

Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Academic Innovations City University Foundations

Proceedings of the Cyber Secure Nigeria Conference – 2024

National Identity Management and National Security in Nigeria in the Era of Artificial Intelligence: The Imperative of AI-Driven Joint National Identity Database

¹Akande, A.T., ²Akande, J., ³Ozomata, B.U., & ⁴Edibo, D.M.

University of Abuja, Nigeria

²Birmingham City University, Birmingham, UK

³Federal University Lafia, Nigeria

E-mails: ¹abdulazeez.akande@uniabuja.edu.ng, ²lekanjava@gmail.com

Phone; +2347034994977

ABSTRACT

This paper examines national identity management and national security in Nigeria in the era of Artificial Intelligence, with a special focus on the need for an AI-driven joint national identity database for a holistic and robust identity management towards ensuring security and strengthening national security in the era of terrorism and banditry. The paper adopts the Information Systems Success Model as its theoretical framework. The model developed by William H. DeLone and Ephraim R. McLean is a foundational framework in information systems research. The paper argued that creating a joint database of all hitherto existing national identity data will ensure holistic, more effective and efficient national identity management that will promote national security and enhance all efforts at tackling insecurity in the country. The paper recommended a joint national identity database domiciled in the office of the National Security Adviser, and a mandatory transfer of all old and new identity data to the created database. The paper concluded that national identity management plays an important role in national security in Nigeria and that the creation of an AI-driven joint identity database is a right and important step towards strengthening national security in Nigeria.

Keywords: national identity, national identity management, security, national security, artificial intelligence and joint database.

Proceedings Citation Format

Akande, A.T., Akande, J., Ozomata, B.U., & Edibo, D.M. (2024): National Identity Management and National Security in Nigeria in the Era of Artificial Intelligence: The Imperative of AI-Driven Joint National Identity Database. Proceedings of the Cyber Secure Nigeria Conference held at The Ballroom Center, Central Business District, Federal Capital Territory, Abuja, Nigeria - 25th - 26th September, 2024. Pp 151-164. <https://cybersecurenigeria.org/conference-proceedings/volume-1-2024/dx.doi.org/10.22624/AIMS/CSEAN-SMART2024P14>

1. INTRODUCTION

Since Nigeria returned to democratic administration in 1999, the country has been beset by continuous and growing security concerns that have destabilised entire regions, imperilled the economy, and impeded growth. Chief among these concerns is terrorism, led principally by Boko Haram, and rampant banditry, particularly in northern Nigeria. These threats have aggravated the already weak security situation in the country and exposed substantial inadequacies in national administration and strategy. One of such gaps is the lack of a robust, harmonised and integrated identity management system. The absence of a harmonised national identity database has impeded the government's capacity to confront these threats and deliver on its democratic mandate.

Boko Haram's insurgency, which began in Nigeria's northeast, has killed tens of thousands and displaced millions. Its violent campaign against the state, coupled with its offshoot faction, the Islamic State West Africa Province (ISWAP), has wrought havoc, destabilising communities and weakening security in the Lake Chad area (Onuoha, 2012). The insurgency has exposed the flaws in Nigeria's security infrastructure, particularly in its ability to monitor and track movements across borders and identify persons associated with terrorist groups and other criminal groups.

In the northwest, banditry has become an equally formidable threat. Bandit organisations, frequently armed with modern weapons, engage in large-scale kidnappings, livestock rustling, and raids on villages, leading to the displacement of thousands of people. States including Zamfara, Katsina, Niger and Kaduna have bore the brunt of these attacks, with local communities living in constant fear of violence (International Crisis Group, 2020). The lack of comprehensive and harmonised identity management systems has made it impossible for law enforcement agencies to follow these criminals and their networks, thus compounding the situation. As smugglers, robbers and rebels exploit Nigeria's porous borders and inadequate security infrastructure, the need for a harmonised identity management system becomes even more important.

To properly address these security concerns, Nigeria must adopt a holistic approach that blends solid planning, clear policy frameworks, and improved governance. One key part of this approach is the establishment and implementation of a joint national identity database. Currently, the country's identity management systems are fragmented, with several agencies keeping separate databases that do not communicate with each other. This fragmented approach makes it impossible to precisely identify individuals and residents, reducing the government's capacity to combat terrorism, banditry and other related crimes efficiently. For example, the National Identity Management Commission (NIMC) is responsible for registering citizens and issuing National Identification Numbers (NIN). However, the NIMC has struggled to obtain extensive coverage due to operational obstacles, funding limits, and insufficient infrastructure. At the same time, other organisations, such as the Independent National Electoral Commission (INEC), maintain their voter registration database, while the Federal Road Safety Commission (FRSC) issues driver's licenses, and the Nigeria Immigration Service (NIS) manages passport issuing. Banks, on the other hand, implement the Bank Verification Number (BVN) system to ensure secure transactions and mitigate fraud (Ogunleye, 2017).

This disconnected approach to identity management produces duplication and inefficiencies, making it difficult for the government to trace individuals across numerous systems. Terrorists, bandits, and other criminals might exploit this vulnerability by using different identifying credentials in different places, escaping law enforcement. A shared national identification database that incorporates all these agencies' data into a single, secure platform would enable the government to authenticate identities accurately and in real-time, increasing national security and minimising fraud (National Identification Management Commission, 2021).

The existing identity management system in Nigeria is a patchwork of autonomous databases and efforts, each servicing a specific sector but lacking collaboration with others. For instance, while the BVN has successfully addressed fraud in the banking sector by providing a uniform identity verification system for account holders, it is limited to financial transactions and does not integrate with the NIMC's database or other government services (Central Bank of Nigeria, 2019). Similarly, the voter registry kept by INEC is exclusively utilised for elections and lacks connectivity with the broader national identity infrastructure.

The FRSC's driver's license system and the NIS's passport issuance processes are also independent projects that do not contribute to a centralised identity management framework. A single national identity database will not only increase national security by enabling the government to trace those involved in criminal activities more efficiently but also improve governance by guaranteeing that citizens have access to key services and social programs. The purpose of this paper consequently is to explore the imperative of an AI-driven unified national identification database to national identity management and national security in Nigeria.

Statement of Research Problems

The advent of Boko Haram in the northeastern region and the spread of banditry, particularly in the northwest, have not only imperilled the lives of civilians but also highlighted major weaknesses in the nation's security architecture (Onuoha, 2012; International Crisis Group, 2020). These security issues have persisted due in large part to the government's incapacity to detect and supervise the activities of those engaging in illegal operations. A significant factor to this issue is the absence of an integrated and harmonised national identity management system. The current status of identity management in Nigeria is fragmented and haphazard, spanning over several entities that function in silos, with little to no coordination among them. This fragmentation hinders efforts to increase national security and diminishes the government's capacity to deliver key services effectively.

The Nigerian government has made several attempts to address the country's identity management issues, including the establishment of the National Identity Management Commission (NIMC) in 2007, which was tasked with overseeing the creation and management of a unified National Identity Database (NIMC, 2021). Despite this effort, the progress has been gradual, with a considerable section of the population still unregistered. In addition, other organisations such as the Independent National Electoral Commission (INEC), the Federal Road Safety Commission (FRSC), the Nigeria Immigration Service (NIS), and commercial banks have built their identification databases.

These authorities issue identity credentials for specific reasons, such as voter cards, driver's licenses, passports, and Bank Verification Numbers (BVN), respectively (Ogunleye, 2017). However, these databases are not linked to the NIMC's National Identification Number (NIN) system, resulting in a lack of interoperability and inefficiency.

This fragmented system of identity management creates a huge concern for national security. The failure to verify identities across sectors has led to circumstances where criminals, including terrorists and bandits, can operate undetected by using numerous identification credentials (Eboh, 2018). For example, an individual could be registered with INEC to vote, carry a passport issued by the NIS, and possess a BVN for banking transactions, all without their records being cross-referenced or merged into a single national database. This lack of integration makes it harder for security services to trace persons across numerous sectors and geographical locations, reducing the country's ability to respond to security concerns efficiently.

The problem is further aggravated by the inefficiencies inside the NIMC itself. Since its founding, the NIMC has struggled to register a significant fraction of Nigeria's over 200 million inhabitants. This is due to various challenges, including inadequate finance, poor infrastructure, bureaucratic bottlenecks, and a lack of public awareness (National Identity Management Commission, 2021). As a result, millions of Nigerians remain undocumented, creating a big, vulnerable population that can readily be abused by criminal networks.

Moreover, the absence of a uniform identity management system has broader consequences for government and the delivery of the benefits of democracy. Without an accurate and trustworthy way of identifying citizens, the government confronts difficulty in implementing social welfare programs, ensuring fair allocation of resources, and combating corruption. For instance, ghost workers and duplicated beneficiaries in government schemes siphon off public monies, while many legitimate residents are unable to access these programs due to a lack of legal identification (Eboh, 2018). This failure diminishes public trust in government institutions and erodes the state's capacity to govern effectively. This paper, therefore, attempts to evaluate how the adoption of an AI-driven joint national identification database could improve national security by enabling better tracking of individuals, increasing law enforcement efforts, and supporting more effective government.

2. CONCEPTUAL REVIEW

National Identity

The psychological bond that a person has with their nation is known as their national identity. This bond is thought to contribute to political stability and the resilience of national security institutions by giving the person a sense of security, loyalty, and belonging to the nation-state (Miller, 2000). The relationship between a person's national identity and the state's larger security framework is highlighted by this perspective. From Smith's perspective (1991), national identity refers to the perception of a country as a unified entity, characterised by unique customs, language, politics, and culture. In a nation's unity and the allegiance of its people, it plays a crucial role. As a key component of preserving national security and cohesiveness, national identity promotes solidarity. This definition emphasises this point.

National Identity Management

According to Thuan (2007), identity management refers to the procedures, guidelines, and tools used to manage user identities throughout their whole lifecycle within a system and to manage user access to resources by linking rights and limitations. Identity management is a large administrative domain that deals with identifying users inside a system and limiting their access to resources by linking user privileges and restrictions to the user's established identity. According to Identity Week America (2023), identity management plays a crucial role in safeguarding digital identities, especially in industries such as government, healthcare, and banking. Identity management in the context of new technologies like as biometrics and Artificial Intelligence (AI) entails effectively managing digital identities to safeguard compliance and avoid fraud in a highly dynamic environment. The National Identity Management Commission (2007) notes, however, that identity management suggests a collection of data management procedures and systems that, when applicable, work to boost people's trust in their identity. It is also described as the collection of guidelines, norms, regulations, procedures, and processes that are applied to achieve the intended results of identification.

The United States Cybersecurity and Infrastructure Agency (2023) views national identity management as a systematic framework that governs how a nation registers, verifies, and maintains the identities of its citizens through legal, technological, and procedural means. This is because national identity management is more intricate and broader due to its framework and scope. It entails building an extensive national database to house private citizen data, guaranteeing that every person may be uniquely identified to expedite access to national security and government services.

Processes like access control, credential issuing, and identity verification are also included in this system. Williams (2023) contends, however, that national identity management provides a safe foundation for digital societies by guaranteeing individuals' access to public services. It uses blockchain, cryptography, and biometrics among other technologies to manage identities in a way that guards against fraud and illegal access. In addition to improving general governance and transparency, the system enables safe access to social welfare, banking, and healthcare services, facilitating quicker interactions between the state and its citizens.

National identity management, according to the National Institute of Standards and Technology (2023), is the process and technology that governments use to manage the lifecycle of citizens' identities, from birth registration to the issuance of national ID cards and death certificates. This viewpoint is influenced by governance and policy. Strict identity verification procedures and the utilisation of compatible systems enable various government entities to instantly validate persons. In compliance with national and international privacy standards, this technology improves not only the delivery of governmental services but also the safeguarding of personal data.

According to Gartner (2023), national identity management is essential to maintaining national security since it makes sure that people's identities are verifiable and trustworthy, which helps with immigration control, law enforcement, and counterterrorism initiatives. Governments can more efficiently identify and monitor people's whereabouts and activities by fusing national identity systems with biometric verification techniques.

These kinds of systems are essential in nations where there is a significant migration rate and a threat from terrorism, as identity management facilitates the separation of legal residents from undocumented immigrants. From the different perspectives presented above, it is evident that national identity management is designed to provide effective planning, policy formation, citizen protection, national security, and the prevention and investigation of criminal activity.

Security and National Security

To protect a state's integrity, sovereignty, and citizens from external and internal threats, security is seen by Buzan (1991) as the use of political, economic, military, and social measures to maintain stability and safety. This conception emphasises the wide range of security that security encompasses, including identity management's role in safeguarding the state's sovereignty and public safety. Also, Smith (2023) contends that security is the state of being shielded from or not exposed to danger or risk, encompassing various dimensions. On the other hand, national security refers to the use of diverse tactics and regulations to defend a country's sovereignty, territorial integrity, and people against dangers both inside and outside the country (Aluko, 2023). Nye (2010) notes that it refers to the actions made by a government to guarantee the defence of its country against external threats as well as the preservation of its territorial integrity, sovereignty, and residents' welfare.

Database

According to Elmasri & Navathe (2023), databases used in identity management systems are made to manage and store identity-related data, including biometric and personal information. This ensures the security and integrity of sensitive data for procedures involving identity verification and authentication. Robinson & Wang (2022) aver that a joint database is a centralised system that aggregates identity data from several government agencies or organisations to enable uniform management and secure access to full identity information for national security objectives. Furthermore, according to Schaefer & Johnson (2024), it is a centralised system that aggregates identity data from many government agencies or organisations to enable unified management and secure access to comprehensive identity information for national security objectives.

3. THEORETICAL FRAMEWORK

The Information Systems Success Model, created by William H. DeLone and Ephraim R. McLean, serves as the theoretical basis for this study and is a key paradigm in the field of information systems research. It is frequently used to clarify, comprehend, and assess the effectiveness of information systems inside businesses and, in a broader sense, throughout a whole nation. In their landmark work "Information Systems Success: The Search for the Dependent Variable" (DeLone & McLean, 1992), they originally presented the concept.

Six interconnected dimensions are proposed by DeLone and McLean (1992) to characterise the success of an information system. The first category is system quality, which covers the technical characteristics of the system, including performance, usability, and reliability. A high system quality indicates that the data system is both user-friendly and satisfies the necessary technical requirements.

The system's output quality, as determined by characteristics like timeliness, correctness, relevance, and completeness, is the second factor in information quality. Sufficient information quality guarantees that the data produced by the information system is practical and fulfils the requirements of the users. Another was included in 2003 as part of an update to the model: service quality. This dimension assesses the level of assistance that users receive from the vendor or information system department.

When providing support services, it entails being receptive, dependable, and empathetic (DeLone & McLean, 2003). Use, on the other hand, describes how and to what extent the information system is used by its intended users. This might involve both required and voluntary use, and it's seen as a vital sign of an information system's effectiveness. Furthermore, user satisfaction gauges how happy users are with the information system as a whole. The evaluation is a subjective one that captures the users' satisfaction and experience with the system. The last category is net benefits, which includes all of the effects of the information system on the business as a whole, including increased customer happiness, productivity, cost savings, and decision-making. Net benefits serve as both the primary indicator of an information system's performance and the rationale for the system's purchase.

A useful framework for assessing the performance of a collaborative database project that compiles information from all of Nigeria's current identity management organisations and parastatals is provided by the Information Systems Success Model. Because it offers a centralised, reliable, and all-inclusive source of identity data for many industries, this kind of database is essential for improving national security. This project places a high priority on system quality since the combined database needs to be technically sound, safe, and able to seamlessly combine data from several sources. A top-notch system guarantees the seamless merging of data from multiple agencies, including the National Identity Management Commission (NIMC), immigration services, and voter registration bodies, resulting in increased dependability and efficiency in all national security-related sectors (Afolabi, 2020).

In this situation, the quality of the information is equally crucial. Ensuring the accuracy, completeness, and timeliness of the data is vital for the unified database to facilitate security agencies' access to comprehensive and uniform identity information. Accurate identification of people is one way that high-quality information helps security services detect and respond to security risks (Adepoju, Akinyemi, & Bashir, 2019). Conversely, service quality concerns the assistance given to different government departments and parastatals for them to use and access the unified database. Coordination and effectiveness of national security measures depend on all relevant entities being able to efficiently retrieve and use the data they require, which is ensured by effective service quality (Okunoye, Karsten, & Frolick, 2010). Ultimately, enhanced national security, enhanced agency coordination for identity management, and more effective citizen service delivery are the Net Benefits of a well-run joint database. Through the use of the Information System Success Model, this database's effectiveness can be evaluated in terms of these observable results, eventually leading to a safer and more well-run Nigeria.

4. RELATIONSHIPS BETWEEN NATIONAL IDENTITY MANAGEMENT AND NATIONAL SECURITY

To achieve national security, national identity management is essential, particularly in countries like Nigeria, where organised crime, banditry, and terrorism pose serious dangers. Due to the lack of a cohesive, effective identity management system, criminals have been able to take advantage of weaknesses in Nigeria's administrative framework, which has led to an increase in banditry, terrorism, and other associated crimes. When national identity management systems are administered correctly, truly, and with seriousness, they give governments the means to track people's movements, verify identities, and curtail criminal activity, all of which contribute to the strengthening of national security (Aina, 2020).

For more than a decade, Nigeria has been plagued by terrorism, spearheaded by organisations like Boko Haram and the Islamic State West Africa Province (ISWAP). These are the kinds of places where people can roam around freely and stay anonymous. In a similar vein, banditry has grown to be a major security risk, particularly in northwest Nigeria. Bandits exploit poor identification systems and permeable borders to carry out violent attacks, kidnappings, and looting. Terrorists and bandits frequently utilise counterfeit or various forms of identification to avoid detection by law enforcement (Onuoha, 2012).

For the government to fight terrorism and banditry more successfully, a strong, harmonised and integrated national identity management system is not only necessary but critical. The National Identity Management Commission (NIMC) can keep an extensive and centralised database that aids in the identification and tracking of people by collecting biometric data, such as fingerprints and facial recognition. Cross-border movements, recruitment efforts, and the financing of terrorism can all be significantly reduced by using biometric data to minimise duplication and make it more difficult for criminals to adopt false identities (Eboh, 2018). Comparable systems have significantly improved national security and reduced crime in the nations where they have been put into place (Aina, 2020).

The Nigerian identity management system is currently disjointed, with disparate databases kept up to date by organisations including the Bank Verification Number (BVN) system, the Nigeria Immigration Service (NIS), the Independent National Electoral Commission (INEC), and the Nigeria Management Council (NIMC). It is challenging for law enforcement organisations to have a comprehensive understanding of a person's identification because these disjointed systems function in silos (Ogunleye, 2017).

For example, an individual engaged in terrorist activities may possess several identity documents from several authorities without any cross-referencing or linking of their data. All institutions, including banks, immigration, and electoral entities, would share a shared database if there were a fully integrated, harmonised and joint national identity management system in place. Security agencies would be able to recognise and keep an eye on suspects in real time thanks to this connection, which would not only increase the effectiveness of tracking persons but also boost intelligence gathering. This is especially crucial in the fight against terrorism since trustworthy identification systems are needed to monitor and intercept communications across terrorist networks (Adedokun, 2021).

The lack of a secure identity management system is frequently exploited by terrorists and criminals to fabricate identities to elude capture by law enforcement. Due to a lack of accountability, Nigeria has seen an increase in the illegal arms trade, human trafficking, and financing of terrorism (Onuoha, 2012). When properly connected with other systems, the National Identification Number (NIN), which is essential to Nigeria's identity management framework, can assist in reducing identity fraud. Nigeria's porous borders, which make it easy for criminals to enter and exit the nation undetected, provide one of the biggest obstacles in the fight against terrorism and banditry. This problem can be addressed with effective national identity management, which makes sure that people crossing borders can be reliably identified via biometric verification methods.

This would facilitate people monitoring and stopping foreign bandits or terrorists from entering Nigeria (Ogunleye, 2017). Additionally, as other nations dealing with comparable issues have shown, biometric identification management is essential to bolstering border security.

Without any iota of doubt, national identity management and national security are closely tied in nations like Nigeria, where stability is seriously threatened by banditry, terrorism, and other associated crimes. Nigeria can improve its overall security framework by boosting its ability to track, monitor, and deter criminal actions through the enhancement of an integrated identity management system based on biometrics. Nonetheless, for this system to be successful, it must be implemented well, work across agencies, and raise public awareness to guarantee that all Nigerians are enrolled and that the system runs smoothly in all areas.

5. IMPERATIVE OF JOINT NATIONAL IDENTITY DATABASE FOR NATIONAL SECURITY

Strengthening national security in Nigeria, where crime, banditry, and terrorism are becoming challenges to stability and governance, requires a single national identity database. The lack of a unified identity system has resulted in serious shortcomings in the nation's capacity to efficiently handle internal security. Creating a common national identity database that unifies demographic and biometric data from all sectors can be the first step towards resolving these security issues.

Fighting the threat has become challenging and time-consuming due to Nigeria's disjointed identity management system, which sees many authorities functioning in isolation from one another. Law enforcement has a difficult time following terrorists and bandits since they have a history of using phoney or multiple identity documents to evade detection (Aina, 2020). It would be more difficult for criminals to operate undetected if the government maintained a single, verifiable identity for every individual through a shared national identity database anchored on the National Identification Number (NIN) (Ogunleye, 2017). Security organisations would be able to follow suspected offenders more successfully and coordinate responses across borders and regions with the help of this information centralisation, especially when combined with biometric data like fingerprints and facial recognition.

Terrorists associated with Boko Haram and other rebel organisations, for instance, take advantage of Nigeria's open borders and deficiency in a strong, harmonised and joint identity verification mechanism. By guaranteeing that only those with verified identities are allowed to enter borders, the implementation of a national identification database could assist border

security services (Onuoha, 2012). Furthermore, prompt information sharing would be made possible by the integration of national identity data with security agencies, decreasing the possibility of terrorist attacks and enabling preemptive action.

To modernise law enforcement across Nigeria, a unified national identity database is essential. The incapacity of Nigerian security forces to effectively authenticate individuals implicated in criminal activities stems from the dispersed databases upheld by organisations like the Nigeria Immigration Service (NIS), banks, the Independent National Electoral Commission (INEC), and the National Identity Management Commission (NIMC) (Adedokun, 2021). Criminals can utilise multiple identities in different industries due to this lack of interconnection, which makes it more difficult to prosecute them.

Identity fraud and impersonation can be considerably decreased by the government by combining all identity information, such as voter registration, passports, driver's licenses, and the Bank Verification Number (BVN) into a single, complete database. The ability of law enforcement to trace criminal suspects would be improved by this integration, which would also decrease the operational capability of criminal networks and increase the overall efficacy of national security operations (Eboh, 2018). Additionally, it would simplify the legal system's and law enforcement's capacity to verify suspects' identities, resulting in more effective prosecutions.

Nigeria has a large number of identification databases, which have resulted in a massive identity fraud problem that is taken advantage of by both corrupt authorities and criminals. According to Aina (2020), issues such as ghost workers, dishonest recipients of government assistance, and those who take advantage of legal gaps to make money have become widespread. By guaranteeing that every citizen and legal resident is registered under a distinct identity that can be validated across all sectors, a shared national identification database would assist in dealing with these problems. By reducing corruption and guaranteeing that social services are provided to the right people, this will not only increase security but also enhance the government. Nigeria's security and governance depend on the establishment of a unified national identity database. Nigeria can more effectively fight terrorism, banditry, and other types of criminal activity by centralising identity data and guaranteeing interoperability between government departments. The implementation of such a system would be a major step towards enhancing good governance and transparency, as well as ensuring efficient law enforcement and national security.

6. TECHNICAL IMPLEMENTATION AND ARTIFICIAL INTELLIGENCE WORKING OF THE PROPOSED JOINT DATABASE DATA FRAMEWORK

A robust data integration framework is essential to consolidate databases from entities such as the National Identity Management Commission (NIMC), the Nigeria Immigration Service, the Independent National Electoral Commission (INEC), and banks. This framework will ensure seamless data exchange and interoperability. The data would be resident with the national security adviser's office and would be searchable upon clearance by other security entities of the government, such as the DSS, military intelligence, the Nigeria Police Force and others.

- Interoperability Standards: Establish common data standards and protocols to facilitate communication between disparate systems.

- Real-Time Data Synchronisation: Implement real-time data synchronisation to provide agencies with up-to-date information, enhancing their ability to respond to security threats promptly.

Data Security Protocols and Scalability

Protecting sensitive data within the centralised database is paramount. Advanced encryption and access control mechanisms must be implemented to safeguard data integrity and privacy.

- Encryption: Utilise end-to-end encryption to protect data in transit and at rest.
- Access Control: Implement role-based access control to ensure that only authorised personnel can access sensitive information.
- Scalability and Redundancy: Design the system to be scalable and redundant to handle large volumes of data and ensure continuous availability.

Data from Friendly Countries and Open Sources

The NSA would need to seek and revive partnerships and intelligence sharing with friendly countries such as countries also fighting insecurity, so this information should be shared and stored by the NSA, we would also need to scrape online for accessible information from open-source platforms and online feeds, such as news feed, online blogs, and social media post to cross validate, optimize the information.

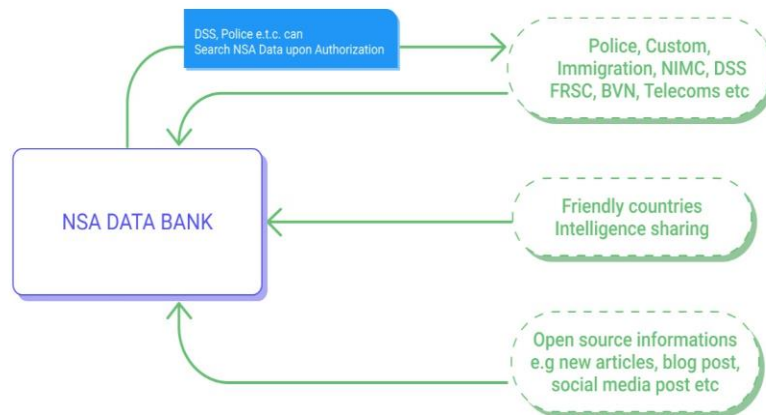


Fig 1: Architecture Diagram of Technical Implementation

AI Integration for National Security

The AI integration on such data would be beneficial in analysing patterns and predicting security threats or breaches, such as terrorist activity, and potential security breaches in the country.

1. **Threat Prediction Models:** Develop machine learning models to identify patterns indicative of security threats.
2. **Real-Time Alerts:** Implement a real-time alert system to notify security agencies of potential threats.

Anomaly Detection

Machine learning models can detect unusual patterns in data, indicating fraudulent activities or security breaches.

1. Fraud Detection Systems: Use AI to monitor transactions and identify anomalies that may signify fraud.
2. Behavioural Analysis: Analyse user behaviour to detect deviations from normal patterns, suggesting potential security issues.

Natural Language Processing (NLP)

NLP can analyse communications for potential threats, enabling early intervention by security agencies.

1. Communication Monitoring: Use NLP to scan communications for keywords and patterns associated with security threats.
2. Sentiment Analysis: Analyse sentiment in communications to assess potential risks.

Benefits of AI Integration for National Security

1. Proactive Security Measures: AI provides actionable insights, enabling proactive security measures and reducing the likelihood of successful attacks.
2. Resource Optimisation: Automating data analysis allows security agencies to allocate resources efficiently, focusing on high-priority threats.
3. Continuous Learning: AI systems continuously learn from new data, adapting to evolving security challenges and improving effectiveness.

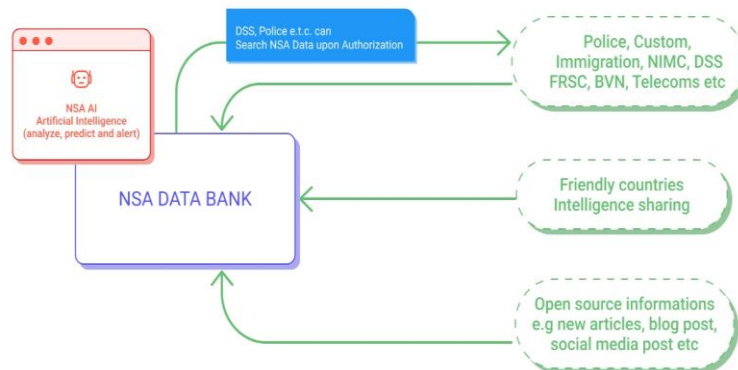


Fig 2: Architectural Diagram of AI Implementation

7. RECOMMENDATIONS

This paper, in line with the findings of this study, makes the following recommendations:

- i. Immediate creation of a sophisticated joint database to house all these national identity data that have been hitherto existing differently in the office of the National Security Adviser. This will help in strengthening national security and resolving criminal investigations by all security and military agencies in the country.
- ii. Also important is the legalisation of the above suggestion through legislation of the National Assembly. This is to make it legal in the eyes of the law and useful in preventing and resolving security challenges and investigations in the country.

- iii. The new legislation should also make it mandatory for all agencies and commissions to transfer a copy of new and existing national identity data to the joint database in the office of the National Security Adviser.

8. CONCLUSION

Conclusively, bolstering Nigeria’s national security requires the creation of a unified national identity database. Nigeria can effectively combat terrorism, banditry, and organised crime by integrating identity management systems across financial institutions, the National Identity Management Commission (NIMC), the Independent National Electoral Commission (INEC), and the Nigeria Immigration Service (NIS). Improved governance and the rule of law would eventually result from the unified system’s increased capacity for security personnel to follow movements, authenticate identities, and stop fraud. Nigeria needs a comprehensive and well-coordinated identity management system to ensure that all citizens benefit from democracy and to improve national security as well as accountability and transparency in government through the provision of a politically and economically stable environment needed for development and common prosperity. The AI-driven future embedded into the database will also enhance crime prevention and investigations.

REFERENCES

1. Adedokun, M. (2021). Enhancing national security through integrated identity management in Nigeria. *African Security Review*, 28(3), 67-89.
2. Adepoju, S. O., Akinyemi, I., & Bashir, M. (2019). National identity management system in Nigeria: A view on use and challenges. *International Journal of Technology Management & Sustainable Development*, 18(1), 21-38.
3. Afolabi, M. O. (2020). Data integration challenges in Nigeria’s national identity management system. *African Journal of Science, Technology, Innovation and Development*, 12(2), 145-152.
4. Aina, F. (2020). Identity management and national security: Implications for Nigeria. *Journal of African Studies*, 45(1), 12-30.
5. Aluko, O. (2023). National security and governance in Nigeria: Contemporary challenges and solutions. *Journal of African Security Studies*, 8(2), 45-67.
6. Buzan, B. (1991). *People, states & fear: An agenda for international security studies in the post-cold war era*. Brighton, UK: Harvester Wheatsheaf.
7. DeLone, W. H., & McLean, E. R. (1992). Information systems success: The quest for the dependent variable. *Information Systems Research*, 3(1), 60-95.
8. DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19(4), 9-30.
9. Eboh, M. (2018). National identity and governance: The role of a joint database. *Nigerian Journal of Governance*, 12(3), 23-45.
10. Elmasri, R., & Navathe, S. B. (2023). *Fundamentals of database systems* (8th ed.). New York: Pearson Incorporated
11. Gartner. (2023). National identity management: The cornerstone of national security and public safety. Accessed 28th August 2024 from <https://www.gartner.com>

12. Identity Week America (2023). Identity Week America 2023: Unveiling the future of identity management. Accessed 29th August 2024 from <https://www.identityweek.net>
13. International Crisis Group. (2020). Violence in Nigeria's North West: Rolling Back the Mayhem. Accessed 28th August 2024 from <https://www.crisisgroup.org>
14. Laws of the Federation (2007) Federal Road Safety Commission Act, No. 22. Abuja: Federal Government of Nigeria
15. Laws of the Federation (2015) Nigeria Immigration Act. Abuja: Federal Government of Nigeria
16. Miller, D. (2000). Citizenship and national identity. Cambridge, UK: Polity Press.
17. National Institute of Standards and Technology. (2023). Identity and Access Management Roadmap. Gaithersburg, Maryland: National Institute of Standards and Technology
18. Nigeria Inter-Bank Settlement System (NIBSS) (2024) Bank Verification Number. Accessed 28th August 2024 from <https://nibss-plc.com.ng/bank-verification-numberbvn/>
19. Nye, J. S. (2010). Understanding international conflicts: An introduction to theory and history (7th ed.). New York: Pearson.
20. Ogunleye, G. (2017). The role of identity management in national security: Nigeria's experience. *African Security Review*, 26(2), 147-165.
21. Okunoye, A., Karsten, H., & Frolick, M. N. (2010). IT identity in government: An exploratory study of national identity management in Nigeria. *Journal of Information Technology for Development*, 16(2), 112-134.
22. Onuoha, F. (2012). The audacity of the Boko Haram: Background, analysis and emerging trends. *Security Journal*, 25(2), 134–151.
23. Robinson, P., & Wang, H. (2022). Integrated identity management systems: Principles and practices. New York: Wiley.
24. Schaefer, B. E., & Johnson, R. (2024). Database systems for national security: An integrated approach. New York: Routledge.
25. Smith, A. D. (1991). National identity. Reno, Nevada, USA: University of Nevada Press.
26. Smith, R. (2023). Contemporary security studies. Oxford: Oxford University Press.
27. Strata Identity Orchestration (2023). IAM terminology: Identity access definitions 2023. Accessed 29th August 2024 from <https://www.strata.io>
28. Thuan, V. D. (2007). The ambiguity of identity. *Teletronikk*. 103(2), 3-4.
29. United States Cybersecurity and Infrastructure Security Agency (2023). Continuous Diagnostics and Mitigation Program: Identity, Credential, and Access Management (ICAM) Reference Architecture. Washington, DC: U.S. Cybersecurity & Infrastructure Security Agency.
30. Williams, C. (2023). Modern-day workforce authentication in identity management. TechRepublic.
31. National Identity Management Commission. (2021). NIMC Enrollment Update. Abuja: NIMC.
32. The Guardian (2021) Nigeria Immigration Service: From Kakawa in Lagos to Technology Building, Abuja. The Guardian Nigeria Newspaper. Accessed 28th August 2024 from guardian.ng/opinion/nigeria-immigration-service
33. The Nation Newspaper (2021) Nigeria Immigration Service: From Kakawa in Lagos to Technology Building, Abuja. The Nation Newspaper. 16 September 2021. Accessed 28th August 2024 from <https://thenationonlineng.net/nigeria-immigration-service-from-kakawa-in-lagos-to-technology-building-abuja/>