

Digital Identity Management Systems and National Security Enhancement

¹Dr. Onuoha Oju

¹PhD

¹Department of Computer Science

¹Ogbonnaya Onu Polytechnic Aba, Nigeria (formerly Abia State Polytechnic)

ojupro@gmail.com

Abstract—Digital Identity Management Systems (DIMS) are now essential tools for enhancing national security, increasing the efficiency of governance, and aiding digital transformation in both rich and developing countries. As governments are moving more and more towards digital public services, financial systems, border checks, and ways to verify citizens, the demand for safe and dependable identity management systems has grown more important. Digital identity systems help to identify citizens correctly, control access, prevent fraud, verify biometrics, secure transactions, and support security operations driven by intelligence. These systems are very important for fighting against terrorism, cybercrime, identity theft, illegal immigration, financial fraud, and cheating in elections. Still, there are problems like worries about privacy, data leaks, weak points in institutions, risks of excluding people, and poor management of cybersecurity that keep threatening how well they work. This paper looks at how digital identity management systems can improve national security, focusing specifically on developing countries. By looking at recent academic research in a thoughtful and detailed way, the study reveals that good digital identity systems can enhance trust in institutions, strengthen security, and improve the delivery of public services. This is especially true when these systems are backed by solid laws, measures to protect privacy, and strong cybersecurity setups. The paper ends by stating that digital identity should be viewed as an important part of the country's security system.

Index Terms—Digital Identity, Identity Management Systems, National Security, Cybersecurity, Digital Governance, Biometrics, E-Government.

I. Introduction

As more and more government services, banking, healthcare, education, and security systems move online, managing identities has become a key priority for the country. In today's world, having a reliable way to identify yourself is very important for using government services, banking, voting, healthcare, and managing borders.

Digital Identity Management Systems (DIMS) are technology setups that help create, check, confirm, and handle people's identities using electronic methods. These systems usually use methods like checking fingerprints or facial features, national ID numbers, digital IDs, ways to confirm identity, and compatible government databases.

Recent research indicates that at least 186 countries around the world have put National Digital Identity systems in place, highlighting their increasing significance in government operations and national safety (Corti, Sassetti, Sharif, Carbone and Ranise, 2025). National digital identity systems help people access government services more easily and build trust in institutions. They do this by allowing secure, reliable, and efficient ways to verify a person's identity (Corti et al., 2025).

In Nigeria, the National Identity Management Commission (NIMC) is still working to increase the number of people using digital identities. By 2025, more than 126 million citizens have signed up in the national identity database. This shows how important having a strong identity system is for good governance and security. (Vanguard News, 2025)

Digital identity systems are becoming more connected to national security because they assist in stopping identity theft, funding for terrorism, cybercrimes, cheating in elections, and illegal immigration. However, they also bring up worries about privacy, being watched, exclusion, and risks to cybersecurity.

This paper looks at how digital identity management systems can improve national security and discusses the necessary institutional structures for successful implementation.

II. Conceptual Review

2.1 Digital Identity Management Systems

Digital Identity Management Systems are tools and processes that help create, confirm, and handle the identities of people or organizations online. These systems consist of biometric databases, digital certificates, electronic ID cards, authentication systems, and identity frameworks based on blockchain technology.

They help ensure safe access to public services, money systems, health records, and border control systems. Digital identity systems are seen as essential for government services that focus on digital solutions and for the overall digital change in the country. (NCSC, 2025)

2.2 National Security

National security means keeping a country safe by protecting its independence, important organizations, people, and valuable resources from dangers that come from inside or outside the country. These dangers include terrorism, cybercrime, financial scams, spying, illegal immigration, and organized crime.

Today, national security relies more and more on digital systems because the way we govern and the important services we need are now based on technology.

2.3 Identity Security

Identity security means keeping digital identities safe from things like unauthorized access, fraud, impersonation, and misuse. It guarantees trust, keeps your information private, verifies who you are, and protects against online dangers.

Research shows that protecting identity is now a key part of managing cybersecurity because identity systems are main targets for attackers looking to gain access to important national infrastructure. (Thiemann, 2024)

III. Role of Digital Identity Management Systems in National Security

3.1 Prevention of Identity Fraud

Digital identity systems help lower the chances of identity theft, impersonation, and fake documents by using biometric checks, safe credentials, and centralized ways to confirm identities.

Old paper-based identity systems can be easily copied or changed, while digital systems offer better ways to confirm identity and keep track of information.

Identity systems that use blockchain technology make it harder to tamper with information and allow for better tracking. This helps to lower the chances of fraud in public services and financial systems.

3.2 Counterterrorism and Crime Prevention

Correctly checking someone's identity helps in collecting information, aiding the police, and securing borders. Security agencies can watch for unusual activities, check criminal histories, and stop people from using fake identities.

Biometric verification systems assist in identifying people who commit crimes repeatedly, those who are wanted, and groups that fund terrorism.

A digital identity also helps improve anti-money laundering (AML) and Know Your Customer (KYC) rules in banks and other financial organizations.

3.3 Electoral Integrity

Digital identity systems help to make voter registration better, stop people from voting more than once, and lower the chances of election fraud by making sure that only confirmed citizens can take part in elections.

This makes democracy stronger and helps to lower conflicts that can happen after elections.

3.4 Border Security and Immigration Control

Immigration systems are using more and more biometric passports, facial recognition, and digital identity checks to stop illegal migration, human trafficking, and international crime.

Connected identity systems enhance border security and help protect the nation's independence.

3.5 Access Control for Critical Infrastructure

Digital identity systems protect access to military bases, government records, healthcare services, and banks by making sure that only people who are allowed can get in.

This lowers the chances of insider threats and prevents unauthorized access to the system.

IV. Digital Identity and Governance Efficiency

Managing digital identities helps improve how things are run by cutting down on repeated data, corruption, and wasteful administrative processes.

National Digital Identity (NDI) systems speed up digital change by allowing easy access to government services and making service delivery more efficient. Research from the UAE indicates that properly set up NDI systems greatly improve how the government operates and the experience of citizens. (Alhammadi, Alhashmi, Lataifeh, and Rice, 2024).

Examples include:

- digital tax systems
- electronic health records
- social welfare targeting
- digital land registration
- online licensing systems
- public procurement verification

These changes make it easier to hold people responsible and build public trust, while also lowering chances for corruption.

V. Challenges of Digital Identity Management Systems

5.1 Privacy and Data Protection Risks

Centralized identity systems can lead to problems like widespread monitoring, improper use of data, and breaches of privacy if there aren't strong protections in place.

Studies indicate that making privacy a priority from the start is still a big issue in national ID systems and needs a stronger commitment from institutions. (Abomhara, Nweke, Yayilgan and Comparin, 2024)

5.2 Cybersecurity Threats

Identity databases are prime targets for cybercriminals. Data breaches can reveal private personal information and weaken people's trust in the nation.

Weak cybersecurity infrastructure significantly increases institutional vulnerability.

5.3 Exclusion and Accessibility Problems

Weak enrollment systems, lack of infrastructure in rural areas, and issues with paperwork can leave vulnerable groups out of digital identity systems.

This might make inequality worse instead of helping people feel included.

5.4 Weak Institutional Governance

Bad teamwork between agencies, corruption, and weak enforcement of policies lower the effectiveness of the system and decrease public trust.

Studies show that a lot of problems with digital identities come from weak institutions rather than just technical issues. A framework from 2025 discovered that around 80% of harms related to NDID were connected to poor institutions and governance systems. (Corti, Sassetti, Sharif, Carbone, and Ranise, 2025)

VI. Institutional Response Mechanisms

6.1 Strong Legal Frameworks

Governments need to create laws that protect people's identities, ensure data privacy, manage digital evidence, regulate the use of biometrics, and hold organizations accountable for cybersecurity.

Laws about data protection are very important for keeping the trust of citizens.

6.2 Cybersecurity Architecture

National identity systems need to use encryption, a zero-trust security approach, multi-factor authentication, and ongoing monitoring to stop unauthorized access.

Trustworthiness assessment frameworks now suggest looking at security, privacy, resilience, ethics, and reliability throughout the entire identity lifecycle. (Bottarellib, Epiphanioua, Mahmoodb, Hooperb, and Maple, 2025)

6.3 Independent Oversight Institutions

Regulatory agencies need to keep an eye on compliance, stop any misuse, and make sure there is openness in how identity management works.

6.4 Public Awareness and Inclusion Policies

People need to know how digital identity systems function and how their information is kept safe. Policies that include everyone should stop the exclusion of people living in rural areas and those who are vulnerable.

6.5 Public–Private Collaboration

Banks, phone companies, security firms, and government organizations need to work together to make better verification systems and prevent fraud.

VII. Recommendations

To make digital identity systems better for improving national security, governments need to:

1. Expand secure national identity registration systems.
2. Strengthen cybersecurity protections for identity databases.
3. Implement strong privacy and data protection laws.
4. Improve biometric verification and secure authentication standards.
5. Promote interoperability across government institutions.
6. Make sure that people living in rural areas and those who are vulnerable can access services and resources.
7. Improve border security by combining it with digital identity systems.
8. Establish independent oversight and accountability systems.

VIII. Conclusion

Digital Identity Management Systems are now essential tools for improving national security in today's digital world. They make it easier to check identities, make borders safer, lower fraud, help police, and make government work better.

Digital identity systems need to find a way to ensure security while also protecting people's privacy, promoting inclusion, and making sure institutions are accountable. If there isn't good management, these systems might cause new problems instead of fixing the ones we already have.

For developing countries, digital identity should be seen as an important part of the country's infrastructure that can enhance security and boost economic growth. To make things sustainable, we need to change laws, invest in cybersecurity, build trust in institutions, and focus on designs that put citizens first.

References

- [1] Abomhara, M., Nweke, L. O., Yayilgan, S. Y., and Comparin, D. (2024). Enhancing privacy protections in national identification systems: An examination of stakeholders' knowledge, attitudes, and practices of privacy by design. *International Journal of Information Security*, 23, 3665–3689.
- [2] Alhammadi, A. A., Alhashmi, S. M., Lataifeh, M., and Rice, J. L. (2024). The influence of national digital identities and national profiling systems on accelerating the processes of digital transformation: A mixed study report. *Computers*, 13(9), 243.
- [3] Corti, G., Sasseti, G., Sharif, A., Carbone, R., and Ranise, S. (2025). Enhancing national digital identity systems: A framework for institutional and technical harm prevention inspired by Microsoft's

harms modeling. *Proceedings of the 22nd International Conference on Security and Cryptography*, 723–728.

- [4] Bottarelli, M., Epiphaniou, G., Mahmood, S., Hooper, M., and Maple, C. (2025). Assessing the trustworthiness of electronic identity management systems: Framework and insights from inception to deployment. *arXiv Preprint arXiv:2502.10771*.
- [5] National Cyber Security Centre. (2025). The future of digital identity: Digital identity underpinning the UK's digital services.
- [6] National Identity Management Commission (NIMC). (2025). National identity database enrollment progress report.
- [7] Bottarelli, M., Epiphaniou, G., Mahmood, S., Hooper, M., and Maple, C. (2025). Assessing the Trustworthiness of Electronic Identity Management Systems: Framework and Insights from Inception to Deployment. *arXiv:10771v1*
- [8] Corti, G., Sasseti, G., Sharif, A., Carbone, R., Ranise and S. (2025) Enhancing National Digital Identity Systems: A Framework for Institutional and Technical Harm Prevention Inspired by Microsoft's Harms Modeling. DOI: 10.5220/0013601400003979 In Proceedings of the 22nd International Conference on Security and Cryptography (SECRYPT 2025), pages 723-728
- [9] Vanguard News (October,2025) Tinubu commends NIMC as National Identity database hits 126m enrolments
- [10] National Cyber Security Centre (NCSC) Annual Review (2025) The future of digital identity
- [11] Thiemann, T (2024) 2025 identity security and data security predictions. TechTarget
- [12] Alhammadi, A. A., Alhashmi, S. M., Lataifeh, M., and Rice, J. L. (2024). The Influence of National Digital Identities and National Profiling Systems on Accelerating the Processes of Digital Transformation: A Mixed Study Report. *Computers*, 13(9), 243.
<https://doi.org/10.3390/computers13090243>
- [13] Abomhara, M., Nweke, L.O., Yayilgan, S.Y. *et al.* Enhancing privacy protections in national identification systems: an examination of stakeholders' knowledge, attitudes, and practices of privacy by design. *Int. J. Inf. Secur.* **23**, 3665–3689 (2024). <https://doi.org/10.1007/s10207-024-00905-0>