International Journal of Engineering Research & Science (IJOER) ISSN: [2395-6992] [Vol-12, Issue-3, March 2026]

Application-Level Privacy Preservation Framework for Aadhaar-Based Applications

Prof. Chandani Patel[1*]; Pankaj Yadav[2]; Harsh Mhapsekar[3]

Department of MCA, University of Mumbai, Mumbai, India
*Corresponding Author

Abstract**—** *Aadhaar has become an important digital identity infrastructure in India, facilitating authentication and e-KYC operations in numerous sectors. Even with the presence of privacy-preserving technologies like encryption, tokenization, and offline verification, challenges to privacy have been encountered while using Aadhaar-based applications in real-world scenarios. Research studies have mainly concentrated on authentication schemes, backend systems, and laws concerning Aadhaar, with little involvement of application-layer privacy concerns. In this paper, we have carried out a qualitative analysis of the application of privacy preservation in Aadhaar-based applications and identified key challenges including data overcollection, poor consent systems, and temporary data exposure. A structured privacy-preserving framework has been proposed with emphasis on data minimization, secure session handling, informed consent, and qualitative evaluation of privacy preservation.*

Keywords— Aadhaar, digital identity, e-KYC, privacy preservation, application-level security.

I. INTRODUCTION

Digital identity systems have become a sine qua non for modern governance and service delivery as they enable efficient authentication and verification systems. In India, Aadhaar is a unique identity solution that enables banking, welfare, telecom, and e-governance services. Large-scale digital identity systems raise privacy concerns related to data linkage and centralized storage [1]. The adoption rate of Aadhaar has ensured efficiency, inclusiveness, and transparency, thereby enhancing nation-building initiatives.

However, the large-scale use of Aadhaar has also generated concerns associated with both privacy and personal data protection. Though proper technical measures and rules regulate such matters, privacy risks generally arise owing to inadequate practices followed at the application level. Aadhaar applications handle personal data while dealing with authentication or verification tasks.

The majority of existing work has focused on Aadhaar core design, cryptographic security, or legal aspects. Less effort has been spent on privacy issues that emerge at the application level when these systems are used in real-world contexts. This paper addresses this gap by focusing on privacy issues that emerge within Aadhaar-based applications.

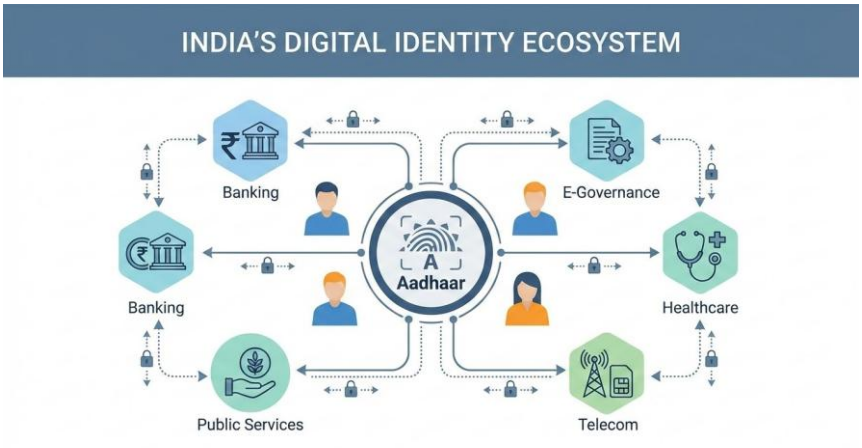

Figure 1: India's digital identity ecosystem showing Aadhaar integration across banking, e-governance, healthcare, telecom, and public services

II. LITERATURE REVIEW

TABLE 1
SUMMARY OF EXISTING STUDIES ON AADHAAR, E-KYC, AND PRIVACY PRESERVATION TECHNIQUES

Ref.	Key Findings	Conclusion
Sadhya & Sahu (2024)	Analyzes Aadhaar architecture and highlights privacy risks such as identity linkage, centralized data use, and weak application-level enforcement	Strong application-level privacy mechanisms are required in addition to core Aadhaar security
Gyanchandani (2025)	Examines the trade-off between usability and privacy in Aadhaar-enabled services	Privacy must be balanced with convenience through better application design
Nalawade et al. (2024)	Proposes a blockchain-based e-KYC system to reduce centralized storage and improve trust	Decentralized models enhance privacy but require careful integration
Sharma & Verma (2024)	Introduces smart contracts to automate privacy-preserving e-KYC processes	Smart contracts can improve privacy control but add system complexity
Banerjee et al. (2025)	Proposes blockchain middleware to isolate sensitive identity data in banking systems	Architectural separation improves privacy and regulatory compliance
Malik (2024)	Reviews biometric security risks such as spoofing, template leakage, and misuse	Biometric data must be protected through minimal exposure and strong safeguards
Guo et al. (2024)	Presents a biometric authentication scheme with enhanced privacy protection	Privacy-preserving biometrics are essential for secure identity systems
Lai et al. (2024)	Proposes a decentralized biometric authentication protocol without central storage	Decentralization reduces privacy risks but faces adoption challenges
Chen et al. (2024)	Introduces anonymization methods that preserve biometric utility	Anonymization can protect privacy while maintaining authentication accuracy
He et al. (2025)	Analyzes deepfake threats against biometric authentication systems	Advanced detection techniques are required to secure biometric identities
Aziz & Komogortsev (2024)	Studies identity linkage risks across platforms using shared identifiers	Preventing cross-platform linkability is critical for privacy protection
Naghmouchi et al. (2025)	Compares national digital identity systems with respect to governance and privacy	Privacy-centric identity design improves citizen trust
Hannan et al. (2023)	Systematic review of blockchain-based e-KYC solutions and challenges	Technology alone cannot ensure privacy without good application design
Wu (2023)	Discusses legal safeguards and privacy concerns in digital identity systems	Legal compliance must align with system-level privacy design
Rodríguez & Nikolaidis (2023)	Examines digital identity systems from a human rights perspective	Inadequate privacy protection may lead to exclusion and surveillance
Robles-Carrillo (2024)	Explores conceptual and legal aspects of digital identity and privacy	Privacy is a foundational requirement for digital identity systems
Madhusudhanan (2025)	Reviews privacy techniques across the entire data lifecycle	Privacy must be enforced at all stages of data handling
Kumar & Singh (2024)	Identifies privacy challenges in large-scale digital identity deployments	Application-level privacy gaps remain a major concern
Mehta (2025)	Discusses ethical and societal privacy issues in India's digital ecosystem	Privacy-aware governance is essential for sustainable digital transformation

Recent research focuses on blockchain-based e-KYC systems, aiming for a shift toward privacy and trust by decentralizing identity storage [3], [14]. While such approaches enhance transparency and data integrity, issues of scalability, interoperability, and legal compliance remain unaddressed. Investigations of biometric authentication point toward additional privacy hazards like template leakage, spoofing attacks, and irreversibility of biometric identifiers [7], [8].

The digital identity literature further stresses the concept of privacy-by-design principles and compliance with data protection regulations [15], [16]. However, few studies investigate application-layer privacy risks, such as consent handling, temporary data storage, and session management in Aadhaar-enabled applications.

III. PROBLEM DEFINITION

Although the Aadhaar system has mechanisms that ensure privacy preservation, breaches still occur. This is caused by the way some Aadhaar-based applications collect data, process data, and handle data during user sessions.

The problem addressed in this work is the absence of a structured application-level privacy assessment and design framework for Aadhaar applications, which leads to potential data leakage.

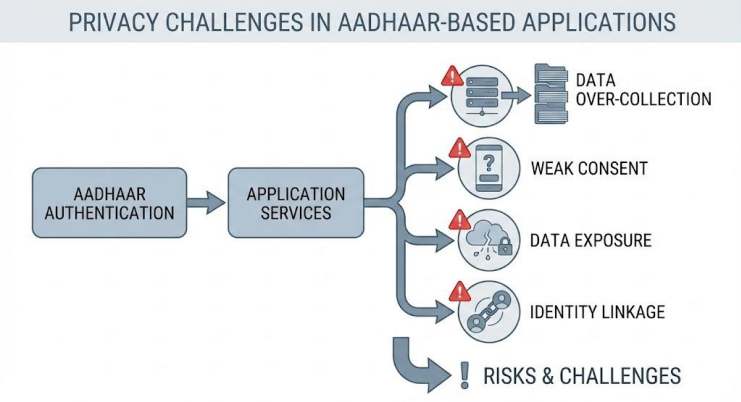

Figure 2: Conceptual illustration of application-layer privacy risks in Aadhaar-enabled authentication workflows

The consent mechanisms provided in Aadhaar-enabled applications are often opaque and ineffective. Identity linkability across digital platforms has been identified as a major privacy threat [12]. Users are often required to submit consent in simplified forms, such as checkboxes or one-time passwords, without being informed about the nature of data processing, usage, retention periods, or third-party data transfers. Consequently, such consent provides limited privacy protection.

IV. OBJECTIVES

The objectives of this research are as follows:

1. To study privacy challenges associated with Aadhaar-based applications
2. To analyze existing privacy preservation techniques
3. To identify application-level privacy risks
4. To propose a qualitative privacy preservation framework
5. To promote privacy-aware Aadhaar application design

V. METHODOLOGY

This research adopts a structured qualitative analytical methodology comprising four phases:

Phase 1: Literature Review — An extensive literature review was conducted to understand privacy mechanisms in Aadhaar-based systems and identify implementation gaps.

Phase 2: Workflow Analysis — Common application workflows involving Aadhaar authentication and e-KYC were conceptually examined to detect privacy exposure points such as temporary storage, consent capture, and session handling.

Phase 3: Risk Categorization — Identified risks were categorized into application-level vulnerabilities including overcollection of data, ineffective consent transparency, identity linkability, and transient data exposure.

Phase 4: Framework Design — Based on these categorized risks, a structured privacy preservation framework was designed incorporating principles of data minimization, tokenization, secure session lifecycle control, and qualitative privacy evaluation parameters.

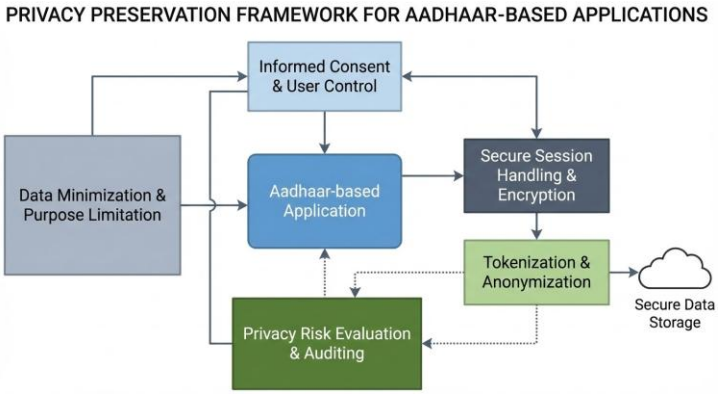

Figure 3: Proposed application-level privacy preservation framework for Aadhaar-based applications

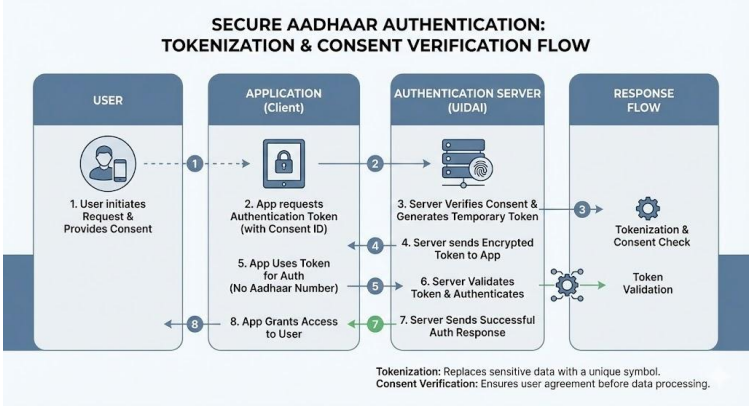

Figure 4: Token-based Aadhaar authentication flow with consent validation and secure response handling

This approach ensures systematic identification of privacy weaknesses and provides structured mitigation guidance without relying on sensitive identity datasets.

VI. RESULTS AND DISCUSSION

The analysis demonstrates that privacy vulnerabilities in Aadhaar-enabled applications primarily originate from design-level implementation gaps rather than inherent flaws in the core authentication infrastructure. Overcollection of personal data, minimalistic consent procedures, and inadequate session handling were identified as dominant risk factors.

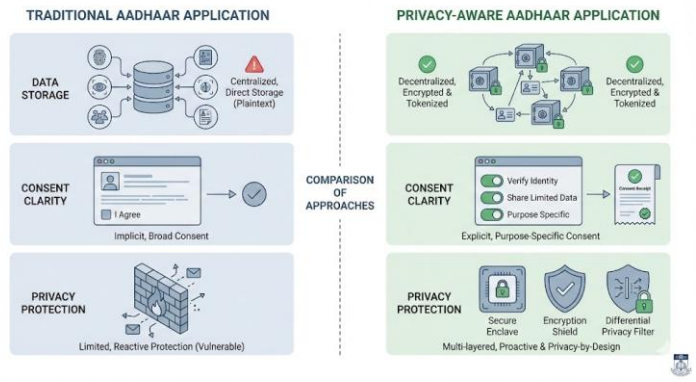

Figure 5: Comparative analysis of traditional and privacy-aware Aadhaar application architectures

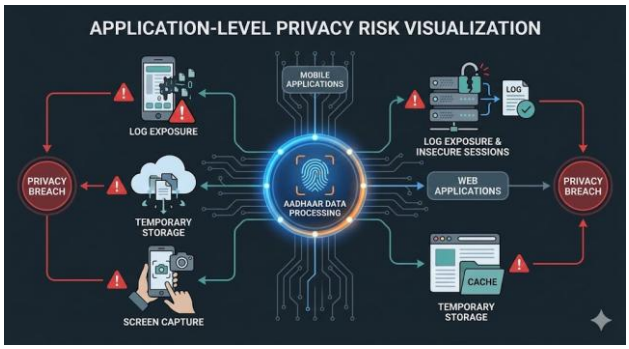

Figure 6: Visualization of application-layer privacy vulnerabilities in Aadhaar data processing environments

The proposed framework introduces structured controls addressing these risks through enforced data minimization, consent clarity requirements, token-based identifier handling, and restricted session data exposure. Unlike generalized privacy models, this framework specifically maps identified risks to corrective application-layer design strategies.

From a practical perspective, the framework can assist developers and institutions in implementing privacy-aware Aadhaar services while maintaining compliance with digital governance standards. It can also serve as a checklist for auditing application-level privacy practices.

TABLE 2
SUMMARY OF APPLICATION-LEVEL PRIVACY RISKS AND MITIGATION STRATEGIES

Privacy Risk	Description	Proposed Mitigation
Data Overcollection	Collection of more data than necessary for authentication	Enforce data minimization principles
Poor Consent Transparency	Users unaware of data usage, retention, and sharing	Clear, layered consent with detailed disclosures
Identity Linkability	Cross-platform tracking using shared identifiers	Tokenization and identifier isolation
Temporary Data Exposure	Residual data from sessions left exposed	Secure session lifecycle management
Inadequate Session Handling	Sessions persisting beyond required duration	Time-bound sessions with automatic termination

VII. CONCLUSION AND FUTURE WORK

This study presented a structured application-level privacy preservation framework for Aadhaar-based applications. While Aadhaar incorporates secure authentication mechanisms, privacy risks continue to arise due to application-layer design weaknesses. Through systematic qualitative analysis, this paper identified critical privacy gaps including ineffective consent mechanisms, identity linkability, and temporary data exposure.

Figure 7: Secure digital identity architecture illustrating user-centric control and encrypted data exchange between service and identity providers

Figure 8: Conceptual model of a privacy-centric digital governance framework for Aadhaar-based systems in India

The proposed framework provides actionable design-level recommendations aligned with privacy-by-design principles and digital governance requirements [15], [16]. By integrating structured privacy controls at the application layer, developers can significantly reduce privacy vulnerabilities while preserving usability.

Future Work:

1. Empirical validation of the framework through prototype implementation
2. Development of measurable privacy evaluation metrics for automated compliance assessment
3. Case studies of framework application in real-world Aadhaar-enabled services
4. Extension of the framework to other digital identity systems beyond Aadhaar

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] A Critical Survey of the Security and Privacy Aspects of the Aadhaar Framework https://doi.org/10.1016/j.cose.2024.103680
[2] A Balanced Approach to Privacy for Aadhaar: Between Privacy and Convenience https://www.researchgate.net/publication/367864932
[3] Privacy Preserving and Trustworthy e-KYC System Using Blockchain https://www.ijacsa.thesai.org/Abstract.aspx?doi=10.14569/IJACSA.2024.015
[4] Enabling Trust and Privacy Preserving e-KYC System Using Blockchain https://ijsrset.com/IJSRSET2411784
[5] e-KYC Based Privacy Preserving Model Using Smart Contracts https://www.researchgate.net/publication/387551233
[6] Enhancing Privacy in Banking Systems Using Blockchain-Based Middleware https://www.tandfonline.com/doi/full/10.1080/23311975.2025.2570063
[7] Biometric Authentication: Risks and Advancements in Biometric Security Systems https://www.researchgate.net/publication/390786249
[8] A Novel Biometric Authentication Scheme with Privacy Protection https://www.sciencedirect.com/science/article/pii/S0167404824003006
[9] BioZero: A Privacy-Preserving Decentralized Biometric Authentication Protocol https://arxiv.org/abs/2409.17509
[10] Model-Agnostic Utility-Preserving Biometric Information Anonymization https://arxiv.org/abs/2405.15062
[11] Identity Deepfake Threats to Biometric Authentication Systems https://arxiv.org/abs/2506.06825
[12] Assessing Privacy Risk of Cross-Platform Identity Linkage https://arxiv.org/abs/2402.08655
[13] Perspectives on National Digital Identity Systems https://www.sciencedirect.com/science/article/pii/S2096720925001563
[14] A Systematic Literature Review of Blockchain-Based e-KYC Systems https://ieeexplore.ieee.org/document/10100622
[15] Digital Identity, Privacy Security, and Legal Safeguards https://link.springer.com/article/10.1007/s13278-022-00954-1
[16] Digital Identity Systems and Human Rights https://jlsda.com/index.php/lsda/article/view/323
[17] Digital Identity: Nature, Concept and Legal Dimensions https://academic.oup.com/ijlit/article/32/1/eaae019/7760180
[18] Privacy Preservation Techniques Across the Data Lifecycle https://www.sciencedirect.com/science/article/pii/S0167404825001622
[19] Privacy Challenges in Large Scale Digital Identity Systems https://www.researchgate.net/publication/382941245
[20] Human Privacy in the Age of Technology in India: Challenges and Opportunities https://journals.sagepub.com/doi/full/10.1177/21582440241234567