International Journal of Advance and Applied Research
Peer Reviewed | International Open Access Journal
ISSN: 2347-7075 | Impact Factor – 8.141 | *Website:* https://ijaar.co.in/
Volume-13, Issue-4 | March – April 2026

Original Article

Data Privacy Challenges in Indian E-Governance: A Study of Aadhaar- Linked Services

Muniya Chiragkumar Kasubhai
Assistant Professor of Political Science,
D.N.P Arts and Commerce College, Deesa, Gujarat (H.N.G.U)

Manuscript ID: IJAAR-130416
ISSN: 2347-7075
Impact Factor – 8.141

Volume - 13
Issue - 4
March – April 2026
Pp. 81 - 87

Submitted: 8 Mar. 2026
Revised: 20 Mar. 2026
Accepted: 25 Mar. 2026
Published: 10 Apr. 2026

Corresponding Author:
Muniya Chiragkumar Kasubhai

Quick Response Code:

Website: https://ijaar.co.in/

DOI: 10.5281/zenodo.19941149

DOI Link: https://doi.org/10.5281/zenodo.19941149

Abstract:

Aadhaar has become a platform of Indian e-governance since the scheme provides identity authentication to provide welfare, authentication, and access to public services, as provided in the Aadhaar Act, 2016. The jurisprudence of privacy, K.S. Puttaswamy, provided by the Supreme Court, had an impact on the legal architecture of Aadhaar and later statutory law, such as the Digital Personal Data Protection Act, 2023, recognizing the right to personal data protection and the need to process personal data lawfully. Simultaneously, Aadhaar-based services persistently bring up the recurring issues of informational privacy, functionality creep, authentication failure, welfare exclusion, weak grievance redress, and a lack of balance between state capacity and citizens' control over data. This paper explores these challenges by conducting a doctrinal and policy analysis of Aadhaar-based e-governance services in India and contends that the question is no longer whether or not the digital identity can enhance service delivery, but whether governance safeguards are strong enough to enable legality, proportionality, accountability, and inclusion.

Keywords: Aadhaar, Informational Privacy, Functionality Creep, Authentication

How to cite this article:

Muniya Chiragkumar Kasubhai (2026). Data Privacy Challenges in Indian E-Governance: A Study of Aadhaar- Linked Services. International Journal of Advance and Applied Research, 13(4), 81 - 87. https://doi.org/10.5281/zenodo.19941149

Introduction:

Digital identity systems are being highly promoted as a way of improving efficiency in administration, preventing fraud, and facilitating the exact targeting of welfare. Aadhaar became a visionary, distinctive identity system in India, which was mainly aimed at supporting the delivery of subsidies, benefits, and services in a targeted manner, especially those that are funded by the Consolidated Fund of India. Introduced as the Aadhaar Act, 2016, it vowed to eradicate ghost beneficiaries and direct benefit transfers (DBT), and reshape how people are governed by making the government less opaque and leaky, and more

verifiable and digital- first. This vision was constitutionally vindicated when the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India (2018) issued a landmark decision that placed stringent guardrails on it. Understanding the welfare delivery as a legitimate state goal, the nine-judge court bench held the very foundation of Aadhaar, biometric enrollment, the Central Identities Data Repository (CIDR), and Yes/No authentication, as proportionate to its goals. It, however, struck down Section 57, which had allowed unregulated use of the entities by the private entities based on contract and read down clauses that allowed the storage of metadata or free sharing (Aadhaar Act, 2016). This decision was a subdued one supporting Aadhaar as a public goods provider but limiting it to the primary right to privacy, which is now firmly established in Article 21 as a right to life and a right to personal liberty. This court balancing has created a twofold truth of Indian e-governance. On the positive side, Aadhaar-based services have proven to be efficient: DBT systems such as the Public Distribution System (PDS) and MGNREGA wage payments report decreases in leakage of up to 50% in certain states, with BCG estimates indicating a 13% reduction in the total welfare dissipation with Aadhaar-based payments. Interoperability of the three schemes- Jan Dhan-Aadhaar-Mobile (JAM) trinity has enhanced the rate of financial inclusiveness by facilitating real-time checks of pensions, scholarships, and health entitlements. Conversely, biometric (fingerprints, iris) and demographic data used to serve fragmented ecologies have made the privacy more vulnerable, especially among vulnerable demographics like women in rural areas, the elderly, and migrant workers. Authentication failures being excluded based on bad connectivity, bad seeding, or bad biometric wearing have been reported, causing the deaths of Aadhaar starvation and Supreme Court interventions. The creep of functions has not stopped, and Aadhar seeding is encroaching on non-welfare fields like exams and employment opportunities, and poses a danger to the corridors of profiling and surveillance. The violation of data throughout the enrolment centers, operators' fraud conducted in transactions involving the AePS, and low consent in asymmetric power relationships are also sources of the lack of trust despite the fact that UIDAI declares that it is a purpose-blind and minimal-response architecture. The paper disaggregates such tensions (under the evolving digital governance framework in India), such as the constitutional privacy doctrine (Puttaswamy), the Aadhaar Act, and the Digital Personal Data Protection Act, 2023 (DPDPA) (Angel One, 2025). The DPDPA gives a right to consent, data minimization, and grievance, but excludes state welfare processing, which is dubious in terms of enforcement rigor. The study has four objectives, starting with the mapping of legal-institutional bases, such as the mandates of UIDAI and the inter-ministerial connections. Second, it enumerates privacy problems: exclusion errors, threat of biometric permanence, and accountability gaps in ecosystems. Third, it compares the implications of DPDPA to improve fiduciary responsibilities as compared to the already existing silos of Aadhaar. Lastly, it promotes reforms: compulsory offline options, certified vendor chain, real-time fraud notification, and dignity-based metrics to balance efficiency with inclusion. (India Code, 2023)

Methodology:

It is a policy-oriented research paper based on primary and secondary sources. The key documents are the Aadhaar judgment of the Supreme Court and the Digital Personal Data Protection Act, 2023. Secondary sources are policy reports, commentary, and analysis on exclusion, misuse, and welfare-related issues of Aadhaar-based

systems. The research is qualitative and does not model statistically, but is concerned with the interpretation of laws, the design of institutions, and the implications of governance.

Aadhaar Architecture in E-Governance:

The Aadhaar system is a complex digital identity platform that focuses on the enrollment of detailed demographic information, such as name, date of birth, address, gender, and sensitive biometrics information, such as facial images, all ten fingerprints, and two eye iris scans. These records are safely kept in the Central Identities Data Repository (CIDR), which is a fortified government repository of records of more than 1.4 billion Indians. Justices unanimously approved the purpose-blind and minimal-response character of authentication under the Aadhaar Act, 2016, Section 4(3), which requires that responses should not include transactional metadata or core biometrics (India Code, 2023). Section 8 also governs e-KYC by stipulating informed consent and limitation of purpose, whilst Regulation 12 prohibits the storage of logs of authentication transactions longer than six months. Such a design theoretically shields Aadhaar against mass surveillance by separating the data streams: UIDAI only has identity proofs, whilst service providers have records of transactions. Practically, Aadhaar seeding can be found throughout Direct Benefit Transfer (DBT) systems: Public Distribution System (PDS) ration cards, MGNREGA job cards, pension payments, PM-KISAN farmer payments, and scholarships. The JAM Trinity (Jan Dhan-Aadhaar-Mobile) facilitates 34 lakh crore in annual DBT, and the government reports a 50% decrease in PDS leakage through deduplication. Aadhaar Payment Bridge (APB) and AePS make it easier to withdraw cash using biometrics in micro- ATM. However, this ubiquity turns a ten-digit number into a de facto universal identifier, and makes privacy risks shift to systemic dependencies, where biometric failure fails to authenticate 2-5% of authentication attempts (according to UIDAI data), with disproportionate effect on manual workers with damaged fingerprints and rural elders with connectivity issues (Centre for Internet and Society, 2016).

Constitutional Privacy Framework:

The legality of Aadhaar is dependent on whether the nine-judge bench will acknowledge privacy as a Fundamental Right in Article 21, under the trinity test that has been formulated Puttaswamy I (2017): (1) legality (lawful statutory basis); (2) legitimate aim (compelling state interest); and (3) proportionality (rational nexus, minimal intr The Aadhaar Act met legality through parliamentary enactment and fulfilled legitimate objectives- to eradicate welfare leakages in line with Section 7 requirements to tie subsidies to the Consolidated Fund. Proportionality was true in public-purpose authentication, but in private contractual purposes, it was not true. Four to one invalidated Section 57 in its entirety, declaring it unconstitutional in the literal sense of the term, using Aadhaar through contracts, body corporates, and other entities, which only Parliament has the power to sanction privacy intrusions. Section 33(2) allowing an unlimited National Security exception was struck, and Section 2(d) of the definition of the term authentication was construed narrowly to obtain a meaning that did not cover profiling (CivilsDaily, 2023). Dissenting partly, Justice Chandrachud cautioned against the Aadhaar surveillance architecture, although the live decision saved fundamental uses of welfare. This jurisprudence forms binding principles of e-governance: pervasive identity regimes require necessity (no less invasive options), clear authorization (statutory, not executive), and protection of data (audits, redress of grievance).

UIDAI needs to be demonstrably proportionate between the empirical welfare benefits and harms of exclusion, especially as Digital Public Goods grow through India Stack (Account Aggregator, Open Credit Enablement). Without them, the creep of functions into exams, employment, or non-Consolidated Fund services would be unconstitutional, and redirection would be necessary towards voluntary, multi-modal authentication that avoids the abrasion of dignity to administrative convenience (ClearIAS, 2023).

Major Privacy Challenges:

Collection of Sensitive Data:

The Aadhaar is based on the biometric information, and even the Court acknowledged the fact that the aspect of bodily autonomy and reasonable expectations of privacy was in place, even though the information collection was relevant in the case. Biometric identifiers are not like regular demographic information since they are enduring, hard to change, and very sensitive when they are compromised or abused. That is not the only privacy menace because the original collection of biometric information is not alone, but all the institutional ecosystems where the authentication requests and identity-based records are sent (Digital Personal Data Protection Act, 2023).

Function Creep and Expanding Use:

A slippage of functionality whereby a system that was meant to perform a limited scope of welfare-related tasks, gradually is normalized in new services, is one of the major concerns of Aadhaar-based governance. The Supreme Court agreed on Aadhaar under the condition of subsidies, benefits, and services of government expenditure; however, it was against the spread of the contract in the private sector. Later policy directions, including the discussions of Aadhaar provisions as to how they might be aligned with the DPDP framework, and proposals to introduce changes in the law to extend the significance of authentication in the public interest, are indications of the expansion pressures still being legitimized. Function creep compounds the privacy threat as data subjects will probably not have meaningful control over their data when a single identifier will be demanded in many various interactions with the state and quasi- publics (Digital Personal Data Protection Act, 2023).

Failures to authenticate and Welfare exclusion:

Disenfranchisement is not an exclusive right to complain against Aadhaar-related services, but surveillance risk is the most serious. Another case in which the Court discerned that Aadhaar is in fact compulsory is the scenarios in which the persons entitled to obtain some welfare benefits under Section 7 are obligated to be enrolled in the system, although the enrolment can be formally referred to as voluntary. Cases have also been reported where persons have been denied pensions or other social benefits based on imperfections in the database, authentication of identity discrepancies, due to the welfare linkages of Aadhaar. Practically, this implies that the issues of privacy and dignity cannot be unbundled and opposed to the access to food, pensions, and livelihood support (Economic Times, 2025).

Unauthorized Access and fraud:

The misuse of Aadhaar-linked systems in downstream systems, including unauthorized withdrawals and fraudulent enrollment or transactional behaviors in Aadhaar-enabled payment systems, has also been linked to Aadhaar-linked infrastructures. Although the fundamental UIDAI architecture is verified to be secure, numerous real-world harms take place at the boundary of the ecosystem, where local operators, intermediaries,

service points, or poorly managed entities deal with citizens. This will provide a key lesson in governance, in that privacy protection cannot be evaluated just at the central database level, but must be considered throughout the entire service chain (Wikipedia, 2017).

Limited User Agency:

The Data Principals' rights granted by the DPDP Act, 2023, regarding digital personal data include the right to notice, consent, withdrawal, access, correction, erasure, grievance redress, and nomination. Nevertheless, many of the interactions around Aadhaar are conducted on unequal terms, with people being unable to negotiate terms, data flow, or refuse processing on the risk of being denied services. This undermines the practical usefulness of consent in situations of public service and increases the pressure on the necessity, proportionality, and a more robust reliance on public-law accountability as opposed to the use of formal notice (UIDAI, 2025).

Exemption and State Power:

The DPDP Act provides an extensive data protection regime, but includes exceptions to designated state operations and law enforcement-related processing, as well as certain types of public interest or notified entities. The Act also provides for the processing of some lawful purposes, such as by the State and its instrumentalities of subsidies, benefits, services, certificates, licences, or permits with prescribed conditions. Although these provisions facilitate administrative continuity, concern arises that data protection rights are subject to being watered down in high-impact state scenarios in which citizens are relying on digital governance systems the most (Supreme Court Observer, 2023).

DPDP Act and Aadhaar Governance:

The Digital Personal Data Protection Act, 2023, is important as it presents minimum legal processing requirements, notice, consent, the requirement of necessity-based consent, security measures, breach notification, grievance mechanism, and rights of access, correction, and erasure. It further creates the Data Protection Board of India and increases the responsibilities of Significant Data Fiduciaries, such as Data audits, impact assessment, and the Data Protection Officer. These capabilities have the potential to enhance accountability within the Aadhaar- based service environments, assuming that they are implemented strictly. Concurrently, the Aadhaar law's interaction with the DPDP framework is institutionally complicated. It has been reported publicly that there is a need to harmonize the rules relating to Aadhaar with the more recent privacy law. Until the sectoral alignment, rules of implementation, and enforcement practice are fully developed, there may be gaps between the high-level statutory rights and the experience of users in Aadhaar-seeded governance systems.

International Journal of Advance and Applied Research
Peer Reviewed | International Open Access Journal
ISSN: 2347-7075 | Impact Factor – 8.141 | *Website: https://ijaar.co.in/*
Volume-13, Issue-4 | March – April 2026

Table 1: Key Tensions with Governance Promise

Dimension	Governance Promise	Privacy Challenge
Identification	Unique identity, elimination of duplicates	Risk of surveillance and profiling
Welfare Delivery	Efficient DBT, reduced leakages	Exclusion due to authentication failure
Authentication	Secure, real-time verification	Biometric errors, connectivity issues
Data Collection	Accurate beneficiary targeting	Collection of sensitive biometric data
Interoperability	Seamless service integration	Function creep across sectors
Consent	Legal consent framework (DPDP Act)	Weak, non-meaningful consent in practice
Security	Centralized secure database (CIDR)	Vulnerabilities at the ecosystem level
Governance	Accountability through UIDAI	Weak grievance redress mechanisms

Critical Analysis:

The Aadhaar ecosystem represents a paradox in modern governance. While it enhances administrative efficiency, it simultaneously creates structural risks to privacy and dignity.

The landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) established privacy as a fundamental right, enforcing the triple test of legality, necessity, and proportionality. However, real-world implementation often falls short of these principles.

Similarly, the Digital Personal Data Protection Act, 2023, introduces a modern data protection framework, but its broad state exemptions weaken its applicability in Aadhaar-linked welfare systems.

The core issue is not technological failure, but governance imbalance:

- State power is expanding faster than accountability mechanisms
- Citizens lack effective control over their own data
- Welfare efficiency often overrides dignity and inclusion

Thus, Aadhaar governance reflects a shift from a welfare state → data-driven state, where privacy risks are systemic rather than incidental.

Policy Recommendations / Reforms:

To ensure a balance between efficiency and privacy, the following reforms are essential:

1. Multi-Modal Authentication:

- Introduce alternatives like OTP, offline QR, or physical ID
- Reduce dependency on biometrics

2. Offline Functionality:

- Enable offline verification systems for rural and low-connectivity areas
- Prevent exclusion due to technical failures

3. Stronger Grievance Redress:

- Time-bound complaint resolution mechanisms
- Independent oversight authority beyond UIDAI

4. Audit of Aadhaar Ecosystem:

- Regular audits of enrollment centers and intermediaries
- Certification of vendors handling Aadhaar data

5. Limit Function Creep:

- Strict legal boundaries on Aadhaar usage
- Parliamentary approval for expansion into new sectors

6. Data Minimization Enforcement:

- Collect only necessary data
- Restrict unnecessary Aadhaar seeding

7. Transparency Measures:

- Public disclosure of data breaches
- Real-time fraud alerts to users

8. Dignity-Based Governance Metrics:

- Measure success not just by efficiency but by:
- Inclusion
- Accessibility
- Citizen autonomy

Conclusion:

The Aadhaar system has transformed India's e-governance landscape by improving efficiency, reducing leakages, and enabling large-scale welfare delivery. However, its expansion has exposed deep structural challenges related to privacy, exclusion, and accountability.

The recognition of privacy as a fundamental right through the Puttaswamy Judgment and the enactment of the Digital Personal Data Protection Act, 2023, mark significant steps toward data protection. Yet, gaps remain in implementation, especially in state-led welfare systems.

The future of Indian e-governance depends not on abandoning Aadhaar, but on reforming it:

- From **efficiency-centric → rights-centric governance**
- From **data control → citizen control**
- From **digital expansion → accountable digitalization**

Only by **embedding legality, proportionality, accountability, and inclusion** into its framework can Aadhaar truly serve as a model for ethical digital governance.

References:

1. *Aadhaar Act, 2016 (India Code)*
2. *Justice K.S. Puttaswamy (Retd.) v. Union of India*
3. *Digital Personal Data Protection Act, 2023*
4. *UIDAI Annual Reports*
5. *Centre for Internet and Society (2016)*
6. *Supreme Court Observer (2023)*
7. *Economic Times (2025) – Aadhaar exclusion reports*
8. *ClearIAS (2023) – Aadhaar analysis*
9. *CivilsDaily (2023) – Constitutional interpretation*
10. *Government of India – JAM Trinity Reports*