DIGITAL IDENTITY ECOSYSTEM

Digital Identity Systems in India: Assessing Citizen Inclusion, Privacy and Governance Effectiveness

S. Shobana[1], K. Shobana[2], R. Kanakarathinam[3]

[1]Department of Commerce and Management, Kamalam College of Arts and Science, Udumalpet, India
[2]Department of BBA (Logistics and Aviation Management), Nehru Arts and Science College, Coimbatore, India
[3]Department of Commerce, Akshaya College of Arts and Science, Coimbatore, India

Published November 2026

Abstract

India's digital identity ecosystem is among the largest implementations of Digital Public Infrastructure (DPI) in the world. Anchored by Aadhaar and complemented by the Unified Payments Interface (UPI), DigiLocker and the Data Empowerment and Protection Architecture (DEPA), it aims to improve public service delivery, deepen financial inclusion and strengthen transparency in governance. Alongside these gains, the system has raised persistent concerns about data privacy, authentication-related exclusion and public trust. This study examines India's digital identity system from a citizen-centric perspective, covering accessibility, financial and digital inclusion, privacy and trust, governance effectiveness and adoption challenges. A descriptive cross-sectional survey was conducted among 200 adult users of DPI services in Coimbatore District, Tamil Nadu, selected through multistage stratified random sampling. Data were analyzed using descriptive statistics, mean-score ranking, the Garrett ranking technique, Cronbach's alpha and Spearman's rank-order correlation. The instrument showed high internal consistency (overall $\alpha = 0.90$), and the mean-score and Garrett rankings of the accessibility items agreed closely ($\rho = 0.975$). Respondents reported that digital identity platforms have substantially improved access to services, transparency and participation in digital payments, with UPI receiving the strongest endorsement. Comparatively lower scores for authentication reliability (mean = 3.86), privacy protection through authentication (3.77) and the effectiveness of grievance redressal (3.45), together with strong support for data protection laws (4.16), indicate that citizen trust remains conditional. The study concludes that the long-term legitimacy of India's digital identity architecture depends on effective enforcement of data protection, inclusive design for digitally marginalized groups and responsive, accountable grievance mechanisms.

Keywords: digital identity; Aadhaar; digital public infrastructure; data privacy; governance effectiveness; financial inclusion; Garrett ranking

1 Introduction

Digital identity has become a foundational instrument of modern governance. It allows the state to verify individuals reliably, deliver services at scale and direct benefits to intended recipients (Gelb & Clark, 2013; World Bank, 2019). In India, digital identity has evolved into the core layer of a wider Digital Public Infrastructure (DPI) that supports service delivery across a society marked by wide demographic and socioeconomic diversity (NITI Aayog, 2020; World Bank, 2021).

Aadhaar, the biometric-based identity system administered by the Unique Identification Authority of India, provides residents with a unique identifier that is now used to access welfare schemes, financial services and digital platforms (UIDAI, 2022). It is complemented by the Unified Payments Interface (UPI) for real-time digital payments (Reserve Bank of India, 2022), DigiLocker for the stor-

age and verification of documents, and the Data Empowerment and Protection Architecture (DEPA) for consent-based data sharing (MeitY, 2023). Together, these layers have changed how citizens interact with the state, shifting many routine transactions from paper and physical visits to authenticated digital channels (NITI Aayog, 2023).

These achievements have been accompanied by sustained debate about privacy, exclusion and data security. Biometric authentication failures, the persistent digital divide and perceptions of state surveillance have been documented in both scholarly and policy literature (Khera, 2017; Srinivasan et al., 2018). The legal environment has also changed substantially: the Supreme Court recognized privacy as a fundamental right in 2017 and upheld Aadhaar subject to proportionality safeguards in 2018, Parliament enacted the Digital Personal Data Protection (DPDP) Act in 2023, and the DPDP Rules were notified in November 2025 (Government of India, 2023; MeitY, 2025). As the new data protection regime is implemented, evidence on how citizens themselves experience and trust digital identity systems is especially timely.

Against this background, the present study offers a citizen-centric assessment of India's digital identity system. Using primary survey data from Coimbatore District, Tamil Nadu, it examines how users perceive the system's contribution to service accessibility, financial and digital inclusion, privacy and trust, and governance effectiveness, and what challenges they face in using it. The remainder of the paper is organized as follows. Section 2 reviews the literature and identifies the research gap. Section 3 presents the conceptual framework and objectives. Section 4 describes the methodology, and Section 5 reports the results. Section 6 discusses the findings, Section 7 summarizes them, and Sections 8 to 10 present the conclusion, policy implications, limitations and directions for future research.

2 Literature review

Research on digital identity systems has grown alongside their rapid adoption. Studies of India's DPI, which includes Aadhaar, UPI, DigiLocker and consent-based data-sharing frameworks, broadly agree that these platforms have widened inclusion and improved administrative efficiency, while also raising questions about privacy, surveillance and exclusion. Public trust and digital literacy recur as conditions that shape adoption, and governance outcomes are linked to platform interoperability and ease of use. This review is organized around four themes that inform the study's conceptual framework.

2.1 Digital identity, service delivery and welfare

Gelb and Clark (2013) examined national identification systems in developing countries and found that digital identity can curb leakages in welfare programs and improve administrative efficiency, provided that institutional capacity and citizen trust are strong. Evidence from e-governance reforms in India points in a similar direction. In a large field experiment on the national rural employment program in Bihar, Banerjee et al. (2020) showed that replacing advance fund transfers with electronic, just-in-time payments reduced leakages and program expenditure, although payment delays increased. Such findings show that digitization can improve accountability while creating new frictions for beneficiaries.

Studies focusing on Aadhaar itself report a similar mix of gains and costs. Abraham et al. (2018) documented the wide uptake of Aadhaar in access to state services, while drawing attention to the risks associated with centralized data collection and the need for stronger legal protection. Khera (2017),

in a critical assessment of Aadhaar-based welfare delivery, highlighted exclusion errors affecting marginalized populations and argued that technological efficiency should not take precedence over welfare entitlements, calling for alternative authentication options to safeguard inclusion.

2.2 Financial and digital inclusion

The World Bank (2019) assessed digital identification systems globally, including Aadhaar, and concluded that digital identity can substantially enhance financial inclusion and service access when supported by interoperable platforms; it also identified data protection and consent as central to public trust. Examining India's digital financial infrastructure, D'Silva et al. (2019) showed how the combination of Aadhaar-linked bank accounts and interoperable payment rails such as UPI accelerated the spread of digital payments, including among lower-income groups, and stressed the importance of ease of use and interoperability. GSMA (2020) similarly reported that digital identity strengthens inclusion most where mobile penetration is high, and identified privacy-by-design as essential to user confidence. At the policy level, NITI Aayog (2020) reported improvements in service delivery, cost reduction and transparency under India's DPI framework, while recommending wider digital literacy programs to address the digital divide.

2.3 Privacy, trust and the legal framework

Concerns about privacy and data use have run alongside the expansion of digital identity. Srinivasan et al. (2018) examined the privacy trade-offs that low-income users make when dealing with identity systems such as Aadhaar and found preliminary evidence of distinct concerns arising from the networked nature of these systems. Ramanathan (2020) reported moderate trust in the government's handling of personal data, coupled with low awareness of consent mechanisms, and concluded that transparency strongly influences citizen acceptance. Narayanan (2021) analyzed data governance in India's digital identity framework, highlighting risks of data misuse and function creep and recommending decentralized architectures and stronger regulatory oversight.

The legal framework has evolved in response to these concerns. In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), a nine-judge bench of the Supreme Court recognized privacy as a fundamental right. In the subsequent Aadhaar judgment (Puttaswamy (Aadhaar), 2019), a five-judge bench upheld the Aadhaar scheme subject to the principles of proportionality, consent and data minimization, while limiting its mandatory use in certain contexts. These judgments now underpin the governance of digital identity in India, and the DPDP Act, 2023, together with the DPDP Rules, 2025, provides the statutory framework for consent, data fiduciary obligations and enforcement through the Data Protection Board (Government of India, 2023; MeitY, 2025).

2.4 Platforms, governance and accountability

A further strand of literature treats digital identity as a platform for state capacity. Bharadwaj et al. (2013) conceptualized digital platforms as catalysts for organizational transformation, a perspective relevant to DPI because it shows how platform ecosystems raise efficiency while depending on trust and institutional safeguards. Masiero and Bailur (2021) framed digital identity as a means of advancing human development and called for attention to the justice implications of identity systems, including who benefits and who is excluded. The OECD (2021), reviewing digital government strategies, likewise identified citizen trust, transparency, inclusive design and accountability mechanisms as conditions for the long-term effectiveness of digital identity systems.

2.5 Research gap

Existing research has examined India's digital identity system largely from policy, legal or system-level perspectives, focusing on service delivery efficiency, financial inclusion and governance reform. Comparatively few studies evaluate the system empirically from the citizen's point of view.

Four specific gaps motivate this study. First, although improved access to public services is widely acknowledged, few studies analyze how accessibility, interoperability and ease of use together shape citizen satisfaction and service use. Second, research on financial inclusion emphasizes adoption outcomes and gives less attention to enabling conditions such as digital literacy, awareness and trust in government technology. Third, privacy and data protection are discussed extensively in legal and theoretical work, but survey evidence on citizens' privacy perceptions and their relationship with trust and use is limited. Fourth, governance effectiveness is usually assessed through administrative indicators rather than citizens' perceptions of transparency, accountability and responsiveness, and few studies examine these dimensions together within a single framework.

This study addresses these gaps through a citizen-centric empirical assessment that brings accessibility, inclusion, privacy, trust and governance effectiveness into one conceptual framework for India's digital identity system.

3 Conceptual framework and research objectives

3.1 Conceptual framework

The conceptual framework (Figure 1) situates India's digital identity system within the wider DPI ecosystem. Aadhaar, together with UPI, DigiLocker and the consent-based DEPA, forms the core infrastructure. The independent variables are digital identity accessibility, platform interoperability, ease of use and assurance of data privacy and security. The mediating variables are citizen awareness, digital literacy, trust in government technology and privacy perception, which shape how effectively citizens engage with identity-enabled services. The dependent variables are public service utilization, financial inclusion outcomes, citizen satisfaction and perceived governance effectiveness. The framework posits that higher awareness, trust and literacy strengthen the positive relationship between DPI and governance outcomes, whereas deficits in these factors weaken accessibility and inclusion. In the present study, the framework guides the design of the instrument and the interpretation of results; formal testing of the mediating relationships is identified as a direction for future research (Section 10).

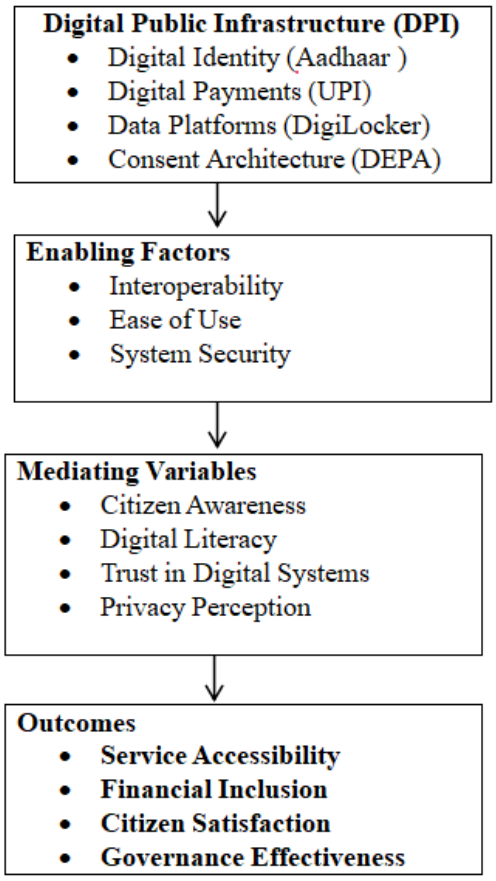


Figure 1. Conceptual framework of the study

3.2 Research objectives

- To examine the role of India's digital identity system in enhancing access to public services.
- To analyze the impact of digital identity on financial and digital inclusion.
- To assess citizen trust and privacy perceptions related to digital identity platforms.
- To evaluate the contribution of digital identity systems to governance efficiency and transparency.
- To identify the challenges faced by citizens in adopting digital identity-enabled services.

4 Materials and methods

The study used a descriptive, cross-sectional research design. A structured questionnaire was administered to assess citizens' perceptions of India's digital identity system across five thematic constructs aligned with the research objectives.

4.1 Study area

The study was conducted in Coimbatore District, Tamil Nadu, which includes urban, semi-urban and rural communities with diverse socioeconomic profiles. As a major industrial and educational center, the district has wide access to digital services, including Aadhaar-based authentication, UPI transactions and e-governance platforms. This makes it a suitable setting for examining citizen perceptions across different demographic groups and levels of digital literacy.

4.2 Target population and sampling unit

The target population comprised adult residents (aged 18 years and above) of Coimbatore District who had used at least one DPI service, such as Aadhaar, UPI, DigiLocker or another Aadhaar-linked government service. The individual citizen was the sampling unit. The sampling frame was drawn from electoral rolls, municipal ward lists and village-level household listings in the selected urban, semi-urban and rural areas.

4.3 Sampling technique

A multistage stratified random sampling technique was used. First, the district was stratified into urban, semi-urban and rural areas to ensure regional representation. Second, sampling units within each stratum were selected by simple random sampling: corporation wards in urban areas, town panchayats in semi-urban areas and villages in rural areas. Third, households within the selected units were chosen by systematic random sampling. Finally, one eligible respondent per household was selected using the Kish Grid method. This procedure ensured proportional representation across strata and reduced selection bias.

4.4 Sample size and period of study

The sample comprised 200 respondents allocated proportionately across strata: 80 (40%) from urban areas, 70 (35%) from semi-urban areas and 50 (25%) from rural areas. This sample size was considered adequate for descriptive analysis, reliability testing and rank-based comparison. Data were collected over a period of three months, allowing sufficient time for fieldwork and response validation. Table 1 summarizes the sampling design.

Table 1. Sampling design for the study (Coimbatore District)

S.No	Sampling Component	Description
1	Study Area	Coimbatore District, Tamil Nadu
2	Target Population	Adult citizens (18 years and above) residing in Coimbatore District
3	Sampling Unit	Individual citizen using at least one Digital Identity / DPI service
4	Sampling Frame	Residents from selected Urban, Semi-Urban, and Rural areas of Coimbatore District
5	Sampling Technique	Multistage Stratified Random Sampling
6	Stratification Criteria	Area of residence: Urban, Semi-Urban, Rural
7	Selection of Areas	Random selection of Corporation wards, Town Panchayats, and Villages
8	Household Selection	Systematic Random Sampling
9	Respondent Selection	Kish Grid Method (one respondent per household)
10	Sample Size	200 respondents
11	Sample Allocation	Urban – 80 (40%); Semi-Urban – 70 (35%); Rural – 50 (25%)
12	Data Collection Method	Structured Questionnaire
13	Period of Study	Three months
14	Inclusion Criteria	Citizens with experience using Aadhaar, UPI, DigiLocker, or DPI services
15	Exclusion Criteria	Individuals below 18 years and those with no exposure to digital identity services

4.5 Research instrument and validity

The questionnaire contained a demographic section and five Likert-scale constructs: Digital Identity Accessibility, Financial and Digital Inclusion, Privacy, Security and Trust, Challenges and Policy Perspectives, and Overall Satisfaction and Future Outlook. Each construct comprised five items rated on a five-point scale from Strongly Agree to Strongly Disagree. Content validity was established through a review of the literature and evaluation by experts in information systems, public administration and digital governance. Construct validity was supported by aligning each item with its intended construct, and face validity was confirmed through a pilot survey, which led to minor wording refinements.

The first three constructs correspond directly to Objectives 1 to 3, and the Challenges and Policy Perspectives construct corresponds to Objective 5. Objective 4 (governance efficiency and transparency) is assessed through a synthesis of governance-related items drawn from the other constructs, namely transparency in service delivery, authentication reliability, trust in government data handling and the effectiveness of grievance redressal (Section 5.6). The Overall Satisfaction and Future Outlook construct captures citizens' overall evaluation of the system.

4.6 Statistical tools used

Descriptive statistics (frequency, percentage and mean score) were used to profile respondents and summarize perceptions for each construct. Likert responses were weighted from 5 (Strongly Agree) to 1 (Strongly Disagree) to compute total and mean scores for ranking items within each construct. As a complementary ranking procedure, the Garrett ranking technique was applied by assigning Garrett scale values to the five response categories (see Table 6) and ranking items by their total Garrett scores. Cronbach's alpha was computed to assess internal consistency at the construct and overall scale levels. Finally, Spearman's rank-order correlation between the mean-score ranking and the Garrett ranking was computed as a check on the consistency of the two ranking procedures. Data were processed using spreadsheet-based analysis compatible with SPSS.

5 Results

5.1 Reliability of the research instrument

Internal consistency was assessed using Cronbach's alpha for each of the five constructs and for the overall scale. As shown in Table 2, all constructs exceeded the accepted minimum of 0.70, with values ranging from 0.79 to 0.88. The overall scale achieved an alpha of 0.90, indicating excellent reliability.

Table 2. Reliability analysis using Cronbach's alpha

S.No	Construct	No. of Items	Cronbach's Alpha	Interpretation
1	Digital Identity Accessibility	5	0.84	Good Reliability
2	Financial & Digital Inclusion	5	0.86	Good Reliability
3	Privacy, Security & Trust	5	0.81	Good Reliability
4	Challenges & Policy Perspectives	5	0.79	Acceptable Reliability
5	Overall Satisfaction & Future Outlook	5	0.88	High Reliability
6	Overall Scale	25	0.90	Excellent Reliability

Source: Primary data.

5.2 Demographic profile of respondents (N = 200)

Table 3. Demographic profile of respondents

Variable	Category	Number of Respondents	Percentage (%)
Gender	Male	104	52.0
	Female	92	46.0
	Others	4	2.0
	Total	**200**	**100.0**
Age Group			
	18–25	38	19.0
	26–35	64	32.0
	36–45	46	23.0
	46–55	34	17.0
	Above 55	18	9.0
	Total	**200**	**100.0**
Area of Residence			
	Rural	50	25.0
	Semi-Urban	70	35.0
	Urban	80	40.0
	Total	**200**	**100.0**
Educational Qualification			
	School Level	28	14.0
	Undergraduate	62	31.0
	Postgraduate	78	39.0
	Doctorate	32	16.0
	Total	**200**	**100.0**
Occupation			
	Student	36	18.0
	Government Employee	44	22.0
	Private Employee	62	31.0
	Self-Employed	38	19.0
	Others	20	10.0
	Total	**200**	**100.0**

Source: Primary data.

The gender distribution was relatively balanced: 52.0% of respondents were male, 46.0% female and 2.0% identified with other gender categories. The largest age group was 26–35 years (32.0%), followed by 36–45 years (23.0%), indicating that working-age adults form the main segment of users

while all age groups are represented. Urban residents accounted for 40.0% of the sample, semi-urban residents for 35.0% and rural residents for 25.0%, reflecting the stratified design. Most respondents held postgraduate (39.0%) or undergraduate (31.0%) qualifications, and 16.0% held doctorates; the sample is therefore more highly educated than the general population, which should be considered when interpreting the results (see Section 10). Private employees formed the largest occupational group (31.0%), followed by government employees (22.0%) and the self-employed (19.0%).

Table 4. Frequency of using digital services

Frequency	Number of Respondents	Percentage (%)
Daily	96	48.0
Weekly	54	27.0
Occasionally	36	18.0
Rarely	14	7.0
Total	200	100.0

Source: Primary data.

Nearly half of the respondents (48.0%) used digital services daily and a further 27.0% used them weekly, indicating a high level of familiarity with digital identity-enabled platforms.

5.3 Digital identity accessibility (Objective 1)

This section addresses Objective 1: to examine the role of India's digital identity system in enhancing access to public services. Table 5 presents the distribution of responses, and Table 6 presents the mean-score and Garrett rankings.

Table 5. Perception of respondents on digital identity accessibility

Statement	SA	A	N	DA	SDA	Total
Aadhaar has made access to government services easier	88	72	22	12	6	200
Digital identity reduces the need for physical documentation	84	76	20	14	6	200
Digital platforms save time in accessing public services	90	70	18	14	8	200
Authentication through Aadhaar is reliable and convenient	72	68	30	20	10	200
Digital identity improves transparency in service delivery	86	74	24	10	6	200

Source: Primary data. SA - Strongly Agree; A - Agree; N - Neutral; DA - Disagree; SDA - Strongly Disagree.

Respondents held strongly favorable views of digital identity as a means of accessing public services. Four of the five statements received agreement (Strongly Agree or Agree) from 80.0% of respondents, including the statements that Aadhaar has made access to government services easier, that digital identity reduces the need for physical documentation and that digital platforms save time. The statement on authentication reliability received lower agreement (70.0%) and the highest share of neutral and disagreeing responses (30.0%), suggesting occasional difficulties with biometric authentication or system availability.

Table 6. Mean score, ranking and Garrett ranking - digital identity accessibility

Statement	Total Score	Mean Score	Rank	Garrett Score	Garrett Rank
Aadhaar has made access to government services easier	824	4.12	I*	14096	II
Digital identity reduces the need for physical documentation	818	4.09	IV	14018	IV
Digital platforms save time in accessing public services	820	4.10	III	14030	III
Authentication through Aadhaar is reliable and convenient	772	3.86	V	13364	V
Digital identity improves transparency in service delivery	824	4.12	I*	14102	I

Source: Primary data. Likert weights: SA = 5, A = 4, N = 3, DA = 2, SDA = 1. Garrett scale values: SA = 82, A = 70, N = 55, DA = 40, SDA = 25. *Tied rank (a rank of 1.5 is used for both items in the Spearman computation).

The statements "Aadhaar has made access to government services easier" and "Digital identity improves transparency in service delivery" jointly recorded the highest mean score (4.12). Time savings ranked next (4.10), followed by reduced need for physical documentation (4.09). Authentication reliability recorded the lowest mean score (3.86) and was also ranked last under the Garrett procedure. The Garrett ranking separated the two top items by a very small margin (14,102 against 14,096), placing transparency first; the two items should therefore be regarded as jointly the most valued benefits. Overall, citizens see digital identity primarily as a means of easier and more transparent access to services, with authentication reliability as the main area for improvement.

5.4 Financial and digital inclusion (Objective 2)

This section addresses Objective 2: to analyze the impact of digital identity on financial and digital inclusion.

Table 7. Perception of respondents on financial and digital inclusion

Statement	SA	A	N	DA	SDA	Total
Aadhaar has helped me access banking services easily	86	70	24	14	6	200
UPI has improved my participation in the digital economy	92	68	20	12	8	200
Digital payments are affordable and easy to use	88	72	18	14	8	200
DigiLocker reduces dependence on physical documents	82	74	26	12	6	200
Digital identity systems promote financial inclusion for all	78	76	28	12	6	200

Source: Primary data.

Table 8. Mean score and ranking - financial and digital inclusion

Statement	Total Score	Mean Score	Rank
Aadhaar has helped me access banking services easily	816	4.08	III
UPI has improved my participation in the digital economy	824	4.12	I
Digital payments are affordable and easy to use	818	4.09	II

Statement	Total Score	Mean Score	Rank
DigiLocker reduces dependence on physical documents	814	4.07	IV
Digital identity systems promote financial inclusion for all	808	4.04	V

Source: Primary data.

Perceptions of DPI's role in financial inclusion were highly favorable, with all five items scoring above 4.0. UPI recorded the highest mean score (4.12) and the largest share of strong agreement (46.0%), underlining its role in widening participation in the digital economy through instant, low-cost and easy-to-use payments. The affordability and ease of digital payments (4.09) and Aadhaar-enabled access to banking (4.08) followed closely, and DigiLocker was valued for reducing reliance on physical documents (4.07). The statement that digital identity promotes financial inclusion "for all" ranked lowest (4.04) and drew a relatively high share of neutral responses (14.0%), suggesting that some groups still face barriers related to digital literacy or connectivity.

5.5 Privacy, security and trust (Objective 3)

This section addresses Objective 3: to assess citizen trust and privacy perceptions related to digital identity platforms.

Table 9. Perception of respondents on privacy, security and trust

Statement	SA	A	N	DA	SDA	Total
My personal data is safe in digital identity systems	64	70	36	20	10	200
Aadhaar-based authentication protects user privacy	60	72	40	18	10	200
I trust government agencies to handle my digital data responsibly	68	74	34	16	8	200
I am concerned about misuse of my digital identity data	78	66	28	18	10	200
Strong data protection laws are necessary for digital identity systems	92	70	22	10	6	200

Source: Primary data.

Table 10. Mean score and ranking - privacy, security and trust

Statement	Total Score	Mean Score	Rank
My personal data is safe in digital identity systems	758	3.79	IV
Aadhaar-based authentication protects user privacy	754	3.77	V
I trust government agencies to handle my digital data responsibly	778	3.89	III
I am concerned about misuse of my digital identity data	784	3.92	II
Strong data protection laws are necessary for digital identity systems	832	4.16	I

Source: Primary data.

Perceptions of privacy, security and trust were positive but cautious, and this construct recorded the lowest mean scores of the five. Around two-thirds of respondents agreed that their personal data are safe (67.0%) and that Aadhaar-based authentication protects privacy (66.0%), while the remaining third were neutral or disagreed. The need for strong data protection laws recorded the highest mean score (4.16), and concern about misuse of digital identity data ranked second (3.92). Trust in government agencies to handle data responsibly was moderate (3.89). The lowest score was for the

statement that Aadhaar-based authentication protects user privacy (3.77). Taken together, these results show that citizens accept and use the system while remaining clearly aware of its privacy risks, and that privacy assurance requires further policy attention.

5.6 Governance effectiveness (Objective 4)

This section addresses Objective 4: to evaluate the contribution of digital identity systems to governance efficiency and transparency. As explained in Section 4.5, governance effectiveness is assessed through governance-related items drawn from the accessibility, privacy and challenges constructs. Table 11 brings these indicators together.

Table 11. Citizen perceptions of governance-related indicators

Governance indicator (source table)	Mean Score	Agreement (%)	Rank
Digital identity improves transparency in service delivery (Table 5)	4.12	80.0	I
I trust government agencies to handle my digital data responsibly (Table 9)	3.89	71.0	II
Authentication through Aadhaar is reliable and convenient (Table 5)	3.86	70.0	III
Existing grievance redressal mechanisms are effective (Table 12)	3.45	55.0	IV

Source: Primary data. Agreement = Strongly Agree + Agree.

The governance indicators reveal a clear gradient. Transparency in service delivery is rated highly (4.12; 80.0% agreement), indicating that citizens see digital identity as making service delivery more visible and less discretionary. Trust in government data handling (3.89) and authentication reliability (3.86) are moderate. The effectiveness of grievance redressal receives the lowest score (3.45), with only 55.0% agreement and 25.0% disagreement. Citizens therefore credit digital identity with improving the transparency and efficiency of front-end service delivery, but they view the institutional mechanisms that respond to failures and complaints as considerably weaker.

5.7 Challenges and policy perspectives (Objective 5)

This section addresses Objective 5: to identify the challenges faced by citizens in adopting digital identity-enabled services, together with related policy perspectives.

Table 12. Perception of respondents on challenges and policy interventions

Statement	SA	A	N	DA	SDA	Total
Lack of digital literacy limits effective use of digital identity systems	90	68	22	14	6	200
Internet connectivity issues affect access to digital services	86	70	26	12	6	200
Biometric authentication failures create difficulties for users	78	72	28	14	8	200
Existing grievance redressal mechanisms are effective	48	62	40	32	18	200
Government policies need to be strengthened to ensure inclusive digital identity access	94	68	20	12	6	200

Source: Primary data.

Table 13. Mean score and ranking - challenges and policy perspectives

Statement	Total Score	Mean Score	Rank
Lack of digital literacy limits effective use	822	4.11	II
Internet connectivity issues affect access	818	4.09	III
Biometric authentication failures create difficulties	798	3.99	IV
Existing grievance redressal mechanisms are effective	690	3.45	V
Government policies need strengthening for inclusive access	832	4.16	I

Source: Primary data.

The need to strengthen government policy for inclusive access recorded the highest mean score in this construct (4.16), reflecting strong public support for inclusive policy frameworks, better infrastructure, user education and regulatory oversight. Lack of digital literacy (4.11) and internet connectivity problems (4.09) were identified as the most significant structural barriers. Biometric authentication failures (3.99) were also widely reported, which is consistent with the lower rating of authentication reliability in Section 5.3. The effectiveness of grievance redressal mechanisms received the lowest mean score in the entire survey (3.45), indicating comparatively weak confidence in existing institutional support.

5.8 Overall satisfaction and future outlook

This section evaluates citizens' overall satisfaction with digital identity systems and their readiness for future digital governance initiatives.

Table 14. Perception of respondents on overall satisfaction and future readiness

Statement	SA	A	N	DA	SDA	Total
Overall, I am satisfied with digital identity services in India	84	72	26	12	6	200
Digital identity systems have improved my quality of life	78	74	30	12	6	200
I am confident using digital identity platforms independently	82	70	28	14	6	200
I am willing to adopt new digital governance services in the future	90	68	24	12	6	200
Digital identity systems are essential for India's digital future	96	66	20	12	6	200

Source: Primary data.

Table 15. Mean score and ranking - overall satisfaction and future outlook

Statement	Total Score	Mean Score	Rank
Overall satisfaction with digital identity services	816	4.08	III
Digital identity has improved quality of life	806	4.03	V
Confidence in using digital identity platforms	808	4.04	IV
Willingness to adopt future digital governance services	824	4.12	II
Digital identity is essential for India's digital future	834	4.17	I

Source: Primary data.

Attitudes towards India's digital identity systems were highly positive. The view that digital identity is essential for India's digital future recorded the highest mean score in the survey (4.17), followed closely by willingness to adopt future digital governance services (4.12). Overall satisfaction (4.08), confidence in independent use (4.04) and perceived improvement in quality of life (4.03) were also high. These results suggest that citizens regard digital identity not only as a functional tool but as a lasting foundation of India's digital transformation.

5.9 Consistency of ranking procedures: Spearman rank correlation

To check whether the ordering of accessibility items depends on the scoring method, Spearman's rank-order correlation was computed between the mean-score ranking and the Garrett ranking of the five accessibility items in Table 6, using a rank of 1.5 for the two tied items. The coefficient was $\rho = 0.975$ ($n = 5$), indicating near-complete agreement between the two procedures. Because the Garrett scale values used here are a monotonic transformation of the Likert categories and only five items are compared, the coefficient is interpreted as a descriptive consistency check rather than as an inferential test. Within these limits, it shows that the conclusion that ease of access and transparency are the most valued benefits, and that authentication reliability is the weakest aspect, does not depend on the choice of scoring method.

6 Discussion

The findings show that citizens perceive clear improvements in service accessibility, transaction efficiency and financial inclusion as a result of India's digital identity system. This is consistent with evidence that digitized service delivery reduces leakages and administrative friction (Gelb & Clark, 2013; Banerjee et al., 2020) and with studies attributing the rapid growth of digital payments to the combination of Aadhaar-linked accounts and interoperable payment rails (D'Silva et al., 2019; World Bank, 2019). The particularly strong endorsement of UPI suggests that, from the citizen's perspective, the payments layer is the most visible and tangible benefit of the DPI stack.

At the same time, the comparatively lower scores for authentication reliability, privacy protection and grievance redressal indicate that governance effectiveness, viewed from the citizen's side, cannot be inferred from administrative efficiency alone. The reported difficulties with biometric authentication echo earlier concerns about exclusion in Aadhaar-based welfare delivery (Khera, 2017). The coexistence of high usage with strong concern about data misuse reflects pragmatic adoption combined with privacy caution, a pattern also observed among users of identity infrastructure in India (Srinivasan et al., 2018) and in cross-country DPI research (OECD, 2021).

The strong support for data protection laws (mean 4.16), alongside only moderate trust in government data handling, suggests that citizens look for credible enforcement rather than the mere existence of legal safeguards. This is in line with the emphasis of the Puttaswamy judgments on proportionality, consent and data minimization, and it makes the effective implementation of the DPDP Act, 2023 and the DPDP Rules, 2025 an important test of citizen trust. The weak evaluation of grievance redressal, the lowest-rated item in the study, points to an implementation gap between technological rollout and citizen-facing institutional responsiveness. This dimension has received less scholarly attention than adoption and inclusion outcomes and deserves greater emphasis in both research and policy (Masiero & Bailur, 2021).

7 Summary of findings

- The respondents were mainly working-age adults (26–45 years) with relatively high educational attainment and frequent use of digital services (75.0% daily or weekly).
- Digital identity has substantially improved access to public services. Ease of access and transparency in service delivery were rated jointly as the most valued benefits (mean 4.12), a result that holds under both mean-score and Garrett ranking ($\rho = 0.975$).
- Authentication reliability was the weakest accessibility item (mean 3.86), and biometric authentication failures were widely reported as a practical challenge (mean 3.99).
- DPI has contributed strongly to financial and digital inclusion, with UPI rated highest (mean 4.12) for enabling participation in the digital economy; inclusion "for all" was rated lowest (4.04) within this construct.
- Privacy and trust recorded the lowest construct-level scores. Respondents strongly supported data protection laws (mean 4.16) and expressed concern about data misuse (3.92), while trust in government data handling was moderate (3.89).
- Citizens credit digital identity with improving transparency (4.12) but rate grievance redressal as the weakest governance mechanism (3.45; 55.0% agreement).
- Lack of digital literacy (4.11) and internet connectivity problems (4.09) were the main structural barriers, and strengthening government policy for inclusive access received the strongest support (4.16).
- Overall satisfaction (4.08) and willingness to adopt future digital governance services (4.12) were high, and digital identity was widely regarded as essential for India's digital future (4.17).
- The questionnaire was reliable, with Cronbach's alpha above 0.70 for every construct and 0.90 for the overall scale.

8 Conclusion

This study concludes that India's digital identity systems, built on Digital Public Infrastructure, are perceived by citizens to have improved access to public services, advanced financial and digital inclusion and made governance processes more efficient and transparent. The integration of Aadhaar-based authentication, UPI and DigiLocker has reduced procedural complexity, lowered dependence on physical documentation and speeded up service delivery. Citizen acceptance and satisfaction are high, reflecting the extent to which digital identity has become part of routine governance and economic activity.

The study also identifies significant unresolved issues of privacy, data security and institutional trust. Although respondents recognized the system's advantages, concerns about data misuse and authentication reliability remained common. Structural challenges, including gaps in digital literacy, connectivity limitations and weak grievance redressal mechanisms, continue to constrain the inclusive adoption of digital identity-enabled services. India's digital identity architecture therefore holds substantial transformative potential, but its long-term legitimacy depends on effective enforcement of data protection, citizen-centric design and sustained institutional accountability.

9 Policy implications

- **Strengthening data protection enforcement:** The phased implementation of the DPDP Act, 2023 and the DPDP Rules, 2025 should be transparent and visible to citizens, so that legal safeguards translate into trust in how personal data are handled.
- **Expanding digital literacy programs:** Targeted digital literacy initiatives, particularly in rural and semi-urban areas, are needed to support inclusive and effective use of digital identity systems.
- **Improving digital infrastructure:** Investment in reliable internet connectivity and system resilience is essential to reduce access barriers and service disruptions.
- **Reforming grievance redressal:** User-friendly, time-bound grievance systems are required to resolve authentication failures and service-related problems efficiently.
- **Ensuring inclusive policy design:** Digital identity policies should include specific provisions, such as alternative authentication options, for vulnerable groups including older persons, persons with disabilities and economically marginalized populations.
- **Enhancing institutional transparency:** Government agencies should adopt transparent data-handling practices and regularly inform citizens about system changes and safeguards.
- **Building trust through public engagement:** Continued stakeholder engagement and awareness campaigns can improve understanding, build trust and encourage voluntary participation in digital governance initiatives.

10 Limitations and future scope

10.1 Limitations

The study is limited to Coimbatore District, and its findings may not apply fully to regions with different socioeconomic and digital infrastructure conditions. The sample is more highly educated than the general population, and groups with very low digital literacy or limited access to devices may be underrepresented. The analysis is descriptive: the sample size and design supported reliability and ranking analyses but not the inferential testing of relationships among variables, and the Spearman coefficient is based on only five items. The study captures citizen perspectives only and does not include the views of policymakers, service providers or technical administrators. It measures perceived rather than objective system performance, and perceptions may change as technologies and policy frameworks, including the new data protection regime, evolve.

10.2 Future scope

Future research could test the proposed framework using Structural Equation Modelling (SEM or PLS-SEM) to estimate the relationships among accessibility, the mediating trust and literacy variables and governance outcomes. Multi-state comparative samples, with deliberate inclusion of digitally marginalized groups, would improve generalizability. Longitudinal designs could track how citizen trust changes as the DPDP Act and Rules are implemented. Text and sentiment analysis of grievance data also offers a promising way to evaluate citizens' experiences with digital public infrastructure at scale.

References

[1] Abraham R, Bennett ES, Bhusal R, Dubey S, Li Q, Pattanayak A, et al. (2018). State of Aadhaar report 2017–18. *IDinsight*.

[2] Banerjee A, Duflo E, Imbert C, Mathew S, Pande R (2020). E-governance, accountability, and leakage in public programs: Experimental evidence from a financial management reform in India. *American Economic Journal: Applied Economics*, 12(4), 39–72. https://doi.org/10.1257/app.20180302

[3] Bharadwaj A, El Sawy OA, Pavlou PA, Venkatraman N (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471–482.

[4] D'Silva D, Filková Z, Packer F, Tiwari S (2019). The design of digital financial infrastructure: Lessons from India (BIS Papers No. 106). Bank for International Settlements.

[5] Gelb A, Clark J (2013). Identification for development: The biometrics revolution (Working Paper No. 315). Center for Global Development.

[6] Government of India (2023). The Digital Personal Data Protection Act, 2023 (No. 22 of 2023). Ministry of Law and Justice.

[7] GSMA (2020). Digital identity: A toolkit for mobile operators. *GSMA*.

[8] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). 10 SCC 1 (Supreme Court of India).

[9] Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar) (2019). 1 SCC 1 (Supreme Court of India).

[10] Khera R (2017). Impact of Aadhaar on welfare programmes. *Economic and Political Weekly*, 52(50).

[11] 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

[12] MeitY (2023). Data Empowerment and Protection Architecture (DEPA). *Ministry of Electronics and Information Technology*, Government of India.

[13] MeitY (2025). Digital Personal Data Protection Rules, 2025 (notified 13 November 2025). *Ministry of Electronics and Information Technology*, Government of India.

[14] Narayanan A (2021). Data governance and privacy in India's digital public infrastructure. *Journal of Cyber Policy*, 6(2), 256–272.

[15] NITI Aayog (2020). India's digital public infrastructure: Unlocking value. *Government of India*.

[16] NITI Aayog (2023). India's DPI ecosystem: Opportunities and challenges. *Government of India*.

[17] OECD (2021). Digital government policy frameworks. *OECD Publishing*.

[18] Ramanathan U (2020). Privacy and data protection in India: Citizens' perspectives. *Indian Journal of Public Administration*, 66(3), 356–370.

[19] Reserve Bank of India (2022). UPI and financial inclusion in India. *Reserve Bank of India*.

[20] Srinivasan J, Bailur S, Schoemaker E, Seshagiri S (2018). The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. *International Journal of Communication*, 12, 1228–1247.

[21] UIDAI (2022). Aadhaar and digital identity in India. *Unique Identification Authority of India*, Government of India.

[22] World Bank (2019). ID4D global dataset: Digital identification systems. *World Bank*.

[23] World Bank (2021). Digital public infrastructure and inclusive growth. *World Bank*.