives, the study seeks to answer key questions regarding the nature and impact of cyber threats, the effectiveness of current regulations, and the role of technological and non-technological solutions in safeguarding mobile money platforms. The significance of this study lies in its contribution to academic discourse on financial technology security, its practical implications for telecom companies, financial institutions, and policymakers, and its emphasis on user awareness as a critical component of cyber resilience. Ultimately, the research supports regional development goals by promoting secure, trustworthy, and inclusive mobile financial services across East Africa.

Key Cybersecurity Challenges Identified

Mobile money services have revolutionized financial transactions, particularly in developing economies, by providing convenient, fast, and accessible means of transferring money. However, the rapid adoption of these platforms has been accompanied by a range of cybersecurity challenges that threaten both users and service providers [9]. Among the most pressing concerns are social engineering attacks, agent-driven fraud, and inadequate regulatory frameworks. Social engineering attacks, which include phishing, vishing, and smishing, exploit human vulnerabilities rather than technical flaws [10]. Cybercriminals manipulate users into revealing sensitive information such as PINs, passwords, and personal identification data, often resulting in unauthorized access to accounts and significant financial losses. Research indicates that 33.4% of respondents strongly agreed that PIN sharing constitutes a major security risk, highlighting the critical role of user behavior in mobile money security (p-value < 0.05) (MDPI) [11]. In addition to user-targeted attacks, agent-driven fraud represents another major challenge. Mobile money agents, who are integral to facilitating transactions and ensuring financial inclusion, can also serve as conduits for fraudulent activities. Instances of collusion between agents and malicious actors have been reported, compromising transaction integrity and eroding trust in the platforms [12]. Approximately 22.3% of respondents acknowledged agent-driven fraud as a substantial security concern (MDPI). Compounding these threats is the issue of inadequate regulatory frameworks. The absence of comprehensive, enforceable policies governing mobile money operations allows cybercriminals to exploit gaps in oversight, enabling activities such as money laundering, terrorist financing, and other illicit financial operations (tracecore.solutions) [13]. Together, these challenges underscore the need for a multifaceted approach to cybersecurity in mobile money systems, combining user education, agent monitoring, and strengthened regulatory mechanisms to safeguard financial transactions and maintain public confidence in digital financial services [14].

Proposed Solutions and Mitigation Strategies

Addressing the growing threats to mobile money security requires a multifaceted approach that integrates technological, educational, and regulatory measures. One of the most effective strategies is the implementation of enhanced authentication mechanisms. Multi-factor authentication (MFA), which combines multiple layers of user verification, has proven to substantially reduce unauthorized access to mobile money accounts [15]. Specifically, a hybrid authentication framework that integrates SIM verification, personal identification number (PIN) entry, and session token binding offers a robust and resource-efficient solution for environments with limited computational capacity. Such frameworks not only strengthen security but also maintain usability, ensuring that legitimate users can access their accounts without unnecessary complexity. Complementing technological solutions, user education and awareness are critical in mitigating security risks associated with human error [16]. Many breaches occur due to social engineering attacks, phishing schemes, or the sharing of sensitive information such as PINs. Comprehensive user education campaigns that inform customers about these risks and promote safe practices, such as avoiding sharing PINs, recognizing suspicious messages, and regularly updating passwords, can significantly enhance the overall security posture of mobile money systems [17]. In parallel, strengthening regulatory policies is essential to create an accountable and secure mobile financial ecosystem. Governments and regulatory authorities must develop and enforce legal frameworks that define clear responsibilities for service providers, establish penalties for negligence or fraudulent activity, and provide mechanisms for reporting and addressing security incidents. Such regulations not only act as a deterrent for cybercriminals but also promote trust among users, which is critical for the adoption and sustainability of mobile money services. Collectively, integrating robust authentication technologies, continuous user education, and strong regulatory oversight provides a comprehensive strategy to mitigate security risks and ensure a safer mobile money environment for both service providers and end-users [18].

CONCLUSION

In conclusion, mobile money platforms have transformed the financial landscape in East Africa by promoting financial inclusion, facilitating economic activities, and bridging the gap between formal banking and underserved populations. However, the rapid adoption of these platforms has exposed users and service providers to significant cybersecurity risks, including social engineering attacks, agent-driven fraud, and gaps in regulatory oversight. Addressing these challenges requires a holistic and multi-pronged approach. Technological solutions, such as multi-factor authentication and hybrid verification frameworks, can reduce unauthorized access and protect sensitive user data. Equally important is sustained user education to enhance awareness of cyber threats and promote safe digital practices. Furthermore, robust and enforceable regulatory frameworks are essential to deter cybercrime, ensure accountability, and foster trust within the mobile financial ecosystem. By integrating these strategies, stakeholders, including telecom operators, financial institutions, regulators, and users, can strengthen the resilience of mobile money systems. Ongoing research, regional collaboration, and adaptive security measures will be critical in safeguarding digital financial services and ensuring their sustainable growth across East Africa.

REFERENCES

1. Tiony, O.K., Yin, Y.: Financial Technology and Its Role in Promoting Financial Inclusion and Economic Growth in Kenya. American Journal of Industrial and Business Management. 14, 943 (2024). https://doi.org/10.4236/ajibm.2024.147049
2. Wachira, G., Njuguna, A.: Enhancing Growth and Productivity Through Mobile Money Financial Technology Services: The Case of M-Pesa in Kenya. International Journal of Economics and Finance. 15, p91 (2023). https://doi.org/10.5539/ijef.v15n12p91
3. Ali, G., Ally Dida, M., Elikana Sam, A.: Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda. Information. 11, 309 (2020). https://doi.org/10.3390/info11060309
4. Mohammed, U., Yakubu, I.N.: The Mobile Money Revolution: Transforming Payments and Financial Access in Africa. Presented at the October 1 (2025)
5. Alawida, M., Omolara, A.E., Abiodun, O.I., Al-Rajab, M.: A deeper look into cybersecurity issues in the wake of Covid-19: A survey. J King Saud Univ Comput Inf Sci. 34, 8176–8206 (2022). https://doi.org/10.1016/j.jksuci.2022.08.003
6. Kyomuhendo, M., Mutebi, J., Venkatachalam, M., Sewanyina, M.: Assessing Mobile Money Security Threats and User Satisfaction in Bushenyi District, Uganda | Asian Journal of Advanced Research and Reports.

7.Africa, F.: Mobile Money Drives Surge in Financial Inclusion, https://fintechnews.africa/45748/fintechafrica/mobile-money-drives-surge-in-financial-inclusion/

8.Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., Hur, J.: Cybersecurity threats in FinTech: A systematic review. Expert Systems with Applications. 241, 122697 (2024). https://doi.org/10.1016/j.eswa.2023.122697

9.9Osabutey, E.L.C., Jackson, T.: Mobile money and financial inclusion in Africa: Emerging themes, challenges and policy implications. Technological Forecasting and Social Change. 202, 123339 (2024). https://doi.org/10.1016/j.techfore.2024.123339

10. Clara Mramba, NNN Nditi (2018). Legal regulation of mobile money transfer service in Tanzania. *The Eastern African Law Review, 42, (2), 90-103.*

11. Ali, G., Mijwil, M., Buruga, B., Abotaleb, M.: A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech. Iraqi Journal for Computer Science and Mathematics. 5, (2024). https://doi.org/10.52866/ijcsm.2024.05.03.004

12. Fund, I.M., Peace, C.E. for I., Bank, W., Forum, the W.E.: Financial Inclusion and Cybersecurity in the Digital Age, https://www.imf.org/en/News/Articles/2020/12/10/sp121020-financial-inclusion-and-cybersecurity-in-the-digital-age

13. Botchey, F.E., Qin, Z., Hughes-Lartey, K.: Mobile Money Fraud Prediction—A Cross-Case Analysis on the Efficiency of Support Vector Machines, Gradient Boosted Decision Trees, and Naïve Bayes Algorithms. Information. 11, 383 (2020). https://doi.org/10.3390/info11080383

14. Echegu D. A., Aleke J. U., Alum B. N. Mobile Money Adoption in Uganda. 2024: 9(2) 10-16. IDOSR JOURNAL OF COMPUTER AND APPLIED SCIENCES https://doi.org/10.59298/JCAS/2024/92.1016

15. Hasan, S.S.U., Ghani, A., Daud, A., Akbar, H., Khan, M.F.: A Review on Secure Authentication Mechanisms for Mobile Security. Sensors. 25, 700 (2025). https://doi.org/10.3390/s25030700

16. Padma, B., Bukya, M., Ujjwal, U.: An Intelligent Hybrid Framework for Threat Pre-Identification and Secure Key Distribution in Zigbee-Enabled IoT Networks Using RBF and Blockchain. Applied System Innovation. 8, 76 (2025). https://doi.org/10.3390/asi8030076

17. Salzano, F., Marchesi, L., Pareschi, R., Tonelli, R.: Integrating blockchain technology within an information ecosystem. Blockchain: Research and Applications. 5, 100225 (2024). https://doi.org/10.1016/j.bcra.2024.100225

18. Baganzi, R., Lau, A.K.W.: Examining Trust and Risk in Mobile Money Acceptance in Uganda. Sustainability. 9, 2233 (2017). https://doi.org/10.3390/su9122233

CITE AS: Arionget Jemima (2026). Cybersecurity Challenges and Solutions for Mobile Money Platforms in East Africa. IAA Journal of Scientific Research 13(1):28-31. https://doi.org/10.59298/IAAJSR/2026/1312831