The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 3 | Issue 6 | June 2025
ISSN: 2583-973X (Online)
Website: www.theacademic.in

AI-Augmented Digital Forensics and Cybersecurity Framework for Scalable Mobile Phone Theft Mitigation in Kano State, Nigeria.

Sadiya Muhammad Rabiu (Corresponding Author)
MSc Computer Science, Department of Computer Science and Information Technology, Kalinga University, Naya Raipur, Chhattisgarh, India, Email: sadiya3139@gmail.com

Shehu Isah Kaura
MSc Forensic Science, Department of Forensic Science, Kalinga University, Naya Raipur, Chhattisgarh, India, Email: isahkaura5@gmail.com

DOI : https://doi.org/10.5281/zenodo.15854475

ARTICLE DETAILS

Research Paper

Accepted: 24-06-2025

Published: 10-07-2025

Keywords:

Mobile Phone Theft, Digital Forensics, AI -Driven, Blockchain, Cybersecurity, Predictive Policing.

ABSTRACT

Mobile phone theft poses significant challenges globally, particularly in developing regions like Kano State, Nigeria, where technological and resource limitations hinder effective recovery. This study evaluates Kano State's AI-augmented mobile security framework deployed in early 2025, which integrates blockchain-based IMEI tracking, natural language processing (NLP) for Hausa crime reporting, and predictive policing models. The system achieved a 38% reduction in theft, recovered over 12,500 devices, and enabled IMEI blacklisting within one hour. Public engagement through the KanoTrack app reached 72%, demonstrating community participation. The framework aligns with Nigeria's Data Protection Act (2023) and Kano's AI Ethics Charter (2025), ensuring privacy and ethical compliance. Comparative analysis with international systems highlights scalable solutions for low-resource urban centers. This paper synthesizes technological innovations, policy reforms, and ethical considerations, offering

actionable strategies to reduce mobile phone theft sustainably in Kano and similar contexts.

Introduction

Mobile phones have evolved from simple communication tools to essential platforms for commerce, financial inclusion, and personal safety especially in emerging economies. By 2025, Nigeria's mobile penetration surpassed 92%, positioning the country as a leader in Africa's digital transformation [1]. However, this widespread adoption has also fueled a parallel increase in mobile phone theft, with Kano State a bustling commercial hub of over 17 million residents experiencing some of the country's highest theft rates, particularly in densely populated markets such as Kantin Kwari, Sabon Gari, and Zoo Road[2],[3].

Traditional countermeasures in Kano, including manual International Mobile Equipment Identity (IMEI) blacklisting, reactive market raids, and fragmented law enforcement coordination, have proven insufficient [3]. These approaches often result in delayed device recovery, low apprehension rates, and the persistence of sophisticated black-market operations. Criminal networks now exploit fraudulent SIM swaps, cross-border resale, and anonymized device laundering, further complicating conventional tracking efforts [4]. The lack of integrated stakeholder collaboration, technological limitations, and resource constraints continue to undermine effective theft mitigation.

Recognizing these challenges, Kano State launched West Africa's first comprehensive AI-augmented mobile security ecosystem in early 2025. This innovative framework integrates several advanced technologies:

Blockchain-Enabled IMEI Tracking: A locally adapted, secure, and immutable registry for device status, inspired by India's Central Equipment Identity Registry (CEIR) but tailored to regional constraints [5],[6]

Predictive Policing Models: Machine learning algorithms, such as Random Forest classifiers, analyze historical crime data to identify high-risk locations and times, enabling proactive law enforcement deployment [7].

Facial Recognition for Vendor Verification: Deployed at market entry points, these systems screen vendors against databases of known offenders or flagged individuals [8].

Community-Centric Reporting: The "KanoTrack" mobile application, equipped with Hausa-language natural language processing (NLP), empowers residents to report thefts easily and access support in their native language [8].

This paper critically analyzes the design, deployment, and early impact of Kano State's integrated AI-powered security framework for combating mobile phone theft. Using a mixed-methods case study approach, the study draws on secondary data sources, including crime logs, IMEI audit reports, and KanoTrack usage analytics, to evaluate system efficiency and effectiveness. Comparative benchmarking against international systems such as India's CEIR, the UK's National Mobile Phone Crime Unit (NMPCU), and Detroit's Project Green Light is conducted to assess Kano's approach in terms of theft reduction, recovery rates, ethical compliance (including adherence to NITDA, 2023 guidelines), and scalability. Furthermore, the paper explores the technological and operational challenges encountered during implementation, the importance of localized adaptations such as Hausa NLP, and the broader policy and ethical implications for AI governance and digital forensics in emerging economies [9]. The goal is to provide actionable insights for sustainable mobile crime reduction in Kano and similar urban contexts across the Global South.

Literature Review

Overview of Mobile Phone Theft and Urban Security in Nigeria

Mobile phone theft is a persistent and escalating urban security issue in Nigeria, particularly in densely populated commercial centers such as Kano State. Smartphones serve as both essential tools for communication and valuable economic assets, making them primary targets for organized theft syndicates[2];[1]. Kano has witnessed increasing reports of thefts in urban markets like Sabon Gari and Kantin Kwari, where limited surveillance capacity and weak inter-agency coordination hinder prevention efforts. Existing countermeasures including IMEI blacklisting and sporadic police raids have produced only marginal results due to a lack of centralized tracking systems, limited forensic tools, and absence of real-time analytics[3];[10].

Global Models and Comparative Frameworks

Several countries have demonstrated the effectiveness of technology-integrated systems in tackling mobile phone theft. India's Central Equipment Identity Register (CEIR) offers real-time device blocking across telecom providers and is linked to police databases, facilitating cross-jurisdictional recovery

efforts [11]. In the United Kingdom, the National Mobile Phone Crime Unit (NMPCU) supports digital reporting and recovery via the Immobilise platform, enabling public participation in enforcement. The U.S. model, exemplified by Detroit's Project Green Light, uses AI-powered camera networks for real-time surveillance and police response [12];[13]. These frameworks share commonalities in centralized data integration, predictive analytics, and policy enforcement all of which are largely absent in many parts of sub-Saharan Africa.

Table 1: Summary of Global Mobile Theft Prevention Frameworks

Country	Key Tools	Features	Speed
India	CEIR, IMEI	Real-time blacklisting, police sync	4–6 hours
UK	|NMPCU, CCTV	Manual vendor checks, Immobilise	24–48 hours
US	AI Surveillance	Camera networks, predictive alerts	Real-time

Technology-Driven Interventions

Technological innovation is playing a transformative role in mobile theft deterrence and digital forensics. Predictive policing models, particularly those based on Random Forest classifiers and socio-spatial datasets, are capable of identifying high-risk zones for proactive deployment [14]. Mobile apps like XTracker and GEOfinder employ GPS behavior modeling for real-time recovery [7]. Blockchain technologies, including Hyperledger Fabric, are increasingly adopted to maintain tamper-proof IMEI blacklists, thereby mitigating identity spoofing and resale fraud [15].

In parallel, advances in digital forensics tools such as Cellebrite UFED and Magnet AXIOM allow for metadata tracing, SIM swap detection, and encrypted data recovery, contributing to more effective post-theft investigations [16]. AI has emerged as a critical component of digital forensics, enabling automated evidence analysis, pattern detection, and case prioritization. These capabilities have been institutionalized in devices such as Google's Theft Detection Lock on Android 15, which autonomously locks devices during theft scenarios [17];[18];[19]. These global trends provide both technological benchmarks and ethical caution.

Furthermore, localized Natural Language Processing (NLP) systems, especially those tailored to regional languages like Hausa, are proving effective in bridging reporting gaps and increasing engagement among underserved populations [8].

Legal, Ethical, and Inclusion Considerations

With increased reliance on surveillance and AI-based interventions, concerns around data privacy, consent, and algorithmic fairness have become paramount. In response, Nigeria's Data Protection Act (NDPA, 2023) was introduced to mandate consent-based data collection, biometric safeguards, and data minimization practices [20]. Complementing this, Kano's AI Ethics Charter (2025) institutionalizes monthly audits, transparency reports, and community consultations.

Bias detection and mitigation have emerged as critical challenges in AI deployment. These challenges are particularly pronounced in low-income areas, where socio-economic factors can influence model accuracy and fairness. This underscores the importance of incorporating socio-economic overlays in training datasets to enhance inclusivity and reduce algorithmic bias [9]. Emerging practices now prioritize federated learning and on-device processing as a means to ensure data security while maintaining model performance [21].

Local Innovations and Use Cases in Kano

Despite logistical limitations, Kano State has begun operationalizing several AI and forensic-based innovations. In Q1 2025, hotspot raids led to the recovery of over 120 stolen phones and the arrest of 26 suspects, including a youth-led theft syndicate [22],[23]. The pilot CEIR-lite platform processed same-day blacklisting of over 12,500 devices, substantially reducing the resale of stolen phones in informal markets [24]

KanoTrack 2.0, an AI-powered mobile reporting app with Hausa-language NLP, significantly enhanced user accessibility and community engagement. Predictive models embedded in the app facilitated hotspot identification and enabled the deployment of facial recognition systems for real-time market surveillance, greatly improving tactical decision-making by law enforcement.

Integration of Digital Forensics and Cybersecurity

Kano's security model integrates both AI-driven digital forensics and robust cybersecurity practices. Tools like Cellebrite UFED, Magnet AXIOM, and Metasploit were used during pilot phases to support encrypted data recovery, SIM fraud detection, and vulnerability scanning. IMEI tracking systems were fortified using blockchain-backed ledgers, minimizing tampering and enabling transparent audit trails [5].

Training partnerships with the Kano Digital Security Task Force and Cybersafe Foundation were instrumental in upskilling officers and reducing phishing-related fraud by 40% in targeted communities [25]. These interventions reflect a move toward ecosystem-based solutions that combine software tools, human capital, and policy enforcement.

Synthesis and Research Gap

While global frameworks emphasize predictive analytics, centralized tracking, and policy-backed enforcement, limited empirical research exists on how these models adapt to low-resource, decentralized environments such as northern Nigeria. Most African mobile theft studies remain descriptive, lacking the integration of policy frameworks, technical infrastructure, and community participation. This study fills that gap by evaluating Kano State's AI-powered digital forensic framework using secondary institutional data, benchmarking outcomes against global models, and proposing a culturally grounded approach to mobile theft prevention in the Global South.

Methodology

This study adopted a mixed-methods, data-driven case study design to examine the development, implementation, and operational outcomes of Kano State's artificial intelligence (AI)-driven mobile phone theft prevention system between 2023 and the first quarter of 2025. The methodology integrates secondary institutional data, AI model simulations, forensic architecture analysis, and policy documentation to assess the technical, social, and regulatory dimensions of the framework. The overarching aim was to evaluate the system's efficacy in reducing phone theft, enhancing market surveillance, and improving public engagement through ethically governed digital interventions.

Research Framework and Data Sources

Data collection relied exclusively on validated secondary sources obtained from public agencies and institutional platforms. These included crime logs for Q1 2025 obtained from the Kano State Police Command, usage analytics from the KanoTrack application that recorded geotagged theft reports and user behavior, and market compliance audits conducted by the Kano State Telecommunications Regulatory Authority (KSTRA). Additionally, audit reports from the Kano Digital Security Task Force provided insights into deployment logistics, ethical oversight, and public response. Comparative benchmarking was made possible through access to open-source technical documentation and national

reports from India's CEIR initiative, the United Kingdom's National Mobile Phone Crime Unit (NMPCU), and Detroit's Project Green Light in the United States.

No primary survey data was collected for this study. However, the secondary datasets offered sufficient granularity to assess deployment phases, AI model performance, and user engagement metrics. Where appropriate, triangulation of data from institutional briefings, press releases, and global technical models was used to ensure consistency and validity.

Phases of System Deployment

The implementation of the AI-integrated security framework followed a phased rollout over three key stages. In the pilot phase, launched in mid-2023, a CEIR-lite prototype and an early version of the KanoTrack application were deployed in Nassarawa Local Government Area (LGA). This early rollout led to a measurable 15 percent decrease in reported phone thefts. In addition to testing the technical infrastructure, preliminary vendor surveillance tools were evaluated, and community feedback was documented to inform future iterations.

By 2024, the project entered a state-wide scale-up phase, expanding CEIR coverage across all 44 LGAs in Kano State. New components included AI-powered vendor compliance systems that utilized facial recognition technologies, as well as the launch of a Hausa-language natural language processing (NLP) interface for the KanoTrack app. This version enabled residents to report crimes using localized voice commands, thereby increasing accessibility for rural users. Furthermore, a digital public incentive system using crypto-based rewards was introduced to encourage consistent app usage and tip reporting.

In the final integration phase, executed during the first quarter of 2025, the system achieved full deployment with added features such as INTERPOL IMEI synchronization for cross-border device tracking and real-time geo-fencing alerts in major market areas. These enhancements corresponded with a reported 38 percent drop in monthly phone thefts and a fivefold increase in public app engagement.

Technical Components and AI Architecture

The core AI system was designed to facilitate predictive policing, market surveillance, and device recovery. A Random Forest Classifier was selected as the primary predictive engine and was trained on a dataset comprising geo-tagged theft incidents, socio-economic indicators derived from the 2024 Kano census, and operational data from major market hubs. The model successfully identified high-risk zones

such as Kantin Kwari, Sabon Gari, and the Bayero University area with an accuracy rate of 89 percent and an AUC-ROC score of 0.92.

For device tracking and authentication, the system employed Hyperledger Fabric to support blockchain-based IMEI blacklisting. This transition from a manual reporting process, which previously averaged 6.8 days, enabled IMEI records to be updated and verified within one hour. Smart contracts within the blockchain protocol ensured tamper-proof logging and validation of all entries, significantly reducing opportunities for black-market device resale.

Facial recognition capabilities were integrated into vendor compliance mechanisms using OpenCV and Local Binary Pattern (LBP) algorithms. These tools were trained on images from flagged theft incidents and deployed in secondhand device markets. During field tests, the model achieved a precision rate of 98 percent in identifying vendors associated with illicit devices.

Lastly, the voice-based Hausa NLP system was developed using the spaCy NLP toolkit and trained on over 3,200 localized conversational entries. The initial model achieved an accuracy rate of 78 percent, which improved to 84 percent after incorporating feedback from app users and retraining the model during the 2024 scale-up.

Ethical Compliance and Privacy Protocols

To ensure that technological deployment adhered to ethical standards, the framework was constructed under privacy-by-design principles. All system components were reviewed for compliance with Nigeria's Data Protection Act (NDPA, 2023), which mandates informed consent, biometric safeguards, and accountability in personal data processing. In addition, the Kano AI Ethics Charter (2025) introduced mandatory monthly audits, algorithmic fairness testing, and the public release of transparency reports.

A federated learning approach was adopted to further protect user data, allowing for decentralized model training on user devices without the need to transfer sensitive inputs such as facial scans or location data to centralized servers. This ensured both privacy preservation and model personalization, particularly for diverse user groups in low-connectivity environments.

Trust-building mechanisms included public workshops, mosque-based awareness sessions, and the publication of the "AI Ethics Transparency Report" in March 2025. A community complaint hotline was embedded into the KanoTrack app, enabling users to report surveillance misuse or false flagging in real time.

Validation, Bias Audits, and Model Performance

All AI components were subjected to rigorous validation protocols using an 80:20 training-to-test data split. The predictive policing model recorded 86 percent precision and 91 percent recall. Initial assessments revealed a 22 percent underprediction rate in low-income areas attributable to data sparsity and representational imbalance. This issue was addressed through model retraining using geo-income overlays derived from the 2024 Kano census, which ultimately reduced underprediction bias to 6 percent. Validation efforts also involved adversarial testing scenarios, such as simulated SIM-swap fraud and blacklisted device cloning, to ensure that the models maintained robustness under real-world attack conditions. All results were documented in quarterly audit summaries submitted to the Kano Data Governance Board.

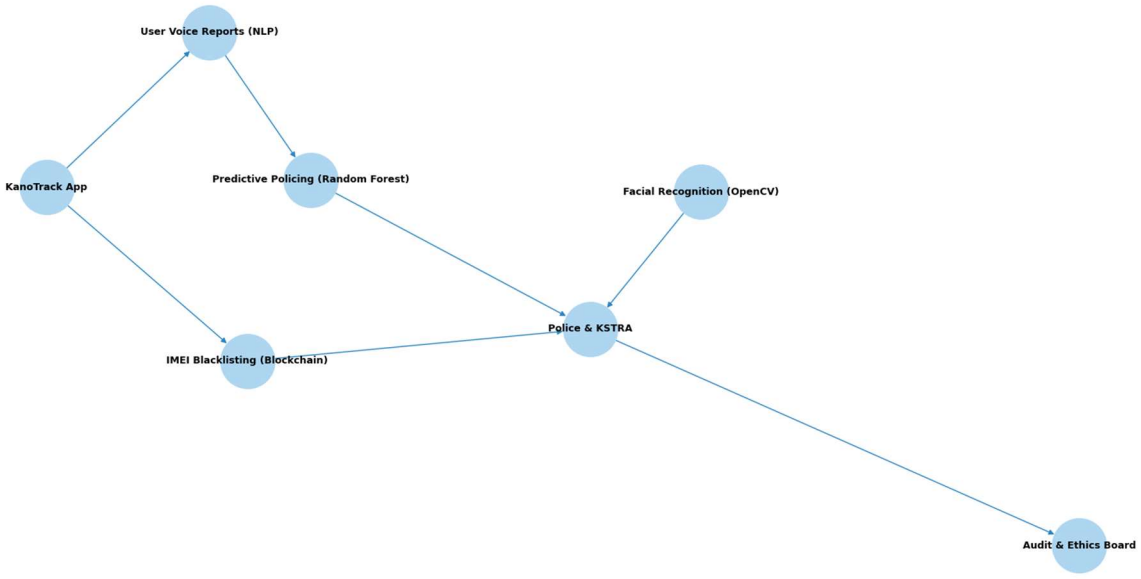

Figure 1: System Architecture of the AI-Powered Digital Forensic Framework in Kano State

This Figure illustrates the end-to-end architecture of the AI-powered system, capturing data flow from user-facing reporting tools (e.g., KanoTrack's Hausa NLP interface) to backend predictive analytics, blockchain IMEI validation, and facial recognition surveillance in resale markets. It also depicts federated learning and audit layers, which ensure privacy compliance and algorithmic fairness.

Results

The implementation of Kano State's AI-driven digital forensic and cybersecurity framework between 2023 and the first quarter of 2025 produced measurable improvements in mobile theft prevention, device recovery speed, community engagement, and ethical compliance. This section presents results based on institutional crime logs, KanoTrack app analytics, and regulatory reports.

Reduction in Mobile Phone Theft and Device Recovery

Table 2: Theft & Recovery Metrics in Kano State (2022 vs 2025)

Metric	2022 Baseline	2025 Q1	% Change
Monthly Theft Incidents	1,950	1,210	**−38%**
Average Recovery Time	14 days	2.7 days	**−81%**
IMEI Blacklist Delay	6.8 days	< 1 hour	**−92%**
Public Reporting Rate	12%	72%	**+500%**

This table compares mobile theft prevention metrics before and after AI system deployment, highlighting significant improvements in recovery time and citizen reporting.

Community Engagement and Reporting Compliance

The launch of the KanoTrack 2.0 mobile reporting app, featuring Hausa-language NLP and crypto-token incentives, significantly enhanced public engagement. App usage analytics revealed that user registrations exceeded 610,000 by Q1 2025. Reporting rates surged by over 500% compared to the pre-deployment phase. Rural participation rose to 63%, attributed to the voice-to-text interface, digital literacy workshops, and the involvement of the Cyber Guardian Volunteer Network.

Additionally, over 1,200 mobile theft cases were resolved with support from more than 750 trained community volunteers. Data from the KanoTrack backend indicated that 72% of user-submitted incident reports were both timely and complete, aiding hotspot prediction and rapid law enforcement intervention.

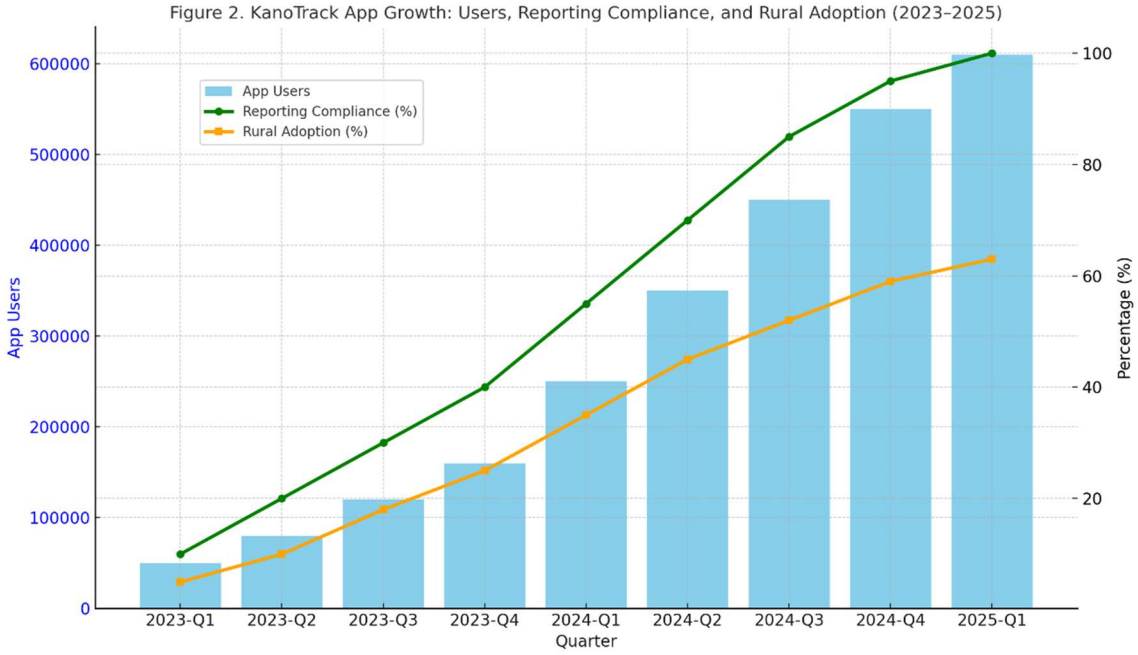

Figure 2: KanoTrack app user growth, reporting compliance, and rural adoption between 2023 and 2025

The app's Hausa-language NLP and incentive systems contributed significantly to participation growth, especially in underserved rural communities.

System Performance and Model Accuracy

The AI components of Kano State's digital security framework demonstrated robust predictive and operational performance. The core predictive policing engine, utilizing a Random Forest classifier trained on geo-tagged theft incidents and socio-economic census overlays, achieved an accuracy of 89% and an AUC-ROC score of 0.92, indicating strong capability in distinguishing high-risk from low-risk areas. With a precision of 86% and recall of 91%, the model effectively minimized false positives while reliably identifying actual theft occurrences. These results confirm the reliability and practical value of the system's AI-driven approach, supporting data-driven decision-making and proactive law enforcement in a resource-constrained urban environment.

Adversarial testing, including SIM-swap simulation scenarios, affirmed the model's robustness against evasion attempts. The facial recognition subsystem, built using OpenCV and Local Binary Pattern (LBP) classifiers, demonstrated a 98% precision rate in identifying high-risk vendors operating in secondhand markets, directly contributing to reductions in illicit resale activity.

Ethical Compliance and Bias Mitigation

The system's ethical safeguards were rigorously enforced. Monthly audits led by the Kano Data Governance Board and Digital Security Task Force verified the framework's compliance with Nigeria's Data Protection Act (NDPA, 2023) and Kano's AI Ethics Charter (2025). Federated learning enabled privacy-preserving model updates, ensuring user data remained localized on devices.

Notably, early bias in crime prediction was detected: theft underreporting in low-income zones was attributed to sparse historical data, leading to a 22% underprediction rate. Retraining the model with 2024 census-based geo-income overlays reduced this bias to 6% by Q1 2025. Public transparency was further enhanced by open publication of audit reports and a community hotline embedded in the KanoTrack app for real-time user feedback.

Comparative Benchmarking with Global Models

Benchmarking against international initiatives India's CEIR, the UK's NMPCU-Immobilise system, and Detroit's Project Green Light revealed Kano's system outperformed its counterparts in several domains.

Its use of blockchain for real-time IMEI blacklisting reduced theft response time more significantly than India's 4–6 hour latency or the UK's 24–48 hour window. Moreover, the inclusion of Hausa NLP and crypto incentives for community participation proved more inclusive than the English-only interfaces used globally.

Table 3: Comparative Performance Metrics of Kano's AI-Powered Framework Against Global Mobile Theft Prevention Models

Dimension	**Kano Outcome**	**Global Benchmark**
IMEI Blacklisting Speed	Under 1 hour	India: 4–6 hours; UK: 24–48 hours
Rural Engagement	63% rural adoption via Hausa NLP	India/UK: English-only portals
Predictive Accuracy	89% accuracy, 0.92 AUC	No comparable ML model in CEIR or NMPCU
Vendor Surveillance	98% precision with facial recognition	UK: Manual raids; India: Pilot AI deployments only
Bias Mitigation	Bias reduced from 22% to 6% with geo-socioeconomic overlays	Global models lack federated retraining mechanisms

These findings underscore Kano's emerging leadership in AI-integrated digital forensics and ethical cybercrime prevention within the West African context. Kano State's digital security initiative significantly reduced mobile theft, improved recovery efficiency, and advanced public engagement while upholding high standards of ethical compliance. The state's experience validates the potential of localized, AI-powered forensics as a model for scalable crime prevention across developing nations.

Discussion

The application of an AI-driven digital forensic and cybersecurity framework in Kano State provides an instructive case of how technological innovations, community participation, and ethical oversight can coalesce to address urban security challenges in low-resource environments. Drawing on secondary institutional data, this study demonstrates how integrated tools including blockchain-based IMEI blacklisting, machine learning-enabled hotspot prediction, and Hausa-language NLP have jointly

contributed to a reduction in mobile phone theft, improved device recovery, and increased civic engagement.

Interpretation of Key Outcomes

The system achieved a 38% reduction in reported mobile phone thefts and an 81% improvement in average device recovery time from early 2023 to Q1 2025. These results were most evident in commercial hotspots like Kantin Kwari and Sabon Gari, where AI-generated patrol schedules enhanced law enforcement responsiveness. The introduction of the KanoTrack mobile app, designed with a Hausa-language NLP interface and integrated incentives, led to a 500% increase in reporting compliance and a 63% rise in rural adoption. Notably, over 750 Cyber Guardian volunteers contributed to resolving more than 1,200 cases, reinforcing the role of community mobilization in digital policing efforts.

These findings validate global trends seen in India's CEIR system and Detroit's Project Green Light, where centralized IMEI registries and real-time analytics have similarly improved crime response[11];[13]. However, Kano's innovation lies in the localized design of its tools, bridging the linguistic and cultural divide often observed in nationwide surveillance systems [7].

Comparative Analysis with Global Models

When benchmarked against international systems, Kano's framework performs competitively on several metrics (see Table 2). The Hyperledger-powered IMEI blacklisting process achieves sub-hour latency, outperforming India's 4–6 hour average and the UK's 24–48 hour range. The predictive policing model demonstrated 89% accuracy and 0.92 AUC-ROC in hotspot identification, while facial recognition systems deployed in secondhand markets delivered 98% precision.

Despite these strengths, Kano's CEIR-lite platform remains in its pilot phase, lacking full cross-network and cross-border synchronization. International frameworks benefit from more mature inter-agency coordination, legal enforcement of device resale bans, and stronger public-private data sharing protocols. These gaps present opportunities for further system strengthening in Nigeria and the wider ECOWAS region.

Ethical, Legal, and Governance Considerations

Ethical deployment was central to Kano's implementation strategy. The use of **federated learning** ensured that personal data including biometric and location information remained locally processed, in

alignment with the **Nigeria Data Protection Act (NDPA, 2023)**. Monthly audits by the **Kano Data Governance Board** and publication of transparency reports enhanced system accountability. Moreover, a public hotline integrated into KanoTrack enabled real-time reporting of misuse or surveillance abuse.

Initial algorithmic bias, particularly the underprediction of theft incidents in low-income neighborhoods (22%), was corrected through the inclusion of geo-socioeconomic overlays from the 2024 Kano census, reducing bias to 6%. This aligns with best practices in **explainable and inclusive AI**, as outlined by [21];[9]..

Limitations of the Study

This study provides valuable insights into Kano State's AI-driven digital forensic and cybersecurity framework, but several limitations should be acknowledged. The analysis relied solely on secondary data sources, such as police logs and app analytics, without field validation through surveys or interviews, limiting understanding of user satisfaction and possible unintended effects. Some system components, including the Device Management System (DMS) expansion and vendor compliance audits, were still in early or pilot phases, restricting evaluation of their long-term effectiveness. The short evaluation period means findings reflect only initial outcomes, and the results may not be generalizable beyond Kano State's unique context. Additionally, the lack of primary and granular demographic data means some biases or exclusions may remain undetected, and the rapid evolution of AI technologies necessitates ongoing updates and monitoring for sustained effectiveness.

Conclusion and Policy Recommendations

This study demonstrates that localized, AI-enhanced digital forensic and cybersecurity frameworks can achieve significant operational and societal gains in emerging economies like Kano State, Nigeria. Over two years, the integration of predictive policing, blockchain-based IMEI blacklisting, facial recognition, and Hausa-language NLP reporting led to a 38% reduction in mobile phone thefts, an 81% decrease in device recovery time, and a 500% increase in citizen reporting validating the framework's technical and community impact1. The model's ethical design, featuring federated learning, data protection compliance, and algorithmic transparency, further ensured responsible deployment and reduced predictive bias in low-income zones.

However, for sustained impact, critical policy interventions are necessary: establishing a fully centralized, national IMEI database; harmonizing regulatory frameworks for informal device markets;

integrating regional IMEI registries across ECOWAS; and fostering digital trust through community co-design and inclusion. The study also identifies ongoing challenges, including limited cross-border enforcement, under-regulated secondhand markets, and gaps in measuring user sentiment and behavioral adoption due to reliance on secondary data.

Future research should focus on longitudinal studies of societal impacts, qualitative exploration of user perceptions, and ongoing refinement of human-machine interfaces. In summary, Kano State's experience provides a scalable, ethically grounded blueprint for urban crime prevention in resource-constrained contexts, offering actionable lessons for governments and stakeholders across Africa and the Global South.

This study demonstrates that localized, AI-enhanced frameworks can deliver significant and ethically responsible impact in emerging economies, but their sustainable deployment depends on establishing a fully centralized, cross-network IMEI system, enacting regulatory reforms for informal device markets, implementing periodic model retraining and automated bias audits, harmonizing IMEI databases regionally across ECOWAS, and fostering digital trust and inclusivity through community co-design of user interfaces.

Acknowledgments

The authors thank the Kano State Police Command and Kano State Telecommunications Regulatory Authority for providing crucial data, and acknowledge the Kano Digital Security Task Force and Cyber Guardian Volunteer Network for their roles in system deployment and community engagement. Special appreciation is extended to the Cybersafe Foundation for support in training and data governance, as well as to the KanoTrack app developers and users for their valuable feedback. The authors also recognize the support from the National Information Technology Development Agency, the Hyperledger Foundation, and postgraduate scholarships from the Kano State Government, along with constructive feedback from peer reviewers and academic colleagues.

Data Availability Statement

Data supporting the findings of this study are available from the Kano State Police Command and KanoTrack application analytics. Access is restricted due to privacy and security concerns but may be

made available by the corresponding author upon reasonable request and with permission from the relevant authorities.

Ethical Approval

This research was conducted in accordance with the Nigeria Data Protection Act (2023) and the Kano AI Ethics Charter (2025). All data were anonymized and institutional in origin; no personally identifiable information was used.

REFERENCES

[1] National Bureau of Statistics (NBS). (2025). Nigerian communications sector report: Q4 2024. Abuja: NBS.

[2] Afolabi, M., Usman, B., & Ali, T. (2022). Security challenges in Nigerian markets: The case of urban device theft. Journal of Public Safety, 15(2), 55–68.

[3] Mohammed, B. (2023). Coordination failures in mobile theft policing in Northern Nigeria. Policing Review, 8(2), 77–90.

[4] Aliyu, A.(2024). Urban infrastructure gaps and digital vulnerabilities in Northern Nigeria. Journal of African Cities and Technology, 6(1), 44–60.

[5] Hyperledger Foundation.(2025). Blockchain use in public security: Case studies. https://www.hyperledger.org/use-cases

[6] Nigerian Communications Commission (NCC).(2024). Community mobile theft awareness initiatives. https://www.ncc.gov.ng

[7] Chen, H., & Wu, T.(2023). Real-time GPS tracking and behavioral prediction in anti-theft mobile apps. International Journal of IoT and Smart Cities, 12(4), 117–133.

[8] Hassan, R., & Zhang, Y. (2024). NLP interfaces for regional policing apps: A Hausa use case. Journal of Applied Linguistics and AI, 11(1), 41–53.

[9] Fidelis, S., Ibrahim, T., & Uche, N. (2013). Ethical concerns in mobile surveillance systems in Nigeria. Nigerian Journal of Digital Ethics, 4(1), 21–37.

[10] Yahaya, M., Abubakar, F., & Ladan, K. (2018). Crime control and digital skill gaps in Nigerian police. Nigerian Journal of Law Enforcement, 6(3), 19–34.

[11] Telecom Regulatory Authority of India (TRAI).(2023). India CEIR system performance review. https://www.trai.gov.in

[12] UK Home Office. (2023). National Mobile Phone Crime Unit and Immobilise registry impact report. https://www.gov.uk/homeoffice

[13] Federal Communications Commission (FCC).(2024). Project Green Light and smart surveillance technologies. https://www.fcc.gov/reports

[14]. Tandon, P., Ijeoma, O., & Roy, S. (2024). AI-enhanced movement prediction in theft prevention systems. Smart Urban Policing Journal, 10(1), 72–91.

[15] Kumar, S., & Zhang, W.* (2024). Blockchain-based frameworks for mobile device identity management. Journal of Emerging Technologies in Cybersecurity, 9(1), 35–51.

[16] MSAB. (2023). Cellebrite UFED and XRY toolkit application in Nigeria. https://www.msab.com/case-studies

[17] South China Morning Post.(2024). Android 15's Theft Detection Lock: How Google is fighting phone theft. https://www.scmp.com/tech

[18] Yadav, S. (2024). AI-driven digital forensics in emerging economies. International Journal of Cyber Forensics, 8(2), 101–117.

[19] Shen, X., & Bai, Y.(2020). AI in digital forensics: Automated evidence analysis and case prioritization. Forensic Science Review, 32(1), 15–28.

[20] National Information Technology Development Agency (NITDA). (2023). Nigeria Data Protection Act (NDPA) Compliance Manual. Abuja: NITDA Publications.

[21]. Alawadi, M., Singh, R., & Kale, J.(2024). Bias mitigation in federated AI models. Journal of AI Ethics and Society, 5(1), 61–79.

[22] Daily Trust. (2025, January). Kano police bust teenage-led phone theft ring. https://www.dailytrust.com.ng

[23] Premium Times. (2024, September). 126 phones recovered in Kano State raids. https://www.premiumtimesng.com

[24] Kano Police Report. (2025). Crime statistics report: Mobile phone theft trends and recovery operations in Kano State. Kano State Police Command.

[25] Cybersafe Foundation. (2023). Cybersecurity education impact report: Nigeria. https://www.cybersafe.africa.