AUREVIAJ JOURNAL OF SOCIAL SCIENCES AND HUMANITIES
DOI: https://doi.org/10.68925/kjvv9861

AUREVIAJ

Research Article | Open Access

Digital identity infrastructure and administrative exclusion in social protection delivery: An integrative review of evidence from developing countries

Mujibur Rahman Yusuf*

Dhaka University, Dhaka, Bangladesh

ABSTRACT

Digital identity systems are increasingly presented as administrative infrastructure that can improve the targeting, verification, and delivery of social protection in developing countries. However, the same systems may create new forms of exclusion when biometric authentication fails, registration documents are unavailable, connectivity is weak, or frontline staff apply eligibility rules inflexibly. This article examines how digital identity infrastructure affects administrative exclusion in social protection delivery. Using an integrative review design, it synthesizes peer-reviewed research and authoritative institutional evidence on digital identity, biometric verification, and social assistance in developing-country settings. The analysis is organized around four dimensions: enrolment and documentation, authentication and service access, data governance and accountability, and administrative capacity. The review finds that digital identity can reduce certain inclusion errors and improve payment traceability, but its benefits are conditional on inclusive registration, reliable fallback procedures, interoperable systems, data protection, and adequate frontline capacity. Without these conditions, digitalization may shift exclusion from paper-based eligibility barriers to technological and institutional barriers. The article contributes a policy-oriented framework for assessing whether digital identity reforms strengthen or undermine equitable social protection delivery.

Cite as: Yusuf, M. R. (2026). Digital identity infrastructure and administrative exclusion in social protection delivery: An integrative review of evidence from developing countries. *Aureviaj Journal of Social Sciences and Humanities*. *1*(2), 14-27 DOI: https://doi.org/10.68925/kjvv9861

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

ARTICLE HISTORY

Revised 12 November 2026
Accepted 13 November 2026

KEYWORDS

Digital identity; social protection; administrative exclusion; biometric authentication; developing countries; public administration

INTRODUCTION

Digital identity has become a central instrument of public administration reform in many developing countries. Governments increasingly use national identity numbers, civil registries, biometric databases, and digital authentication platforms to identify citizens, verify eligibility, deliver benefits, and link administrative records. In social protection, these systems are expected to reduce duplicate registrations, limit leakage, improve payment traceability, and make assistance more responsive during shocks. International organizations have therefore promoted identification as a foundation for financial inclusion, health care, education, social protection, and broader access to rights (World Bank, 2025). Yet the administrative promise of

*CONTACT [1]Mujibur Rahman Yusuf mujib.yusuf35@gmail.com Dhaka University, Dhaka, Bangladesh

digital identity is not automatic. A system that can verify identity more accurately may also prevent an eligible person from receiving food, cash, pensions, or health services if enrolment is incomplete, biometric authentication fails, or frontline staff lack the authority to use alternative verification procedures.

The scale of the identification gap makes this issue particularly important for developing countries. The World Bank estimates that approximately 800 million people worldwide still lack official proof of legal identity, while about 2.8 billion people live in economies without access to digital identification systems capable of supporting online authentication (World Bank, 2025). These gaps are unevenly distributed. Rural populations, women, children, displaced people, persons with disabilities, and poorer households are more likely to face barriers to obtaining or using identification documents (World Bank, 2024). Consequently, when social protection programs make digital identity a precondition for benefits, they may reproduce pre-existing inequalities through administrative systems rather than eliminate them.

Scholarship on digital identity has developed along several lines. A first body of work examines the technical and institutional design of identification systems, including civil registration, biometric enrolment, interoperability, cybersecurity, and data protection (World Bank, 2020). This research generally treats identification as a foundation for state capacity and service delivery. It emphasizes that reliable identification can reduce duplication, improve targeting, and support the integration of public services. However, it also recognizes that identification systems depend on broader institutional conditions, including civil registration, legal frameworks, administrative capacity, and citizen trust (World Bank, 2020).

A second line of research investigates the developmental potential of digital identification, especially its contribution to financial inclusion, service delivery, and social protection. Gelb and Clark (2013) argue that biometric identification can improve the ability of states to identify individuals and deliver services at scale. Similarly, the International Monetary Fund (2022) finds that digital identities linked to bank or mobile-money accounts can improve the delivery of social protection and help programs reach eligible beneficiaries. These studies highlight the potential efficiency gains of digitalization, particularly in contexts where paper-based records are difficult to verify and administrative resources are limited. They suggest that digital identity may reduce certain forms of leakage and strengthen the traceability of benefit flows.

A third, more critical literature examines how identity infrastructures reshape citizenship, surveillance, privacy, and access to entitlements. Masiero and Bailur (2021) argue that digital identity raises questions of justice because identification systems determine who is recognized by the state and who can access rights and services. This perspective moves beyond technical performance and asks whether digital identity systems distribute recognition, rights, and risks fairly. It is particularly relevant to social protection because beneficiaries are often among the most marginalized members of society and may have limited capacity to challenge administrative errors or technological failures.

Studies of India's Aadhaar system provide important evidence on these issues. Aadhaar assigns enrolled residents a unique identification number and supports authentication through demographic and biometric credentials. In the Public Distribution System, Aadhaar-based authentication is intended to reduce leakage and ensure that subsidized food reaches intended

beneficiaries. Research nonetheless shows that biometric authentication can create exclusion when fingerprints cannot be read, connectivity fails, or beneficiaries cannot resolve mismatches between identity records and program databases (Masiero, 2020b; Masiero & Shakthi, 2020). These problems are particularly consequential for older people, manual labourers, persons with disabilities, and others whose fingerprints may be difficult to capture or verify.

Masiero (2020b) finds that digital identity platforms can produce degenerative outcomes across access, monitoring, and policy layers. Exclusion occurs when entitled users cannot access the Public Distribution System; distortion occurs when monitoring systems fail to capture the realities of service delivery; and redirection occurs when policy shifts from public provision of subsidized goods toward cash transfers. This analysis is important because it shows that the effects of digital identity are not limited to individual authentication failures. Digital identity infrastructure may reshape the broader institutional logic of social protection, including the balance between in-kind assistance, cash transfers, public provision, and market-based delivery.

Research on Aadhaar also shows that exclusion is not experienced uniformly. Chaudhuri (2020) examines how citizens experience the state through Aadhaar and finds that the system can appear distant, opaque, and unevenly accessible. Krishna (2020) similarly shows that informal workers may face particular difficulties when digital identity requirements interact with precarious employment, mobility, and limited administrative support. These studies suggest that digital identity reforms must be evaluated through the experiences of users, not only through administrative indicators such as enrolment rates or authentication success rates.

Evidence from other developing-country contexts points to similar institutional challenges. The World Bank (2020) reports that more than 40 per cent of people lacking identification globally live in Africa, and that weak civil registration, limited documentation, and uneven administrative capacity constrain access to services. The World Bank (2024) likewise emphasizes that identification is a gateway to social protection, financial services, education, and formal employment. In this context, digital identity may offer important opportunities, but it may also deepen exclusion where foundational civil registration is weak or where digital systems are introduced before the underlying identification ecosystem is inclusive.

Broader research on digital inequality reinforces these concerns. Arora (2019) shows that digital access is shaped by social context, infrastructure, literacy, and everyday practices rather than by device ownership alone. Gurstein (2003) similarly argues that meaningful use of information and communication technologies requires more than physical access; it requires the capabilities, institutions, and support needed to translate access into beneficial outcomes. These insights are relevant to digital identity because a person may possess an identity number but still be unable to use it effectively if they lack connectivity, digital literacy, mobility, or assistance from frontline staff.

Research on datafication also highlights the political character of digital administration. Van Dijck (2014) shows that datafication transforms social relations by making aspects of life measurable, comparable, and governable through data. In public administration, this transformation can improve coordination but may also reduce complex social circumstances to administrative categories. Kitchin (2014) similarly emphasizes that data are not neutral

representations of reality; they are produced through technical systems, institutional practices, and forms of power. In social protection, these insights imply that identity data and eligibility records can shape access to rights in material ways.

Street-level bureaucracy theory provides an additional lens for understanding these processes. Lipsky (1980) argued that frontline public servants exercise discretion when implementing policy because rules cannot anticipate every situation they encounter. In digital identity systems, frontline staff—including enrolment officers, social workers, ration-shop dealers, payment agents, and grievance officers—interpret rules, assist citizens with authentication, decide whether exceptions are appropriate, and manage the practical consequences of system failures. Their discretion can either protect access or reinforce exclusion. Digital systems do not eliminate discretion; they often reconfigure it.

While prior scholarship has largely concentrated on the technical capabilities of digital identity systems or on single-country case studies, fewer studies have systematically examined the conditions under which digital identity infrastructure produces administrative exclusion in social protection delivery. Existing research often treats exclusion as a consequence of biometric failure alone. This narrower focus overlooks the wider administrative chain through which exclusion occurs: civil registration, enrolment, record matching, eligibility determination, authentication, grievance redress, and frontline implementation. It also gives insufficient attention to the institutional conditions that determine whether digital systems include or exclude vulnerable populations.

To address this gap, this article asks three questions. First, through which administrative mechanisms does digital identity infrastructure contribute to exclusion from social protection? Second, which institutional and design conditions mitigate exclusion while preserving the potential efficiency gains of digitalization? Third, what implications do these findings have for public administration and social protection policy in developing countries? The principal objective is to develop an integrated, policy-oriented understanding of the relationship between digital identity infrastructure and administrative exclusion in social protection delivery.

The article makes three contributions. First, it moves beyond a narrow focus on biometric failure by conceptualizing administrative exclusion as a process that may arise at multiple points in the social protection delivery chain. Second, it connects literature on digital government, street-level bureaucracy, and social protection to explain how frontline discretion and system design jointly shape access to entitlements. Third, it derives practical policy implications for developing countries implementing or expanding digital identity systems. The argument is not that digital identity should be abandoned. Rather, it contends that digital identity reforms must be assessed according to their effects on equitable access, not only according to administrative efficiency, fraud reduction, or technological sophistication.

The remainder of the article is organized as follows. The next section explains the research methodology. The findings section presents the four dimensions through which digital identity infrastructure affects social protection access. The discussion section interprets these findings in relation to the literature and develops their theoretical and policy implications. The final section presents conclusions, limitations, and directions for future research.

RESEARCH METHODOLOGY

This study used an integrative literature review design. An integrative review is appropriate when a research problem spans multiple disciplines, methods, and forms of evidence. Unlike a narrow meta-analysis, it allows the researcher to synthesize empirical studies, conceptual papers, and authoritative policy reports in order to develop a broader understanding of a complex public-administration phenomenon. The approach was selected because digital identity and social protection are studied across information systems, development studies, public administration, social policy, and law. A single methodological tradition would therefore exclude relevant evidence.

The review followed a structured, transparent, and reproducible procedure. Literature was identified through searches of Scopus, Web of Science, Google Scholar, and institutional repositories. Search terms combined concepts related to digital identity, digital ID, biometric identification, Aadhaar, national identity systems, social protection, social assistance, cash transfers, public distribution, exclusion, inclusion, and developing countries. Searches were conducted using combinations of these terms and their variants. The search strategy prioritized peer-reviewed journal articles, scholarly books and book chapters, systematic reviews, and reports from authoritative international organizations.

Studies were included when they addressed digital identity or biometric identification in relation to public-service delivery, social protection, welfare administration, or access to entitlements; focused on developing-country contexts or provided directly relevant conceptual or comparative analysis; and were published in English. Reports from the World Bank, International Monetary Fund, and other recognized international organizations were included when they provided systematic evidence, policy analysis, or cross-country data relevant to the research questions. Opinion pieces, news articles, promotional materials, and studies unrelated to social protection or public-service delivery were excluded. Where a study addressed digital identity but did not examine social protection or administrative access, it was retained only when it offered a directly relevant conceptual contribution to exclusion, data justice, or implementation.

The analysis proceeded in three stages. In the first stage, studies were screened for relevance to the research questions and organized according to their substantive focus: technical design, social protection delivery, citizen experience, governance, or policy implementation. In the second stage, the selected literature was coded using an initial framework derived from the research questions. Codes included enrolment barriers, documentation requirements, biometric authentication, connectivity, interoperability, frontline discretion, grievance redress, privacy, data protection, accountability, and administrative capacity. In the third stage, codes were compared and grouped into broader analytical themes. This process followed the logic of thematic synthesis, in which findings from different studies are translated into common constructs and interpreted in relation to the research questions (Braun & Clarke, 2006).

Document analysis complemented the academic literature. Institutional reports, program guidance, and policy documents were examined to understand how international organizations

conceptualize inclusive identification and how governments are advised to manage risks. Document analysis is appropriate when the research problem concerns policies, institutional arrangements, and official narratives embedded in written records (Bowen, 2009). The documents were read to identify stated objectives, implementation requirements, identified risks, and recommended safeguards. Their claims were then compared with peer-reviewed evidence on actual implementation and citizen experiences.

The review was limited by its reliance on published sources and by the uneven geographic distribution of research. India, particularly Aadhaar and the Public Distribution System, is heavily represented in the literature, while evidence from other developing regions is less extensive. This imbalance means that the findings should be interpreted as analytically general rather than statistically representative. The review also could not assess causal effects independently because it synthesized studies using different designs, measures, and contexts. These limitations are addressed by treating the review as a basis for developing an integrated explanatory framework rather than as a test of a single causal hypothesis.

RESULTS

The synthesis indicates that digital identity infrastructure affects social protection access through four interconnected dimensions: enrolment and documentation; authentication and service access; data governance and accountability; and administrative capacity. These dimensions do not operate independently. Weak civil registration may produce missing records, which in turn complicates authentication and eligibility verification. Limited frontline capacity may prevent staff from resolving authentication failures. Weak grievance mechanisms may leave citizens unable to correct errors. The findings therefore support an integrated understanding of administrative exclusion as a chain of institutional failures rather than a single technological problem.

Enrolment, Documentation, and Foundational Identification

The first dimension concerns whether people can obtain a digital identity in the first place. Digital identity systems depend on foundational civil registration, accurate demographic records, and accessible enrolment processes. Where birth registration is incomplete or identity documents are difficult to obtain, digital systems may inherit existing exclusion. The World Bank (2025) estimates that approximately 800 million people worldwide lack official proof of legal identity, and that progress remains uneven across regions and population groups. This means that digital identity reforms may not reach the people most likely to need social protection unless they are accompanied by measures to improve civil registration and documentation.

The literature shows that enrolment barriers are often social as well as administrative. Women, rural residents, displaced people, persons with disabilities, and poorer households may face greater difficulty obtaining identity documents because of distance from registration offices, costs, literacy constraints, gendered mobility restrictions, or lack of supporting evidence (World Bank, 2024). These barriers are especially important in social protection because eligibility for

assistance is often concentrated among populations with limited resources and weaker connections to formal institutions. A digital identity system that requires documents that vulnerable people cannot obtain may therefore exclude precisely those groups that social protection is intended to reach.

This finding challenges a common assumption that digitalization automatically improves inclusion. Digital systems can make services more convenient for people who are already registered and connected, but they may create a new administrative threshold for people who are not. The policy implication is that digital identity should be treated as part of a broader identification ecosystem rather than as a stand-alone technological reform. Governments need to invest in civil registration, mobile enrolment, fee waivers, assisted enrolment, and simplified procedures for people who lack conventional documentation.

Authentication, Service Access, and Fallback Mechanisms

The second dimension concerns the point at which a beneficiary attempts to use a digital identity to access a benefit. Biometric authentication is often presented as a solution to fraud and duplicate registration, but it can fail in practice. Fingerprint authentication may be difficult for agricultural workers, older people, and persons whose fingerprints have been worn down by manual labor. Iris or facial recognition may also fail because of disability, illness, poor image quality, or environmental conditions. When authentication fails and no alternative is available, the beneficiary may be unable to collect food rations, withdraw cash, or access a service.

Masiero (2020b) shows that Aadhaar-based authentication in India's Public Distribution System produced exclusion when users could not be recognized through biometric credentials. The problem was not merely that some authentication attempts failed; it was that the system did not always provide accessible, timely, and reliable alternatives. Where users were allowed only a limited number of attempts or were asked to return another day, a technical failure could become an effective denial of entitlement. This illustrates how a system designed to improve verification may generate exclusion when its operational rules do not account for real-world variability.

The findings also show that connectivity and infrastructure conditions matter. Digital authentication depends on electricity, network coverage, functioning devices, and trained operators. In rural or remote areas, these conditions may be unreliable. A beneficiary may possess a valid identity credential but be unable to use it because the point-of-service device is offline, the biometric reader is malfunctioning, or the operator cannot resolve a system error. In such circumstances, digital identity does not remove the administrative burden of proving eligibility; it may increase it by requiring citizens to travel repeatedly, wait for connectivity, or seek assistance from staff.

A central implication is that mandatory digital authentication should not be the only route to entitlement. Social protection systems need fallback procedures, including manual verification, one-time passwords, community-based verification, temporary authorization, and offline

transaction records that can later be reconciled. These mechanisms should be governed by clear rules that protect against fraud without making exceptions so difficult that eligible people are excluded. The appropriate standard is not perfect technological accuracy but reliable access to entitlements under imperfect real-world conditions.

Data Governance, Privacy, and Accountability

The third dimension concerns how identity data are collected, stored, shared, and used. Digital identity systems often involve centralized databases, biometric records, and links between social registries, financial accounts, and service platforms. These linkages can improve coordination, but they also increase the stakes of data errors, security breaches, and unauthorized access. Citizens may be unable to understand how their information is used, who can access it, or how to correct inaccurate records. Such opacity can undermine trust and make people reluctant to enroll, particularly where state institutions have historically been perceived as coercive or unresponsive.

Masiero and Bailur (2021) argue that digital identity raises questions of justice because identification systems shape who is recognized by the state and who can exercise rights. Data justice requires attention not only to privacy but also to the fairness of data collection, the accuracy of records, the transparency of decision-making, and the ability of individuals to contest adverse decisions. In social protection, these issues are particularly acute because an incorrect record may determine whether a household receives food, cash, health care, or a pension.

Accountability is therefore not an optional complement to digital identity; it is a condition of legitimate administration. Governments need clear legal frameworks governing consent, purpose limitation, data minimization, security, retention, correction, and redress. They also need accessible mechanisms through which citizens can challenge mismatches, incorrect eligibility classifications, or wrongful exclusion. Without such mechanisms, digital systems may shift power toward technical administrators and away from citizens, even when the stated objective is improved service delivery.

Administrative Capacity, Discretion, and Implementation

The fourth dimension concerns the capacity of public organizations to implement digital identity systems effectively. Digitalization requires more than software and hardware. It requires trained staff, functioning devices, reliable connectivity, interoperable databases, clear procedures, and resources for maintenance and support. Where these conditions are absent, digital systems may increase workload, produce errors, and shift unresolved problems to frontline workers and citizens.

Street-level bureaucracy theory helps explain why implementation capacity is decisive. Frontline staff must interpret rules and respond to situations that automated systems cannot resolve. Their discretion can protect access when they are authorized and able to use alternatives, but it can also produce inconsistent treatment when guidance is unclear or

resources are inadequate. The literature on Aadhaar shows that exclusion is shaped not only by biometric technology but also by the organizational rules governing authentication attempts, manual verification, and the resolution of mismatches (Masiero, 2020b; Masiero & Shakthi, 2020).

The synthesis therefore suggests that digital identity reforms should be evaluated as administrative reforms rather than purely technical projects. Successful implementation requires investment in human capacity, service design, monitoring, and citizen support. It also requires realistic recognition that some users will need assistance to navigate digital systems. Digital literacy programs, help desks, community intermediaries, and accessible complaint channels can reduce the burden placed on vulnerable users and improve the equity of service delivery.

Integrated Assessment of Digital Identity and Exclusion

The four dimensions can be combined into an integrated framework for assessing digital identity reforms in social protection. Table 1 summarizes the main exclusion risks, their administrative mechanisms, and possible mitigation strategies.

Table 1. *Digital identity, administrative exclusion, and mitigation strategies in social protection delivery*

Analytical dimension	Main exclusion risk	Policy and administrative response
Enrolment and documentation	Missing civil records, costly or distant enrolment, lack of acceptable documents, gendered and disability-related barriers	Invest in civil registration, mobile and assisted enrolment, fee waivers, alternative evidence, and simplified correction procedures
Authentication and service access	Biometric failure, connectivity interruptions, device malfunction, repeated travel, denial of entitlement when digital verification fails	Provide manual verification, offline procedures, temporary authorisation, multiple authentication methods, and clear fallback rules
Data governance and accountability	Inaccurate records, opaque data use, security risks, limited ability to correct errors or contest decisions	Establish data-protection law, purpose limitation, correction rights, accessible grievance mechanisms, and independent oversight
Administrative capacity and implementation	Inadequate staff training, rigid rules, weak interoperability, insufficient maintenance, uneven frontline discretion	Train staff, clarify exception procedures, fund maintenance, monitor user experience, and support frontline discretion within accountable rules

The framework is intended to support policy analysis and program design rather than to provide a fixed checklist. Its central premise is that digital identity should be assessed according to whether it expands meaningful access to entitlements for the populations it is intended to serve.

DISCUSSION

The findings show that the relationship between digital identity and exclusion is conditional. Digital identity can improve social protection delivery when it is embedded in an inclusive identification ecosystem, supported by reliable fallback procedures, governed by strong data-protection rules, and implemented by adequately resourced frontline organizations. It can undermine access when it becomes a rigid precondition for entitlement without alternatives, when foundational registration is weak, or when citizens lack effective means to correct errors and seek redress. The policy challenge is therefore not to choose between digital and non-digital administration, but to design hybrid systems that combine digital efficiency with administrative flexibility.

These findings extend earlier research on the developmental potential of digital identity. Gelb and Clark (2013) and the International Monetary Fund (2022) emphasize that digital identification can improve targeting, reduce duplication, and support the delivery of benefits at scale. The present review does not dispute these potential gains. Rather, it shows that they are conditional. Digital systems may reduce certain administrative errors, but they may also generate new exclusion errors when users cannot enroll, authenticate, or resolve mismatches. The relevant question is therefore not whether digital identity improves administrative performance in general, but for whom and under what institutional conditions.

The findings also support the critical argument that digital identity systems are not neutral instruments of administration. Masiero and Bailur (2021) show that identification systems shape recognition, rights, and access to services. The present analysis develops this argument by showing that exclusion may arise at different stages of the delivery chain. A person may be excluded before reaching a service point because they cannot obtain a document; at the service point because biometric authentication fails; or after the service point because they cannot correct an erroneous record. This broader view makes visible forms of exclusion that narrow measures of authentication success may conceal.

The role of frontline staff is central to this interpretation. Lipsky (1980) argued that street-level bureaucrats exercise discretion because policy rules cannot anticipate every practical situation. The evidence reviewed here suggests that digitalization does not remove this discretion. Instead, it redistributes it. Automated systems may standardize some decisions, but frontline staff still decide how to respond to failed authentication, missing documents, connectivity interruptions, and mismatched records. Where staff have clear authority to use alternatives, digital identity systems may become more inclusive. Where staff are constrained by rigid rules or audit pressures, technical failure may become a denial of entitlement.

The findings also have implications for how governments measure the success of digital identity reforms. Enrolment coverage, authentication rates, and reductions in duplicate records are important indicators, but they are insufficient. Policymakers should also measure denial rates, time and cost of resolving errors, availability of fallback options, grievance resolution, user satisfaction, and access among historically marginalized groups. A system may appear efficient in aggregate while performing poorly for the populations most dependent on social protection. Equity-oriented monitoring is therefore necessary to prevent digital identity reforms from concealing exclusion behind aggregate performance indicators.

The findings also have theoretical implications. They support a view of digital government in which technology, organizations, and citizens are mutually constitutive. Digital identity systems do not simply transmit policy decisions; they reshape the conditions under which citizens can make claims and under which officials can respond. This perspective aligns with street-level bureaucracy theory by showing that discretion remains central even in highly standardized digital environments. It also extends data-justice scholarship by showing that exclusion may arise not only from unequal access to technology but also from the institutional rules that determine when technological failure becomes a denial of rights.

Several methodological limitations qualify these conclusions. The review relies on published research and institutional documents, which may overrepresent well-studied programs such as India's Aadhaar and underrepresent contexts with weaker research infrastructure. The review also cannot establish causal effects across countries because the included studies use different designs, measures, and settings. In addition, the rapid evolution of digital identity technology means that findings may require updating as governments adopt new authentication methods, interoperability standards, and data-governance frameworks. These limitations do not undermine the central argument, but they indicate that the framework should be applied contextually rather than treated as a universal template

CONCLUSION

This article examined the relationship between digital identity infrastructure and administrative exclusion in social protection delivery in developing countries. The integrative review shows that digital identity can improve administrative coordination, support verification, and strengthen the traceability of social assistance. These potential benefits are important in contexts where governments seek to expand coverage, reduce leakage, and respond rapidly to shocks. However, the evidence also shows that digital identity systems can create new barriers to access when enrolment is difficult, authentication fails, data records are inaccurate, or frontline staff lack the capacity and authority to provide alternatives.

The central contribution of the article is an integrated framework that treats administrative exclusion as a process spanning enrolment, authentication, data governance, and frontline implementation. This framework challenges the assumption that digital identity is inherently inclusive or inherently exclusionary. Its effects depend on institutional design, implementation capacity, and the availability of meaningful alternatives when digital systems fail. Digital identity should therefore be understood as a governance reform with distributional consequences, not simply as a technical upgrade to public administration.

Future research should use comparative and mixed-methods approaches to examine how digital identity systems affect access to social protection across different institutional, technological, and socioeconomic contexts. Research should pay particular attention to women, rural populations, persons with disabilities, displaced people, older adults, and informal workers. Studies should also examine the effects of fallback procedures, grievance mechanisms, and frontline discretion on equitable access to benefits.

For policy, the central recommendation is that digital identity reforms should be designed with inclusion as a primary objective rather than as a secondary safeguard. Governments should

ensure that no eligible person loses access to essential social protection solely because of a digital authentication failure. This requires investment in civil registration, accessible enrolment, reliable fallback procedures, data protection, grievance redress, and frontline capacity. Digital identity can support equitable social protection, but only when public administration treats access to entitlements as a core measure of successful implementation.

Policy Implications

First, governments should treat civil registration and identity enrolment as prerequisites for inclusive digital social protection. Digital systems should not be introduced as mandatory gateways before the underlying identification ecosystem can reach vulnerable populations. Mobile enrolment units, fee waivers, simplified documentation rules, and community-based registration can reduce barriers for people who are otherwise difficult to reach.

Second, social protection programs should institutionalize fallback verification procedures. Manual verification, alternative credentials, temporary authorization, and offline reconciliation should be available when biometric authentication or connectivity fails. These procedures must be governed by clear rules that balance fraud prevention with the need to protect access to entitlements.

Third, data governance should be strengthened before digital identity systems are scaled. Legal frameworks should specify purposes for data use, limits on sharing, security requirements, correction rights, retention periods, and independent oversight. Citizens should be able to understand how their data are used and challenge decisions that affect their access to benefits.

Fourth, public administrations should invest in frontline capacity. Staff need training, authority, time, and resources to resolve authentication failures and assist citizens with digital procedures. Performance management should reward equitable access and effective problem resolution, not only transaction volume or authentication success.

Fifth, monitoring systems should measure exclusion as well as efficiency. Governments should collect disaggregated data on denial rates, authentication failures, grievance resolution, time taken to correct errors, and access among marginalized groups. This would allow policymakers to identify exclusion risks early and adjust implementation before they become systemic.

REFERENCES

Arora, P. (2019). *The next billion users: Digital life beyond the West.* Harvard University Press.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.1177/1468794108098068

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Chaudhuri, B. (2020). Distant, opaque and seamful: Seeing the state through the workings of Aadhaar in India. *Information Technology for Development, 27*(1), 37–49. https://doi.org/10.1080/02681102.2020.1734184

Gelb, A., & Clark, J. (2013). *Identification for development: The biometrics revolution (Working Paper No. 315).* Center for Global Development. https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315

Gurstein, M. (2003). Effective use: A community informatics strategy beyond the digital divide. *First Monday, 8*(12). https://doi.org/10.5210/fm.v8i12.1107

Heeks, R. (2018). *Information and communication technology for development (ICT4D).* Routledge. https://doi.org/10.4324/9781315645827

International Monetary Fund. (2022). *Digitalization and social protection: Macro and micro lessons for Vietnam (Working Paper No. 2022/185).* https://www.elibrary.imf.org/view/journals/001/2022/185/article-A001-en.xml

Krishna, S. (2020). Digital identity, datafication and social justice: Understanding Aadhaar use among informal workers in south India. *Information Technology for Development, 27(*1), 67–90. https://doi.org/10.1080/02681102.2020.1800582

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences.* SAGE Publications.

Lipsky, M. (1980). *Street-level bureaucracy: Dilemmas of the individual in public services.* Russell Sage Foundation.

Masiero, S. (2020a). COVID-19: What does it mean for digital social protection? *Big Data & Society, 7*(2), 1–6. https://doi.org/10.1177/2053951720978995

Masiero, S. (2020b). Biometric infrastructures and the Indian Public Distribution System. *South Asia Multidisciplinary Academic Journal, 23,* 1–22. https://doi.org/10.4000/samaj.6459

Masiero, S., & Bailur, S. (2021). Digital identity for development: The quest for justice and a research agenda. *Information Technology for Development, 27*(1), 1–12. https://doi.org/10.1080/02681102.2021.1859669

Masiero, S., & Shakthi, S. (2020). Grappling with Aadhaar: Biometrics, social identity and the Indian state. *South Asia Multidisciplinary Academic Journal, 23,* 1–8. https://doi.org/10.4000/samaj.6279

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, Article n71. https://doi.org/10.1136/bmj.n71

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104,* 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

World Bank. (2016). *World development report 2016: Digital dividends.* https://doi.org/10.1596/978-1-4648-0671-1

World Bank. (2020). *The state of identification systems in Africa: Country briefs.* https://openknowledge.worldbank.org/entities/publication/5bff75ca-beaf-5181-81e8-310eaa2e2019

World Bank. (2024). Identification for Development (ID4D) and digitalizing G2P payments (G2Px) 2023 annual report. https://documents1.worldbank.org/curated/en/099647503042425828/pdf/IDU-a9d1a6be-30dc-48e6-9318-cf9d26959fb9.pdf

World Bank. (2025). ID4D global dataset 2025: Trends in identification for development. https://openknowledge.worldbank.org/entities/publication/3c36d203-5ed0-419c-84df-3cc850f242e4