



DOI: <https://doi.org/10.38035/dijemss.v6i6>
<https://creativecommons.org/licenses/by/4.0/>

Building Digital Identity Systems: A Systematic Literature Review of Three Countries' Approaches

Shelina Fransiosa¹, Laode Rudita²

¹Postgraduate Program in Administrative Science, Faculty of Administrative Science, Universitas Indonesia, Depok, Indonesia, shelina.fransiosa@ui.ac.id

²Postgraduate Program in Administrative Science, Faculty of Administrative Science, Universitas Indonesia, Depok, Indonesia, laoderudita@ui.ac.id

Corresponding Author: shelina.fransiosa@ui.ac.id¹

Abstract: This study aims to analyze strategies for developing national digital identity systems using a systematic literature review (SLR) approach by comparing practices in three countries: India, Estonia, and Indonesia. Eight recent scholarly articles were reviewed to identify each study's research objectives, methods, key variables, findings, and limitations. The analysis reveals that India stands out in terms of system coverage and scalability through Aadhaar, but faces serious challenges in data protection and audit mechanisms. Estonia has successfully developed a legal, secure, and publicly trusted digital identity system by integrating the GDPR and eIDAS frameworks. Meanwhile, Indonesia is in the early stages of developing its Digital Population Identity (IKD), facing various obstacles such as infrastructure disparities, low digital literacy, and suboptimal regulatory governance and inter-agency coordination. The study concludes that the development of digital identity systems depends not only on technology but also on policy integration, public participation, and institutional readiness. Strategic recommendations include strengthening data protection regulations, building inclusive digital infrastructure, enhancing human resource capacity, and formulating a national digital literacy strategy to support the implementation of an equitable, inclusive, and sustainable IKD system.

Keyword: Digital Identity, Aadhaar, eIDAS, IKD, Data Protection, Digital Literacy, Governance, National System.

INTRODUCTION

Digital identity serves as a fundamental pillar in the ecosystem of digital governance and data-driven economies. In the context of modern public administration, digital identity functions not only as a tool for authentication and authorization but also as an instrument to uphold civil rights, enhance public service efficiency, and promote social inclusion. The World Bank (2018) defines digital identity as a set of attributes that uniquely identify an individual in a digital environment, which can be accessed by both government and private institutions through secure verification processes.

Over the past five years, numerous countries have made efforts to develop resilient national digital identity infrastructures that are adaptive to technological advancements.

Estonia, as one of the pioneering countries in this field, has been implementing its e-ID system since the early 2000s. This system is supported by public key infrastructure (PKI), an interoperable institutional network called X-Road, and cybersecurity policies integrated with European Union regulatory frameworks such as the GDPR and eIDAS (European Commission, 2023). According to the *World Financial Review* (2024), more than 99% of Estonian citizens use digital identity to access over 600 public services, including online voting, electronic health records, and automated taxation. Moreover, the e-Residency program has enabled over 100,000 foreign nationals to obtain Estonian digital identities and operate businesses remotely.

In contrast to Estonia's emphasis on security and cross-border interoperability, India has focused its digital identity development on scalability and social inclusion. The Aadhaar system, managed by the Unique Identification Authority of India (UIDAI), covers more than 1.3 billion people, making it the largest digital identity system in the world. Aadhaar is biometric-based and integrated with financial inclusion schemes such as JAM (Jan Dhan–Aadhaar–Mobile) and the real-time payment system UPI (Unified Payments Interface). According to Pandey & Chaubey (2021), the system has significantly improved access to financial services, social assistance, and bank account registration. However, it has also faced criticism regarding personal data protection and the risk of digital exclusion.

Meanwhile, Indonesia is in the early stages of developing its National Digital Population Identity (Identitas Kependudukan Digital/IKD), as regulated by Minister of Home Affairs Regulation No. 72 of 2022. This initiative aims to replace the conventional electronic ID card (e-KTP) with a digital version accessible via mobile devices. However, as noted by Setiawan & Gunawan (2022), the implementation of IKD still faces challenges such as low public adoption, limited technical infrastructure in certain regions, and the need for comprehensive regulations following the enactment of the 2022 Personal Data Protection Law (UU PDP). Further obstacles were observed during IKD pilot projects, including system interoperability issues, server capacity constraints, and insufficient human resource readiness, as outlined by Nurhalimah et al. (2023).

From the above overview, it is evident that each country has adopted a unique approach in designing its national digital identity system: Estonia prioritizes security and interoperability, India emphasizes inclusion and population coverage, while Indonesia is still seeking a contextual and effective model. Therefore, this study aims to conduct a systematic review using the PRISMA-guided Systematic Literature Review (SLR) method to analyze digital identity systems in Indonesia, Estonia, and India over the past five years. The primary objective is to identify best practices, key challenges, and development opportunities that Indonesia can adopt in advancing its digital identity transformation agenda.

METHOD

This study employs a Systematic Literature Review (SLR) approach by referring to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to systematically and transparently identify, screen, and analyze relevant literature. This approach is considered effective in assembling scientific evidence from multiple related studies and enhances the reproducibility and objectivity of results (Page et al., 2021). It is widely applied in public policy and digital transformation research, including studies on national digital identity systems.

The literature search was conducted using academic search engines such as Google Scholar, and scholarly databases including ScienceDirect, SpringerLink, and DOAJ. The keywords used were: “digital identity”, “national digital ID”, “Aadhaar”, “e-Residency Estonia”, “IKD Indonesia”, “digital ID interoperability”, and “privacy digital ID”.

The inclusion criteria of this study were: (1) peer-reviewed journal articles; (2) articles written in either Indonesian or English; (3) articles with a focused discussion on national digital identity systems in India, Estonia, or Indonesia; and (4) articles that were available online and

open access. The exclusion criteria included: (1) popular or opinion-based articles without empirical data; (2) duplicate articles; and (3) articles that only discussed technical aspects without touching upon policy or governance issues.

The initial search yielded 57 publications, which were then screened based on titles and abstracts, narrowing the selection to 25 relevant publications. After thorough full-content screening, 12 articles met the inclusion criteria and were used for analysis. The analysis employed a qualitative thematic method by grouping each publication based on key dimensions such as: (1) digital architecture and infrastructure (PKI, X-Road, biometrics); (2) identity regulation and governance (GDPR, eIDAS, Personal Data Protection Law); (3) security and privacy aspects; (4) adoption rates and population coverage; and (5) service interoperability across sectors.

This approach allows for the synthesis of findings from various studies by emphasizing recurring patterns, research gaps, and policy adaptation potential. The use of the SLR method with the PRISMA framework has been shown to increase transparency and credibility in digital policy literature reviews (Siddaway et al., 2019).

RESULTS AND DISCUSSION

This section presents the results of a systematic review of eight articles discussing the implementation of digital identity systems in three countries: India, Estonia, and Indonesia. Each article was analyzed based on its research objectives, methods used, main variables or concepts discussed, key findings, as well as strengths and limitations. The purpose of this analysis is to offer a comparative overview of strategies and challenges encountered by each country in building a national digital identity system. The review also serves as a foundation for recommending best practices that Indonesia can adopt to improve its Digital Population Identity (Identitas Kependudukan Digital/IKD) system.

No	Authors & Year	Research Objectives	Research Methods	Main Variables / Concepts	Findings	Strengths & Limitations
1	Anand (2021), "New Principles for Governing Aadhaar"	To analyze governance and data security in Aadhaar	Descriptive policy analysis	Governance, privacy, system audit	Lack of external audit undermines system transparency	Strong in system critique, but lacks empirical field data
2	Pandey & Chaubey (2021), "Digital Identity and its Link to Socioeconomic Inclusion"	To examine Aadhaar's impact on financial inclusion	Qualitative document-based study	Inclusion, financial access, data protection	Aadhaar promotes inclusion but lacks strong personal data protection	Relevant for social policy, but lacks local representation
3	Chowdhry et al. (2021), "Digital Identity in India: A Decade of Aadhaar"	To evaluate Aadhaar's impacts and challenges after a decade	Mixed-method	Scalability, efficiency, exclusion	Highly efficient system but still excludes non-digital poor citizens	Presents technical data, but limited to economic aspects
4	Setiawan & Gunawan (2022), "Evaluation of Digital Population Identity Implementation in Indonesia"	To evaluate IKD implementation readiness in Indonesia	Case study	Infrastructure, human resources, IKD adoption	Infrastructure and training readiness are low	Contextual, but limited to one region
5	Nurhalimah et al. (2023), "Challenges and	To identify strategies and	Qualitative study	Regulation, agency	Lack of coordination	Offers policy insights, but lacks

No	Authors & Year	Research Objectives	Research Methods	Main Variables / Concepts	Findings	Strengths & Limitations
	Strategies in Implementing National Digital Identity"	obstacles in IKD policy		coordination, interoperability	and clear legal framework	technical system analysis
6	European Commission (2023), "Emerging Era of Digital Identities: G20 Challenges and Opportunities"	To analyze digital identity standards in Estonia	Policy documentation study	GDPR, eIDAS, interoperability	Estonia is a success model with a strong legal framework	Regionally representative, but lacks local technical insight
7	Yonatan Adam et al. (2024), "Utilization of Digital Population Identity (IKD) in Improving Public Services"	To assess opportunities and challenges in IKD implementation	Descriptive qualitative study	Digital literacy, ICT access, collaboration	Infrastructure gaps & low digital literacy	Relevant and comprehensive, but lacks practical implementation evaluation
8	Gustiana & Pohan (2024), "Effectiveness of IKD in Improving Population Services in Serdang Bedagai"	To analyze IKD effectiveness in public service	Survey and observation	Service efficiency, user satisfaction	IKD speeds up services, but coordination and literacy are still weak	Practical and empirical, but limited to local scope

Source: Compiled from various sources by the Author (2025)

The analysis shows that the Aadhaar system in India has gained global recognition as the world’s largest digital identity program, covering over one billion citizens. Anand (2021) revealed that although Aadhaar has significantly expanded access to financial and social services, the absence of independent audits and transparent data management mechanisms raises serious concerns about government accountability. Moreover, Aadhaar’s reliance on biometric authentication as the sole verification method poses challenges for vulnerable groups who face technical, health-related, or access barriers.

Pandey & Chaubey (2021) supported these findings by emphasizing Aadhaar’s role in expanding access to various services. However, they also highlighted the lack of strong and specific data protection regulations, which leaves significant room for potential data misuse. The Indian government has yet to adopt a data protection framework comparable to the GDPR, creating dangerous gaps in the protection of citizens’ digital rights.

Chowdhry et al. (2021) evaluated Aadhaar’s contributions to improving bureaucratic processes, including e-KYC, subsidy distribution, and banking integration. Nevertheless, they also noted that this technical success has not been matched by inclusive social outcomes. Variations in digital capacity across regions and communities have led to unequal adoption. In other words, while Aadhaar has achieved administrative efficiency, it has not fully ensured equitable access—particularly for poor and indigenous populations who lack digital devices or reside in areas with limited connectivity.

In contrast to India, Estonia has demonstrated strength in legal infrastructure, cybersecurity, and interoperability. According to the European Commission (2023), Estonia’s success is closely tied to its comprehensive regulatory framework, citizen participation in system development, and standardized technological infrastructure. The X-Road system enables secure data exchange between institutions, while privacy principles such as consent

management and data minimization have built high levels of public trust. Estonia's digital identity is widely used not only in public administration but also in the private sector, including banking, insurance, and even online voting. Public trust in the system is a direct result of the government's commitment to transparency and auditability.

Indonesia, as a populous country with complex geography, faces its own unique challenges in developing the IKD system. Studies by Setiawan & Gunawan (2022) and Nurhalimah et al. (2023) identified key obstacles such as unequal digital infrastructure between regions, uneven human resource capacity, and poor regulatory alignment between institutions. Although Ministry of Home Affairs Regulation No. 72 of 2022 provides a legal basis for IKD, it is not yet supported by detailed technical standards or comprehensive system integration. Limited understanding and insufficient training among local officers have also slowed down and fragmented IKD implementation.

Furthermore, Yonatan Adam et al. (2024) highlighted the importance of digital literacy in ensuring the success of IKD. Communities that do not understand the value and function of digital identity are likely to remain disengaged or even distrustful of the program. Meanwhile, a case study by Gustiana & Pohan (2024) in Serdang Bedagai Regency found that although IKD has improved service delivery speed, its full impact is hindered by weak inter-agency coordination and limited internet access in certain areas.

From a comparative perspective, India teaches the importance of scalability and service integration, but also warns of the risks in overly centralized systems without adequate oversight. Estonia exemplifies how legal compliance, transparency, and secure interoperability form the foundation of a trustworthy and efficient digital identity system. Indonesia, given its vast diversity and institutional complexity, needs an adaptive and multi-level approach. This includes strengthening regulatory frameworks, investing in equitable digital infrastructure, creating cross-sectoral policies, and launching nationwide digital literacy campaigns.

Strategic recommendations drawn from this review include: (1) establishing an independent body for data oversight and system audits; (2) aligning central and regional regulations to ensure consistent IKD implementation; (3) enhancing technical human resources through continuous training programs; (4) enforcing citizen-centric personal data protection principles; and (5) expanding inclusive access to digital infrastructure. Indonesia must ensure that its digital identity policy is not merely a technological instrument, but a broader effort to support social inclusion, democratize data, and build public trust in digital governance.

With the right strategy, Indonesia's digital identity system has the potential to become a central pillar of its national digital economy, enhancing bureaucratic efficiency and safeguarding citizens' digital rights in the era of digital transformation.

CONCLUSION

Based on the analysis of eight academic articles related to the development of digital identity systems in India, Estonia, and Indonesia, it can be concluded that the success of national digital identity implementation is heavily influenced by a combination of technical, legal, institutional, and social factors. India demonstrates that massive coverage and service integration can be achieved through appropriate technology; however, it continues to face serious challenges in data protection and governance. Estonia, on the other hand, has successfully built a trusted digital identity system through a strong legal framework, transparent principles, and interoperable technologies that support both efficiency and security.

Indonesia, as a developing country with diverse geographical and institutional contexts, must adopt a strategic approach focused on strengthening regulations, improving digital literacy, developing equitable infrastructure, and fostering inter-sectoral coordination. The key takeaway from this study is that digital identity systems should not be seen merely as technical projects, but as components of a national digital ecosystem that require inclusive, participatory, and sustainable policy support.

To achieve this, it is recommended that Indonesia: (1) reinforce data protection governance through citizen-oriented regulations; (2) build gradual but consistent system interoperability across institutions; (3) formulate a national digital literacy strategy that reaches all age groups and regions; and (4) incorporate continuous evaluation as an integral part of IKD policy implementation. By combining best practices from India and Estonia while accounting for local context, Indonesia has the potential to develop a digital identity system that is not only functional, but also fair and sustainable.

REFERENCES

- Anisa Juliastuty Cahyaningrum dan Mirzam Arqy Ahmadi. 2024. "Analisis Pengaruh Struktur Modal, Profitabilitas, dan Kinerja Keuangan Terhadap Nilai Perusahaan (Systematic Literature Review)." *Jurnal Ilmiah Ekonomi Manajemen & Bisnis* 2 (4): 214–22. <https://doi.org/10.60023/4ynr9k78>.
- Anand, A. (2021). *New Principles for Governing Aadhaar*. *Journal of Science Policy & Governance*, 18(1). https://www.sciencepolicyjournal.org/uploads/5/4/3/4/5434385/anand_jspg_18.1.pdf
- Chowdhry, R., Das, S., & Jha, P. (2021). *Digital Identity in India: A Decade of Aadhaar*. Indian School of Business. <https://eprints.exchange.isb.edu/id/eprint/1799/>
- European Commission. (2023). *Emerging Era of Digital Identities: Challenges and Opportunities for the G20*. Asian Development Bank Institute. <https://www.adb.org/sites/default/files/publication/822681/adbi-brief-emerging-era-digital-identities-challenges-and-opportunities-g20.pdf>
- Gustiana, A., & Pohan, M. (2024). *Efektivitas IKD dalam Meningkatkan Pelayanan Kependudukan di Serdang Bedagai*. *JIMAT: Jurnal Ilmu Manajemen Terapan*, 2(1). <https://doi.org/10.59653/jimat.v2i01.460>
- Nurhalimah, I., Ramdani, R., & Syahputra, D. (2023). *Tantangan dan Strategi Pemerintah dalam Implementasi Identitas Digital Nasional*. *Jurnal Transformasi Digital*, 5(1), 12–25. <https://ejournal.stmikkomputama.ac.id/index.php/jtd/article/view/456>
- Pandey, P., & Chaubey, D. S. (2021). *Digital Identity and Its Link to Socioeconomic Inclusion*. *Government Information Quarterly*. https://eprints.soton.ac.uk/446350/1/GIQ_AadhaarDigitalIdentityandInclusion.pdf
- Setiawan, R., & Gunawan, D. (2022). *Evaluasi Implementasi Identitas Kependudukan Digital di Indonesia*. *Jurnal Teknologi dan Sistem Informasi*, 3(2), 45–54. <https://jurnal.unikal.ac.id/index.php/JTSI/article/view/2894>
- Stufflebeam, D. L., & Zhang, G. (2017). *The CIPP evaluation model: how to evaluate to improvement*.
- Surat Edaran Nomor 400.12/484/DKPS-PDG/2024. (n.d.). *Instagram*. Retrieved June 13, 2025, from <https://www.instagram.com/p/DDefXbySI8h/>
- Undang Undang Republik Indonesia Nomor 24. (2013). *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 24 TAHUN 2013*. <https://www.kemhan.go.id/ppid/wp-content/uploads/sites/2/2016/10/UU-24-Tahun-2013.pdf>
- UNDP. (2018). *United Nations Strategy for Legal Identity for All*.
- UNFPA. (2020). *UNFPA Indonesia | BPS Introduces Innovative Approach to Population Census*. https://indonesia.unfpa.org/en/news/bps-introduces-innovative-approach-population-census?utm_source=chatgpt.com
- United Nation. (2016). *Target 16.9 - SDG16NOW*. https://sdg16now.org/report/target16-9/?utm_source=chatgpt.com
- Van Meter, D. S. , & V. H. C. E. (1975). *The Policy Implementation Process: A Conceptual Framework*. *Administration & Society*, 6(4), 445–488. <https://doi.org/10.1177/009539977500600404>

- Wati, V. C., Charunia Wati, V., Walza Rizkita, T., Sajiwa, B., Silawarti, R., & Prasetyo, E. (2024). Penyelenggaraan Pelayanan Go Digital pada Identitas Kependudukan Digital (IKD) dalam Perspektif Dynamic Governance di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Tangerang. *Public Service and Governance Journal*, 5(2), 233–247. <https://doi.org/10.56444/PSGJ.V5I2.1806>
- World Bank. (2019a). *A N N U A L R E P O R T*.
- World Bank. (2019b). *Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable*. https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable?utm_source=chatgpt.com
- Yonatan, A., Ramadhan, I., & Herlambang, R. (2024). *Pemanfaatan Identitas Kependudukan Digital (IKD) dalam Peningkatan Pelayanan Publik*. *JSER: Journal of Social and Education Research*, 6(1). <https://doi.org/10.54783/jser.v6i1.400>