Digital Identity Systems and Security Administration in Nigeria: The Role of BVN and NIN in Combating Banditry and Kidnapping

Njoku Uchenna Gertrude; Ovuoh, Chukwuemeka Ronald, Esq

Political Science Department, Alvan Ikoku Federal University of Education, Owerri.

DOI: https://doi.org/10.51584/IJRIAS.2026.11060011

Received: 25 May 2026; Accepted: 30 May 2026; Published: 17 June 2026

ABSTRACT

Banditry and kidnappings are surging across Nigeria, exposing major gaps in the country's security system. These challenges have sparked fresh debates about how technology can help prevent crime. Recent steps like the Bank Verification Number (BVN) and National Identification Number (NIN) are building blocks for digital IDs that go way beyond banking or basic services. This study looks at how BVN and NIN could be used to fight banditry and kidnapping through effective security administration. It focuses on the balance between improving security and protecting people's rights. It uses Governance and Information Systems theories as the theoretical framework to navigate through this work, while descriptive approach and content analysis were used to x-ray the variables and concepts for this study. The paper analyzes how digital identity systems can support intelligence-led policing through identity traceability, financial intelligence, and communication monitoring. It also highlights key challenges, including data protection risks, digital exclusion, institutional fragmentation, and public trust deficits. Arguing that while BVN and NIN can help reduce criminal anonymity and disrupt illegal networks, they will only work if backed by strong legal protections, judicial oversight, and fair implementation. It concludes that digital identity systems must be built into a governance framework that respects human rights. That way, Nigeria can improve security without sacrificing civil liberties or democratic accountability.

Keywords: Digital Identity, Security Administration, Banditry, and Kidnapping

INTRODUCTION

Banditry and kidnapping have become pervasive security challenges in Nigeria, particularly in the North-West and Middle Belt regions. These crimes thrive on obscurity, fragmented identity records, and unregulated financial flows. Nigeria introduced digital identity systems like the National Identification Number (NIN) and Bank Verification Number (BVN) to strengthen internal security governance amid rising threats such as banditry and kidnapping. These systems aim to create a unified identity framework for tracking criminals and disrupting their financial operations.

Digital Identity Systems in Nigeria like Bank Verification Number (BVN) was introduced by the Central Bank of Nigeria in 2014, BVN assigns a unique identifier to individuals across all bank accounts. It enables cross-bank identity verification, transaction monitoring, and account freezing. National Identification Number (NIN) is managed by the National Identity Management Commission (NIMC). NIN serves as the foundational identity number linking citizens to civil registries, SIM registration, and government services. Together, BVN and NIN form the backbone of Nigeria's digital identity ecosystem. Adewole, Muna & Odumu (2022) argue that the BVN regulatory framework has strengthened Nigeria's banking system by improving customer verification, reducing fraud, and enhancing trust in financial transactions.

The BVN acts as a centralized biometric identifier for the banking sector, in the context of kidnapping, it is designed to identify the beneficiaries of ransom transfers. Freeze accounts associated with suspicious inflows, Prevent the use of "ghost accounts" for laundering criminal proceeds. In this regard, the NIN is the foundational identity. Under the "NIN-SIM Linkage" policy that was fully enforced by September 2024, no SIM card can function without a verified NIN. This serves two functions i.e every call made by a kidnapper is theoretically linked to a verified human identity. It enables security agencies to use cell tower data to pinpoint the origin of

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

ransom demands. Yusuf & Mohammad (2023) posit that digital ID systems act as foundational e-governance tools that enhance the ability of law enforcement to accurately attribute criminal acts to specific individuals. By linking NIN to SIM cards, the "anonymity of the caller" is theoretically removed. According to IFAC (2024), the BVN serves as a critical node in Anti-Money Laundering (AML) efforts. Scholars argue that the BVN helps "follow the money," making it difficult for kidnappers to move ransom payments through the formal banking system without detection. Matthew (2023) emphasizes that these databases are vital for tackling terrorism, cybercrime, and identity theft. He notes that robust data management systems, legal frameworks, and inter-agency collaboration are necessary to maximize their security potential. Without these, BVN and NIN remain underutilized in combating organized crime. Many scholars argue that while the technology is sound, the "Nigerian factor" such as corruption, poor infrastructure, and lack of political will neutralizes its benefits. Okwuwada (2023) highlights that the effectiveness of the NIN-SIM linkage is undermined by the illicit sale of pre-registered SIM cards. Criminals bypass the system by using IDs belonging to innocent citizens or compromised registration agents. Former Minister Ali Pantami and other observers (cited in HumAngle, 2025) have argued that the failure is not in the policy, but in the security agencies' inability to utilize the data. Scholars note that despite millions of linked SIMs, tracking still fails in rural "blind spots" where there is no cell coverage. This aligns with broader academic concerns about cybersecurity loopholes and weak enforcement in Nigeria's digital identity infrastructure. Moreso, BVN and NIN can only succeed if citizens trust the system. Trust, transparency, and accountability are repeatedly emphasized as prerequisites for compliance. Without them, citizens may resist registration or exploit loopholes. This reflects broader governance theory assumptions that identity systems are not just technical but socio-political instruments requiring legitimacy. In essence, BVN and NIN are indispensable for Nigeria's financial integrity and internal security governance, their effectiveness is limited by data breaches, poor enforcement, and lack of citizen trust. Strengthening cybersecurity, legal frameworks, and inter-agency collaboration is essential if BVN and NIN are to fulfill their promise in combating banditry and kidnapping.

Statement of the Problem

Nigeria is currently confronted with escalating insecurity, particularly banditry and kidnapping, which have become pervasive threats to national stability, economic growth, and human security. These crimes thrive on anonymity, fragmented identity records, and unregulated financial flows.

The Federal Government's policy mandating the linkage of NIN to Subscriber Identity Modules (SIM cards) was predicated on the logic that de-anonymizing communication and financial transactions would eliminate the "operational cover" used by bandits and kidnappers. However, a significant disconnect persists between identity enrollment and security enforcement.

Despite the aggressive implementation of the National Identification Number (NIN) and the Bank Verification Number (BVN) as pillars of Nigeria's digital identity architecture, internal security remains in a state of oscillation. Criminal syndicates have circumvented the NIN-SIM linkage through the use of "pre-registered" SIM cards, imitating technologies, and identities harvested from vulnerable rural populations, allowing them to coordinate attacks and demand ransoms with continued anonymity.

While the BVN was designed to monitor suspicious financial flows, kidnappers have adapted by demanding ransoms in physical cash effectively bypassing the formal banking sector's surveillance capabilities. Technical limitations in geolocating signals in Nigeria's vast forest reserves such as Sambisa and Kamuku, mean that even when a linked SIM is identified, physical interception remains a challenge.

Even though the government has created a vast biometric database, this so-called "digital net" has not been effective against bandit groups that are constantly on the move and quick to adapt. Without fixing the gaps in identity verification and building a system that allows security agencies to share intelligence seamlessly, the BVN and NIN databases function more as static administrative records than as practical tools for strengthening internal security.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Objective of the Study

The general purpose of this study is to examine the Role of BVN and NIN in combating banditry and Kidnapping in Nigeria. It will specifically:

1) Examine how BVN and NIN could be used to fight banditry and kidnapping.
2) Identify Structural and Technical Loopholes in the Digital Identity Framework
3) Recommend policy interventions and technical upgrades necessary to transform Nigeria's digital identity databases from mere administrative records into proactive instruments of national security.

Research questions

1) How could BVN and NIN be used to fight banditry and kidnapping.
2) What are Structural and Technical Loopholes in the Digital Identity Framework
3) What policy interventions and technical upgrades are necessary to transform Nigeria's digital identity databases from mere administrative records to proactive instruments of national security.

Theoretical Framework

The theory used for this study is Information Systems theory.

Information Systems (IS) Theory is not a single unified theory but a field of interrelated frameworks developed from the 1970s and beyond. The key contributors include Gordon B. Davis (1974), who helped establish the Information System as an academic discipline, and later scholars such as William H. DeLone and Ephraim R. McLean (1992 (Updated in 2003), Yogesh K. Dwivedi, Michael Wade, and Scott Schneberger (2012), who consolidated Information System theories into a comprehensive framework. The central assumption is that information systems are socio-technical systems, which comprises technology, people, and organizations that influence and are influenced by social and institutional contexts. They opined that technology alone does not determine outcomes.

Information System effectiveness depends on human, organizational, and technical alignment. Users play an active role in shaping system use, social and cultural context matters. They believe that information systems exist to support decision-making and performance. System success is not just about "having the technology." It is measured across six dimensions: System Quality, Information Quality, Service Quality, Use, User Satisfaction, and Net Benefits.

This study adopts the DeLone and McLean Information System Success Model to argue that the 'Net Benefits' of Nigeria's digital identity systems in combating kidnapping are currently hindered by poor 'Information Quality' (identity theft) and a lack of 'Facilitating Conditions' (infrastructure in rural areas) as suggested by Unified Theory of Acceptance and Use of Technology (UTAUT).

RESEARCH METHODOLOGY

This study adopts a descriptive research design to explore the intersection of digital identity systems and security administration in Nigeria, with particular emphasis on the effectiveness of the Bank Verification Number (BVN) and National Identification Number (NIN) in curbing banditry and kidnapping.

Employing qualitative content analysis as its principal method, the research systematically reviews academic literature, policy frameworks, and security reports. By integrating diverse theoretical perspectives with empirical evidence, the study seeks to fill critical gaps in the existing scholarship on digital forensics and national security in Nigeria.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Clarification of Key Concepts

Digital Identity

Digital identity could be seen as the collection of electronically stored attributes and credentials that serve to uniquely distinguish an individual within digital and administrative systems. Scholarly discourse on digital identity spans multiple dimensions, including technological innovation, governance frameworks, security imperatives, and rights-based considerations. Friedman and Wagoner (2025) define digital identity as a set of data that uniquely describes a person or thing and contains information about the subject's relationships to other entities. Masiero, & Bailar, (2021) view digital identity as a development tool. They argue that digital identity systems can promote justice and inclusion but also risk exclusion of marginalized groups if poorly implemented. This means that a development tool links identity to justice, inclusion, and human development. Cameron (2005), in his seminal "Laws of Identity", famously posits that digital identity is a set of assertions made by one digital subject about itself or another. He argues that because the Internet was built without an "identity layer," digital identity systems must now serve as that missing layer to ensure trust. Gelb & Clark (2013) explained that digital identity is a foundational governance infrastructure, especially in developing countries. They argued that digital identity enhances service delivery, improves accountability and reduces fraud and duplication. To them, digital identity strengthens state capacity and administrative efficiency.

David Birch (2022) provides a provocative scholarly view by suggesting a move away from solving "who someone is" (pre-digital identity) and focus instead on certified credentials. In his view, "Identity is an asset i.e. a certified claim about an attribute." This means the BVN/NIN should not just prove "This is Peter Jombo," but should provide a "certified claim" that "This person is a verified citizen with no criminal alerts," which can be instantly checked by security agencies. World Bank (2019) defines digital identity as "a system that enables individuals to prove who they are in a digital environment." The Bank emphasizes its role in Financial transparency, Social protection targeting Anti-corruption initiatives. This entails that secure and inclusive digital identity systems improve accountability and governance outcomes. Scholars broadly agree that digital identity is not merely a technical tool but a governance system with profound implications for accountability, security, inclusion, and civil liberties. Its impact depends on institutional design, legal safeguards, and public trust. Digital identity fits to BVN/NIN, because they align with the governance and accountability perspective.

Security Administration

Security administration refers to the structured management of protective measures, risks, and operations to safeguard assets, people, and systems.

In the contexts of public administration, it entails effective resource coordination, both human, material, and financial to minimize threats. Security is often defined in public administration through the lens of law enforcement and national stability. Post and Kingsbury (1991) describe security administration not merely as guarding property, but as the organized application of security functions (planning, policy, loss prevention, disaster planning) within business, industry, and government contexts. It is perceived by the Scholars of "Systemic Security Governance**" in** (2025)**,** as a three-tiered governance structure consisting of risk containment, factual clarification, and institutional consolidation within a rule-of-law framework. Contemporary scholars define it as a multi-disciplinary, strategic process that integrates technology, human behavior, and risk management. As contained in the Security Sector Governance (SSG), security administration is seen as the management and oversight of security providers (military, police, intelligence, private security). It stresses transparency, accountability, and efficiency in delivering security services to citizens. Fay (2023) defines security administration as the set of principal functions and responsibilities required for security professionals in supervisory positions. It is the art of integrating security operations i.e planning, organizing, and managing with the overall mission of the entity. Chandler (2020/2021) suggests that security administration in the 2020s has shifted toward "governance." It is no longer just about preventing threats but about administering a system's ability to "bounce back" from unavoidable disruptions in a complex, interconnected world. From the combined literature Security administration is the systematic process of planning, organizing, directing, and controlling security functions and resources within an organization or society to protect people, assets, and information from

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

threats, risks, and harm. It integrates policy development, risk assessment, implementation of controls, operational oversight, and continuous monitoring.

Security administration in Nigeria has leveraged BVN (Bank Verification Number) and NIN (National Identification Number) primarily through mandatory linkages to SIM cards and bank accounts to enhance tracking of criminals involved in banditry and kidnapping. These systems help by tightening identity management and reducing anonymity, which criminals often exploit.

Despite the administrative intent, It is believed that there are underutilization of these tools by security agencies. As contained in the Punch Newspaper of January, 16, 2024 the former Minister of Communications Isa Pantami also acknowledged that the NIN-SIM linkage policy has worked, but the challenge lies in security agencies not fully using the data for tracking and investigation. The Guardian news of January, 26, 2023 has it that Civil rights groups and commentators have expressed skepticism over claims that NIN and BVN have significantly reduced kidnapping or banditry, noting that while data collection is strong, actual arrests using these systems have been limited. Combating the rising tide of kidnapping and banditry in Nigeria requires a holistic security governance model. While military intervention remains necessary, scholars emphasize that national security is multifaceted, encompassing economic stability and social equity. Therefore, the deployment of digital identity systems like NIN and BVN must not be viewed merely as surveillance tools, but as part of a broader governance strategy to bridge the gap between state presence and marginalized communities, thereby mitigating the systemic poverty and exclusion that fuel internal insecurity.

Banditry

Banditry is a form of organized violent criminal activity carried out by non-state actors, often in areas of weak governance, involving robbery, kidnapping, cattle rustling, and attacks on communities for economic or political purposes**.** United Nations Office on Drugs and Crime (2022) (UNODC) broadly describes banditry as "Criminal acts involving armed robbery, violence, and illegal appropriation of property, often carried out by organized groups in areas with limited state presence." Osasona (2023) defines armed banditry in Nigeria's North-West as "the gravest security threat Nigeria currently faces, driving her worst humanitarian crisis in decades". He situates banditry within frameworks of organized crime and explores its overlap with international humanitarian law. Eric Hobsbawm, a classical scholar on banditry, defines it as "A form of social crime carried out by outlaws who are often supported by local communities and may be seen as heroes or rebels against oppressive systems." He introduced the concept of social banditry, where bandits are not merely criminals but may represent resistance against injustice. To Arnold Onyekachi David Okoro (2022) banditry as a violent crime involves "destruction of properties, wanton killings, rape, kidnapping, abduction, looting, waylaying and invasions, using sophisticated weapons". He emphasizes its impact on national security and categorizes it as both a crime and a crisis. In the Nigerian context, Abdullahi (2019) defines banditry as "A form of violent criminality involving armed groups engaging in cattle rustling, kidnapping, robbery, and attacks on rural communities."To him, it reflects the modern manifestation of banditry in Nigeria, particularly in the North-West region. Egwu (2016) sees banditry as "an illegal activity which involves the use of force or threat to intimidate and rob people of their property." He emphasizes that in Northern Nigeria, this has evolved from simple theft into a complex web of cattle rustling and rural terror. Many scholars in their different fields, categories and capacity have described banditry in several ways. However, all point at it as criminality against humanity as a result of weak governance, which undermines socio-economic, political and technological growth and overall development of the society.

Kidnapping

Kidnapping is the unlawful abduction, seizure, or detention of a person against their will, which is carried out through force, fraud, or coercion, often for purposes such as ransom, exploitation, or political and economic gain.

In the Nigerian and African context, most scholars see kidnapping as a form of organized criminal activity, often driven by ransom demands, economic benefits, and coercion. Their definitions reflect the contemporary reality where kidnapping is closely tied to insecurity and criminal networks. Onuoha (2014) defines kidnapping as "The forceful seizure and holding of individuals by criminal groups for economic gain, often involving ransom

demands and threats to life." He sees it as organized crime and economic motivation. Abdullahi, Fasoranti & Abrifor (2022) explained that kidnapping in Nigeria is linked to unemployment, poor governance, border insecurity, and illegal arms possession. They defined it as a criminal enterprise with severe consequences like loss of lives, property, investment, and disruption of education. Alemika (2013) defines kidnapping as "The illegal abduction and detention of a person for ransom, political bargaining, or other forms of coercion.". His definition reflects the ransom-driven and socio-political nature of kidnapping in Nigeria. Lyman & Potter (2011) define kidnapping as "The unlawful taking and carrying away of a person by force or fraud or the unlawful seizure and detention of a person against their will." This definition highlights force, deception, and unlawful detention as key elements.

Although BVN and NIN have not eradicated banditry and kidnapping, they have curbed criminals' operational freedom by limiting anonymity in financial and communication systems, the implementation of Nigeria's digital identity architecture, specifically the NIN-SIM linkage, presents a critical challenge to the protection of civil liberties. Scholars highlight a growing tension between traditional freedoms and modern security governance. For Nigeria to avoid the pitfalls of a 'surveillance state,' the integration of BVN and NIN data into internal security operations must be balanced with robust digital rights protections. This ensures that while the state pursues the legitimate goal of combating banditry, it does not simultaneously dismantle the systemic inequality or fundamental freedoms that anchor its democratic legitimacy.

In the analysis of this study, we consider it necessary to address the following research questions?

Research question One: How could BVN and NIN be used to fight banditry and kidnapping?

BVN (Bank Verification Number) and NIN (National Identification Number) can support the fight against banditry and kidnapping by improving identity-based tracking of suspects, their communication, and financial transactions. Dengiyefa Angalapu (2024) asserts that integrating these systems strengthens surveillance, disrupts criminal networks, and raises the perceived risk of getting caught.

Some scholars like Usman Ojedokun (2019) emphasize that kidnappers often use phones and banks to negotiate ransom and move money, so linking BVN and NIN to phone-SIM and bank-account data makes it harder for offenders to remain anonymous. When each line and each bank account is tied to a verified NIN/BVN, law-enforcement agencies can more quickly trace calls, locate suspects, and freeze or monitor ransom-related transactions.

Research Question Two: What are Structural and Technical Loopholes in the Digital Identity Framework?

With respect to Nigeria's internal security Administration, scholars argue that while the Bank Verification Number (BVN) and National Identification Number (NIN) are theoretically robust, they are undermined by systemic failures. These are categorized into Structural Loopholes (institutional, social, and policy-based) and Technical Loopholes (technological, infrastructural, and data-driven. Some challenges regarding to Structural loopholes are:

The "Identity Black Market" and Insider Corruption: The most significant loophole is the human element. Compromised enrollment agents illicitly sell pre-registered NINs or link multiple SIM cards to a single, legitimate NIN belonging to an unsuspecting citizen. This "identity laundering" allows bandits to maintain anonymity despite the linkage policy. (Okwuwada, 2023) and Mbam et al., 2024)

Weak Institutional Coordination: Digital identity systems often suffer from fragmented institutional arrangements, leading to poor data sharing and oversight gaps. This results in duplication of identity records, lack of compatibility between agencies and inefficient security response. The "siloed" nature of Nigerian databases, where the Central Bank (CBN) manages BVN and NIMC manages NIN creates a bureaucratic lag. Security agencies often lack real-time, "hot-link" access to these databases, meaning by the time a subpoena is processed to track a kidnapper's phone or bank account, the trail is cold. (Lyon, 2014, Adesina, 2023)

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

The "Cash-Out" Economy: Okoli and Ugwueze (2018) noted that the structural reliance on physical cash in rural Nigeria allows kidnappers to bypass the BVN entirely by demanding ransoms in untraceable banknotes, rendering the digital financial footprint irrelevant.

Poor Governance and Accountability: World Bank (2019) explained that Weak governance structures reduce trust and increase risks of corruption and data misuse.

Inadequate Legal and Regulatory Frameworks: Gus Hosein (2018) opined that many digital identity systems are deployed without robust legal safeguards, exposing citizens to misuse of personal data and this leads to Privacy violations, lack of accountability and weak enforcement of data protection laws.

Technical loopholes involve weaknesses in technology, infrastructure, and cybersecurity systems. These include but not limited to:

Data Breaches and Cybersecurity Vulnerabilities: Bruce Schneier (2015) argued that Centralized identity databases are prime targets for cyberattacks due to the concentration of sensitive personal data. Like Hacking of biometric databases, Identity theft and Unauthorized access among others.

Infrastructure Deficits (Blind Spots): Rufai (2021) and Abdullahi (2019) point out that many "banditry hotspots" in the North-West and North-Central are forest zones with zero telecommunication coverage. Technically, if a kidnapper makes a call using a satellite phone or moves into a "blind spot," the NIN-SIM triangulation fails because there are no local towers to provide geolocation data.

Data Integrity and Synchronization Errors: Amiara (2024) observes that millions of Nigerians have "un-synchronized" data where names or fingerprints on a BVN do not match the NIN. These technical discrepancies lead to "false negatives," where legitimate security flags are ignored because the system cannot verify the conflicting data points across platforms.

Biometric Bypassing and Spoofing: Yusuf and Mohammad (2023) highlights the technical vulnerability of biometric systems to "spoofing" or the use of 2D/3D replicas. They argued that the current system lacks "Liveness Detection" during every transaction, meaning a stolen identity can sometimes be used if the initial registration was fraudulent.

Research Question Three: What policy interventions and technical upgrades are necessary to transform Nigeria's digital identity databases from mere administrative records to proactive instruments of national security.

Digital identity systems such as Nigeria's National Identification Number (NIN) and Bank Verification Number (BVN) have evolved from administrative tools into critical infrastructures for governance and security. However, scholars argue that for these systems to function as proactive national security instruments, deliberate policy reforms and technological enhancements are required.

Stronger Legal Frameworks: It is believed by various scholars that data protection laws that criminalize BVN/NIN misuse and mandate strict penalties for identity fraud is necessary for proactive national security administration.

Intelligence-Led Identity Governance: Sami. Tunji mentioned in Punch Newspaper of September 16, 2025, asserts that traditional identity systems are administrative, but for security-driven identity governance, there should be embed identity databases into Law enforcement systems, Counter-terrorism frameworks, Financial intelligence units to reduce fraud and enhance national security.

Establishing a Unified National Security Data Hub: It has been argued that the current "siloed" nature of the NIN (NIMC) and BVN (CBN) is the greatest policy hurdle. Adesina (2023) and Yusuf and Mohammad (2023) propose a policy mandate for a Unified National Security Data Hub (UNSDH). This would move beyond mere linkage to creating a real-time, inter-agency platform where the Police, DSS, and Military can access identity data without the current 24 to 48 hour bureaucratic delay.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VI June 2026

Zero-Tolerance" Agent Accountability Policy: To stop the "identity black market," Amiara (2024) recommends a policy of strict criminal liability for enrollment agents. Believing that NIN or SIM registered through an agent and later found in the hands of a bandit should result in the immediate prosecution of the registering officer, thereby cleaning up the "insider threat" in the digital ID supply chain.

Public Awareness and Regulation of Data Sales: Shuaib S. Agaka mentioned in Blue Print Newspaper of July 30, 2025 stated that BVN/NIN being sold illegally show the need for public sensitization campaigns and stricter monitoring of digital identity brokers. Stressing that BVN, NIN sale, is a threat to national security.

Real-Time Data Analytics : It would be also helpful to use big data and machine learning to flag unusual financial transactions linked to ransom payments or bandit networks.

Blockchain-Enabled Data Integrity:

To prevent the tampering of records by corrupt officials, Adesina (2023) suggests a technical upgrade to a distributed ledger (Blockchain) architecture. This ensures that once a bandit's identity is flagged, the record is "immutable" and cannot be deleted or altered by a "mole" within the security or identity agencies.

Secure Interoperability: Building encrypted, interoperable databases that allow law enforcement to cross-check BVN and NIN records instantly without compromising privacy.

In essence, to transform Nigeria's digital identity systems from passive "administrative records" into "proactive instruments of national security there is need to pay attention to the above mentioned scholarly perspectives.

RECOMMENDATION

As have extensively discussed, to transform Nigeria's digital identity terrain from a passive database into a proactive security shield and administration, a multidimensional approach is required. These recommendations focus on closing the "structural" gaps in governance and the "technical" gaps in infrastructure. Hence we suggest that the Federal Government should mandate an encrypted, real-time Application Programming Interface (API), which will access tactical security units through the establishment of the National Security Data Integration Protocol. This would allow the Police or DSS to instantly verify the NIN/BVN of a suspect during an active kidnapping case without waiting for manual bureaucratic approvals. It is imperative to introduce Telecom Identity Risk Management Systems (TIRMS). This means implementing systems to monitor SIM recycling, detect fraudulent registrations, and flag unusual call/SMS activity linked to kidnappers. It would be of great importance to conduct Public Awareness Campaigns on Community and Public Engagement. In these campaigns Citizens should be educated on the importance of digital identity registration, Reporting suspicious activities, and Protecting personal identity information. Also, the government must ensure Rural and vulnerable populations are registered and have easy access to identity enrollment centers. This prevents criminals from exploiting unregistered populations. It has been observed that the "identity black market" is fueled by compromised registration agents. So there is a need to implement a strict "Chain of Custody" policy. If a SIM card used in a crime is traced to a NIN that was fraudulently registered, the agent who performed the registration should face mandatory criminal prosecution. This creates a powerful deterrent against "insider threats." The Ministry of Communications should deploy "Tactical Towers" and satellite-linked signal boosters in identified "blind spots" (e.g., Kamuku and Sambisa forests). These should be integrated with Geospatial Intelligence (GEOINT) to provide live triangulation of any NIN-linked device entering these zones.

If the outlined recommendations are well coordinated and implemented it will result in Reduced Anonymity, Financial Disruption, Public Confidence and Enhanced Intelligence.

CONCLUSION

This study has shown that the Nigerian state has successfully built a massive biometric database However, these systems remain largely "administrative records" rather than "proactive security instruments." Secondly, Nigeria's digital identity systems particularly the Bank Verification Number (BVN) and the National

Identification Number (NIN), when effectively managed through strong security administration, can significantly reduce banditry and kidnapping in Nigeria. By integrating databases, strengthening policies, deploying advanced technologies, and enhancing inter-agency collaboration, Nigeria can transform its identity infrastructure into a powerful tool for national security, crime prevention, and intelligence gathering.

REFERENCES

1. Abdullahi, H. I., Fasoranti, O. O., & Abrifor, C. A. (2022). "Felson and Cohens' routine activity theory and waves of kidnapping in Nigeria: A theoretical exploration of criminal enterprise". Journal of Social and Development Studies, 5(2), 34–50.
2. Adewole, C., Muna, C., & Odumu, V. (2022). "BVN Regulatory Framework and Banking System Stability in Nigeria". International Journal of Innovative Research in Social Sciences and Strategic Management Techniques.
3. Awofisayo Oladoja Abosede & Eseyin Olorunfemi Abraham (2022) Establishment of criminal/profile DNA database and use of forensic intelligence to combat nationwide insecurity issues in Nigeria. https://doi.org/10.4314/br.v20i2.2
4. Buzan, B. (1991). People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. Hemel Hempstead: Harvester Wheatsheaf.
5. Cameron, K. (2005). The Laws of Identity. Microsoft Corporation. Retrieved from identityblog.com. 30/12/2025
6. David, O. (2009). (cited in Akeem, .A. K. & Idowu, .M. O., 2020) International Journal of Social Science and Humanities Research. https://www.ijsshr.com/journal/index.php/IJSSHR/article/download/572/502
7. Egwu, S. (2016). The political economy of rural banditry in contemporary Nigeria. In M. J. Kuna & J. Ibrahim (Eds.), Rural banditry and social conflicts in Nigeria (pp. 12–46). Centre for Democracy and Development.
8. Fage, M. D., & Alabi, J. O. (2017). "Prevalence of kidnapping and its socio-economic implications". TSU Journal of Social Sciences and Research.https://oer.tsuniversity.edu.ng/index.php/tijossr/article/download/1471/1192/2945
9. Lyon, D. (2009). Identifying Citizens: ID Cards as Surveillance. Polity Press.
10. Lyman, M. D., & Potter, G. W. (2011). Organized crime (5th ed.). Pearson.
11. Matthew, B. (2023). "Leveraging NIN and BVN Databases to Address Nigeria's Security Challenges: An Analysis". ResearchGate.
12. Masiero, S. & Bailur, S. (2021). Digital identity for development: The quest for justice and a research agenda. Information Technology for Development.
13. Ochoga, E. & Mazdli, M.O. (2023). "National Security: An Assessment of Concepts, Structures, and Plans". FASSJASSR Journal.
14. Okwuwada, N. (2023). The modern day consequences, causes, and nature of kidnapping and banditry in Nigeria. Munich Personal RePEc Archive (MPRA). https://mpra.ub.uni-muenchen.de/117234/
15. Onuoha, F. C. (2014). "Kidnapping and national security in Nigeria". African Security Review, 23(2), 1–15
16. Ortmeier, P. J. (2022). Introduction to Security: Operations and Management. Pearson.
17. Turner, S. (1998). The social construction of risk and safety. In J. Franklin (Ed.), The politics of risk society (pp. 45–62). Polity Press.
18. Ukor, .V. A. & Ugumanim, B.O. (2025) "Combating Internal Security Problems in Nigeria: The Relevance of Surveillance". UJJPS University of Jos Journal of Political Science. Volume 2, Issue 1