

The Role of Artificial Intelligence and Blockchain in Enhancing Cybersecurity and Fraud Prevention in African Digital Banking Systems

Ashibi, Denis Ekpan¹ and Adeboje, Fehintoluwa Oladayo¹

¹Adeyemi Federal University of Education, Ondo, Nigeria
ekpanis68@gmail.com, bolajifehintoluwa@gmail.com

Abstract

The rapid growth of digital banking across Africa has significantly improved financial inclusion. However, it has also exposed the sector to escalating cybersecurity threats and sophisticated fraud. This study examines how Artificial Intelligence (AI) and Blockchain technology can be integrated to strengthen cybersecurity and prevent fraud in African digital financial systems. It evaluates current fraud patterns, existing cybersecurity frameworks, and the potential of AI-driven anomaly detection systems alongside blockchain's immutable ledger and smart contract capabilities. Preliminary findings suggest that AI excels at real-time fraud detection through machine learning algorithms, while blockchain provides transparent, tamper-proof transaction records that significantly reduce identity theft, money laundering, and unauthorized access. The study further identifies key challenges to adoption in the African context, including infrastructure gaps, regulatory uncertainty, high implementation costs, and limited technical skills. This research proposes a hybrid AI-Blockchain framework tailored for African digital banking environments. The framework offers practical recommendations for financial institutions and regulators to build more resilient, secure, and trustworthy digital financial systems. The study contributes to the discourse on technological innovation for financial sector resilience and provides actionable insights for achieving sustainable economic transformation in Africa.

Keywords: Artificial Intelligence, Blockchain, Cybersecurity, Fraud Prevention, Digital Banking, Financial Inclusion, Africa

INTRODUCTION

Digital banking has transformed financial service delivery in Africa, offering greater convenience and broadening access for underserved populations. According to the Global Findex Database, account ownership in sub-Saharan Africa increased substantially, rising from 34% in 2014 to 58% in 2024, with mobile money playing a central role (World Bank, 2025). The GSMA (2026) further reports that mobile money in sub-Saharan Africa processed over \$1.4 trillion in transactions in 2025, underscoring the sector's rapid growth and contribution to financial inclusion.

Despite these gains, the expansion of digital banking has been accompanied by rising cybersecurity challenges. African financial institutions frequently report cyberattacks, with phishing, social engineering, ransomware, and emerging AI-powered deepfakes among the dominant threats (Serianu, 2025; INTERPOL, 2025; BusinessDay, 2026). These incidents result in significant financial losses and risk eroding customer trust, potentially undermining the progress made in financial inclusion.

Artificial Intelligence and Blockchain technology have emerged as promising complementary solutions. AI excels in processing large volumes of data to detect anomalies and predict threats in real time, while Blockchain provides transparency, immutability, and decentralized security (Simon et al., 2026; Pramudito, 2025). This paper examines the roles of these technologies, analyses adoption challenges in the African context, and proposes a tailored hybrid framework grounded in recent empirical studies.

CONCEPTUAL REVIEW

Artificial Intelligence refers to systems capable of performing tasks that typically require human intelligence, such as learning from data, recognizing patterns, and making predictions. In digital banking, machine learning and deep learning models are widely applied to analyse transaction patterns, user behaviour, and contextual factors for fraud detection (Matheri, 2024; Jejenywa, 2025).

Blockchain is a distributed ledger technology that records transactions across multiple nodes in a secure, chronological, and tamper-resistant manner. Its core features — decentralization, cryptographic security, immutability, and smart contracts — make it particularly valuable for financial applications where trust and transparency are essential (Simon et al., 2026; Gitobu, 2024).

Cybersecurity involves protecting digital systems, networks, and data from unauthorized access and attacks. Fraud prevention focuses on detecting and mitigating illicit financial activities. In Africa's predominantly mobile-driven digital banking environment, these areas intersect with challenges such as limited infrastructure and evolving threat tactics (INTERPOL, 2025; Serianu, 2025).

THE GROWTH OF DIGITAL BANKING IN AFRICA

Africa's digital banking sector has experienced remarkable expansion, driven by increasing smartphone penetration, fintech innovation, supportive government policies, and the lasting effects of the COVID-19 pandemic. Sub-Saharan Africa continues to lead global mobile money growth, with substantial increases in registered accounts and transaction volumes (GSMA, 2026; World Bank, 2025). This growth has significantly improved financial inclusion, particularly for rural and previously unbanked populations. However, security infrastructure has not always developed at the same pace as innovation, creating vulnerabilities that cybercriminals actively exploit (Serianu, 2025).

CYBERSECURITY THREATS IN AFRICAN DIGITAL BANKING SYSTEMS

African digital banking systems face a diverse and evolving threat landscape. Phishing and social engineering attacks remain prevalent, increasingly augmented by AI tools such as deepfakes

(BusinessDay, 2026; Smile ID, 2026). Other common threats include identity theft, SIM swapping, malware, ransomware, insider threats, and data breaches (INTERPOL, 2025; Serianu, 2025). Reports indicate that financial services consistently rank among the most targeted sectors, with substantial financial losses recorded across countries like Nigeria, Kenya, and South Africa (Serianu, 2025). These threats not only impose direct economic costs but also risk reversing gains in public confidence and financial inclusion.

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY AND FRAUD PREVENTION

AI has shown considerable promise in enhancing fraud detection capabilities. Machine learning models can analyse real-time transaction data, user behaviour (including location, device usage, and spending patterns), and other indicators to identify suspicious activities with improved accuracy and reduced false positives (Matheri, 2024; Jejenywa, 2025). Behavioural analytics and predictive intelligence further support proactive threat mitigation, while AI-powered biometrics strengthen customer authentication processes.

Several African banks and fintechs have begun deploying these systems, reporting positive outcomes in fraud reduction (Gitobu, 2024). Nevertheless, challenges such as data quality, potential model bias, and the need for explainable AI must be carefully addressed to ensure responsible implementation (Matheri, 2024).

THE ROLE OF BLOCKCHAIN TECHNOLOGY IN CYBERSECURITY AND FRAUD PREVENTION

Blockchain contributes to security through its immutable transaction records and decentralized architecture, which significantly reduce opportunities for tampering and single points of failure. Smart contracts enable automated, rule-based transaction validation, while transparent ledgers facilitate better compliance with anti-money laundering and regulatory requirements (Simon et al., 2026; Pramudito, 2025).

In African contexts, Blockchain applications have shown potential in secure remittances, digital identity management, and audit trails, although issues related to scalability and integration with existing systems require ongoing attention (Gitobu, 2024).

INTEGRATION OF AI AND BLOCKCHAIN

The integration of AI and Blockchain creates a powerful synergy, combining AI's analytical and predictive strengths with Blockchain's data integrity and transparency. Hybrid systems allow real-time fraud detection on tamper-proof ledgers, automated responses through smart contracts, and enhanced privacy-preserving mechanisms (Simon et al., 2026; Pramudito, 2025).

Experimental work in Nigeria, for instance, has validated hybrid frameworks that deliver strong performance metrics, suggesting suitability for high-volume mobile banking environments common across the continent (Simon et al., 2026).

CHALLENGES AFFECTING ADOPTION IN AFRICA

Despite the demonstrated potential, several barriers hinder widespread adoption. These include inadequate digital infrastructure (such as unreliable power and broadband), high implementation costs, acute shortages of skilled AI and Blockchain professionals, regulatory uncertainty, data privacy concerns, and varying levels of digital literacy (Gitobu, 2024; Simon et al., 2026). Overcoming these challenges demands coordinated efforts among governments, financial institutions, regulators, and technology providers.

PROPOSED HYBRID AI-BLOCKCHAIN FRAMEWORK

This study proposes a modular hybrid AI-Blockchain framework tailored for African digital banking contexts. The framework consists of interconnected layers:

An AI-Driven Fraud Detection Layer that employs ensemble models (such as XGBoost, LSTM networks, and anomaly detection algorithms) for real-time monitoring and behavioural profiling (Jejenewa, 2025; Simon et al., 2026).

A Blockchain Transaction Layer responsible for immutable recording and verification of transactions.

A Biometric and Secure Identity Layer combining AI-enhanced biometrics with decentralized identities.

Smart Contract Mechanisms for automated validation, compliance checks, and conditional executions.

A Regulatory Compliance and Monitoring Layer to facilitate oversight, reporting, and auditability. The framework emphasises edge computing for low-resource settings, phased pilot implementations, and continuous model retraining. It builds upon validated Nigerian architectures while remaining adaptable to other African countries (Simon et al., 2026).

IMPLICATIONS FOR FINANCIAL INSTITUTIONS AND POLICYMAKERS

Financial institutions are encouraged to invest strategically in hybrid technologies, prioritise staff training and capacity building, collaborate with fintech companies, and implement ongoing customer education on digital security. Policymakers and regulators can support adoption by developing clear, harmonised legal frameworks, promoting regional cooperation, investing in digital infrastructure and skills development, and fostering public-private partnerships (Gitobu, 2024; Matheri, 2024).

CONCLUSION

The continued digitization of banking in Africa presents significant opportunities for financial inclusion and economic development, but it must be supported by robust security measures. Artificial Intelligence and Blockchain technologies, particularly when integrated, offer powerful tools to address current vulnerabilities and build resilient systems. The proposed hybrid framework provides a practical, context-specific pathway forward. Success will depend on sustained collaboration, strategic investment, and adaptive policy responses. Future research should include large-scale empirical evaluations across multiple countries, detailed cost-benefit analyses, and investigations into emerging threats such as advanced AI-driven attacks and quantum computing risks.

REFERENCES

- Adebayo, T., & Mensah, K. (2024). Artificial intelligence applications in fraud detection within African banking systems. *Journal of African Financial Technology*, 12(2), 45–61.
- Gitobu, C. (2024). Harnessing Artificial Intelligence (AI) and Blockchain technology in African FinTech. *Journal of Information Systems*.
- GSMA. (2026). State of the Industry Report on Mobile Money 2026.
- INTERPOL. (2025). Africa Cyberthreat Assessment Report 2025.
- Jejenywa, T. O. (2025). Leveraging hybrid AI for real-time fraud detection: A case study on Nigerian FinTechs. *Digital Security and Forensics Journal*.
- Matheri, J. (2024). The effect of emerging digital security solutions on fraud risk management in Kenya's banking sector. Strathmore University.
- Pramudito, D. (2025). Exploring Blockchain and AI in digital banking. *Sistemasi Journal*.
- Serianu. (2025). Africa Cybersecurity Report – Kenya 2024/2025.
- Simon, B., et al. (2026). Development of an Artificial Intelligence and Blockchain-Based Cyber-Security Framework for Combating Financial Fraud in Nigeria's Digital Banking Ecosystem. *International Journal of Research and Scientific Innovation*, 13(3), 1086-1095.
- World Bank. (2025). The Global Findex Database 2025.

ICFB-UCB-2026-029