2025 Volume: 01 Issue: 04 www.ijrpa.com Review Article

International Journal Research Publication Analysis

Page: 01-15

EKYC BIOMETRIC ENTRANCE AND REGISTRATION USING EKIOSK

***[1]Siya Dadheech, [2]Ram Babu Buri, [3]Dr. Vishal Shrivastava, [4]Dr. Akhil Pandey**

[1]Computer Science and Engineering, Arya College of Engineering and Information Technology, Jaipur, India.

[2]Assistant Professor, Computer Science and Engineering, Arya College of Engineering and Information Technology, Jaipur, India.

[3]Professor, Computer Science and Engineering, Arya College of Engineering and Information Technology, Jaipur, India.

[4]Professor Computer Science and Engineering Arya College of Engineering and Information Technology Jaipur, India.

Article Received: 30 June 2025
Article Revised: 20 July 2025
Published on: 10 August 2025

***Corresponding Author: Siya Dadheech**
Computer Science & Engineering, Arya College of Engineering and Information Technology, Jaipur India. DOI: https://doi-doi.org/101555/ijrpa.7756

ABSTRACT

This paper proposes the development of an eKYC-enabled self-service eKiosk for secure biometric-based Aadhaar registration and authentication. The system captures a user’s biometric data and verifies it against information stored on a portable storage medium, such as an optical memory card. In addition to biometric matching, the kiosk facilitates photo capture, manual data entry, and real-time Aadhaar enrolment or updates. Upon successful registration, the kiosk securely writes the user's information to the storage medium and dispenses the card immediately. This approach reduces the need for manual intervention, accelerates identity verification, and promotes broader access to digital public services through automated and contactless processes.

KEYWORDS: eKYC, Aadhaar, biometric authentication, eKiosk, self-service system, UIDAI, digital identity, optical memory card, identity verification, digital governance.

I. INTRODUCTION

According to the World Population Data Sheet (2013) by the Population Reference Bureau, India is the second most populous country globally, with a population of approximately 1.277

billion, and is projected to become the most populous by 2050, reaching 1.652 billion. This rapid population growth has intensified the need for a streamlined and scalable identity management system. Traditionally, citizens have relied on multiple identity cards—such as ration cards, voter ID cards, and PAN cards—to access various government services and welfare schemes, including LPG subsidies and the Mahatma Gandhi National Rural Employment Guarantee Act (MGNREGA). Managing and verifying these multiple forms of identity has become increasingly complex and burdensome for both citizens and administrators.

To address these challenges, the Government of India established the Unique Identification Authority of India (UIDAI), with the objective of issuing a single, unified identity number known as Aadhaar. This 12- digit number is intended to serve as a universal identity across services. Although the initial target was to issue Aadhaar to 1.2 billion residents by 2020, the effort fell short due in part to limited accessibility of enrolment centers, particularly in rural and remote areas.

This research proposes the development of a self-service eKiosk system inspired by Automated Ticket Vending Machines (ATVMs) used in Indian railway stations. These kiosks will enable users to perform a range of Aadhaar-related tasks independently, such as new enrolment, biometric and demographic updates, mobile/email linking, and requests for physical Aadhaar cards. The goal is to simplify the user experience, improve service accessibility, reduce dependency on manual processes, and enhance the overall efficiency of Aadhaar-related services. The proposed solution also integrates biometric authentication and eKYC to ensure secure and accurate identification.

II. LITERATURE SURVEY

The rise of biometric authentication has reshaped identity verification systems globally, and in India, the Aadhaar program has served as a major catalyst. Multiple studies have explored the use of biometric data for identity verification, emphasizing its potential for enhancing security and operational efficiency across public services.

Alrawili et al. (2023) conducted a detailed survey of biometric authentication techniques, noting that fingerprint, iris, and facial recognition systems offer varying degrees of accuracy and resilience depending on environmental conditions and device quality. Their study underscores the importance of multimodal biometric systems to reduce failure rates in real-world scenarios.

In the context of Aadhaar, a comprehensive survey by Paliet al. (2020) analyzed its security and privacy framework. They discussed issues related to centralized data storage, potential breaches, and the legal and ethical implications of biometric data collection. They recommended implementing secure encryption protocols and regular audits to strengthen public trust—key considerations when designing eKYC kiosks that will handle sensitive user data.

Further research by Panigrahi (2022) critically evaluated the social impact of Aadhaar's biometric authentication, especially among marginalized populations. The study revealed that biometric mismatches, device failures, and poor fingerprint quality—especially among manual laborers—often led to exclusion from welfare benefits. These findings highlight the need for kiosk systems that support redundancy (e.g., facial + iris recognition) and offer user-friendly alternatives in case of biometric errors.

Real-world implementations support these findings. The Delhi International Airport's use of biometric kiosks for immigration processing demonstrated the potential for reducing processing time by over 50%, proving that well-designed biometric self-service systems can enhance both user experience and operational throughput (Business Standard, 2024).

However, infrastructure challenges persist. Studies on rural deployments, especially in Aadhaar-based Public Distribution System (PDS) rollouts, have revealed failures due to poor internet connectivity, outdated biometric sensors, and low digital literacy. Reports indicated that up to 28% of rural users faced difficulties during biometric authentication, leading to exclusion from basic services (Khera, 2019). These challenges suggest that eKYC kiosks must include offline capabilities, simple UI/UX, and multilingual support to function effectively in diverse socio-economic contexts.

On the technical front, research in biometric data matching has evolved toward AI-based models. A deep- learning-based biometric authentication survey (Saxena et al., 2020) demonstrated significant improvements in real-time facial and fingerprint recognition accuracy. These models, when integrated with kiosk systems, can enable faster, more accurate identity verification with lower error margins.

III. CONCEPTUAL FRAMEWORK

The conceptual framework for the eKYC biometric entrance and registration using eKiosk consists of the following core components:

1. User Interaction Layer

The user interacts with the eKiosk through an intuitive interface, providing biometric inputs (fingerprint, iris scan, facial image) and entering demographic details.

2. Biometric Data Capture and Verification

The kiosk captures biometric data using specialized sensors and compares it against data stored on a portable storage medium (e.g., optical card) or central Aadhaar database for identity verification.

3. Data Processing and Authentication Module

This module processes biometric inputs, matches them with stored biometric data, and authenticates the user based on the match result.

4. Registration and Update Services

Once authenticated, users can perform Aadhaar-related services such as new enrollment, biometric updates, linking mobile/email, and address updates.

5. Portable Storage Device Management

Biometric and registration data are securely saved on a portable storage device, which is then issued to the user.

6. Security and Privacy Controls

All data exchanges and storage incorporate encryption and secure authentication protocols to ensure user privacy and data integrity.

IV. METHODOLOGY

The development of the eKYC Biometric Entrance and Registration System using eKiosk was carried out through a structured approach, encompassing system design, hardware integration, software development, and compliance with UIDAI (Unique Identification Authority of India) guidelines. The methodology is divided into several key phases

3.1 System Design and Architecture

The system was designed to facilitate seamless user interaction, secure biometric data capture, and efficient processing of Aadhaar-related services. The architecture comprises:

- User Interface (UI): A touch-based interface enabling users to select services, provide biometric inputs, and enter personal details.

- Biometric Capture Devices: Integrated sensors for capturing fingerprints, iris scans, and facial images.
- Processing Unit: A central processor handling data validation, authentication, and communication with UIDAI servers.
- Data Storage: Secure storage solutions for temporary data retention during the session.
- Connectivity Module: Ensures real-time communication with UIDAI databases for authentication and data updates.

3.2 Hardware Components

The eKiosk is equipped with the following hardware components

- Fingerprint Scanner: Captures high-resolution fingerprint images for authentication.
- Iris Scanner**:** Records iris patterns to enhance security.
- Camera: Captures facial images for biometric matching.
- Touch Screen: Allows users to interact with the system and input personal information.
- Card Reader: Reads and writes data to portable storage devices like optical cards.
- Processor and Memory: Handles data processing and temporary storage during sessions.

3.3 Software Development

The software development followed a modular approach

- Frontend Development: Utilized React.js for building a dynamic and responsive user interface. JSX syntax was employed to render HTML elements within JavaScript code, enhancing modularity and maintainability. State management was achieved using React Hooks, and CSS was applied for styling and responsiveness across devices.
- Backend Development: Node.js was used to develop the server-side logic, providing RESTful APIs for communication between the kiosk and UIDAI servers. The backend handled user authentication, data validation, and session management.
- Database Management: A secure database system was implemented to store session data and transaction logs. Data encryption techniques were employed to ensure privacy and integrity.

3.4 Biometric Data Capture and Authentication

- Data Capture: Users provide biometric data through integrated sensors. The system captures fingerprints, iris scans, and facial images, ensuring high-quality input through pre processing techniques like noise reduction and image enhancement.

- Data Verification: The captured biometric data is compared against pre-stored templates in the UIDAI database. Matching algorithms assess the similarity between input and stored data, determining authentication success.
- Authentication Process: Upon successful biometric verification, users can access Aadhaar services such as enrollment, updates, and linking of mobile numbers or emails.

3.5 Security Measures

To ensure the security and privacy of user data

- Data Encryption**:** All biometric and personal data are encrypted during transmission and storage.
- Secure Authentication: Multi-factor authentication mechanisms are implemented to prevent unauthorized access.
- Compliance with UIDAI Guidelines**:** The system adheres to UIDAI's security standards and protocols for biometric data handling and authentication.

3.6 Testing and Evaluation

The system underwent rigorous testing to evaluate

- Biometric Matching Accuracy**:** Assessed the precision of fingerprint, iris, and facial recognition systems.
- System Performance: Evaluated the response time and reliability of the kiosk under various conditions.
- User Experience: Collected feedback from users to identify areas for improvement in interface design and functionality.

3.7 Deployment and Maintenance

Post-development, the eKiosk system was deployed in select locations for real-world usage. Continuous monitoring and maintenance were conducted to address any technical issues, update software components, and ensure compliance with evolving UIDAI standards.

V. REAL-TIME APPLICATIONS

The integration of biometric authentication with self-service kiosks for eKYC has found practical relevance across various sectors, especially in the context of digital identity systems like Aadhaar in India. Below are the key real-time applications of this technology:

6.1 Aadhaar Enrollment and Updates

The primary application of the eKYC biometric kiosk is to facilitate Aadhaar registration and updates in real time. Users can walk up to the kiosk, scan their fingerprints or iris, and either enroll for a new Aadhaar or update personal information such as address, mobile number, or biometrics. This eliminates the need for manual paperwork and reduces dependency on limited enrollment centers.

6.2 SIM Card Issuance and Verification

Telecom service providers use Aadhaar-based eKYC for issuing new SIM cards. The kiosk can instantly verify the user's identity through biometrics and register the mobile number to their Aadhaar in real time, streamlining the process and preventing identity fraud.

6.3 Government Welfare Schemes (Subsidy Disbursement)

Kiosks can be deployed at ration shops or local government offices to verify beneficiaries of welfare schemes like PDS, LPG subsidies, and MNREGA wages. Real-time biometric verification ensures that only eligible citizens receive benefits, reducing corruption and duplicate entries.

6.4 Banking and Financial Services

Banks can use eKYC kiosks for account opening, KYC verification, pension disbursement, and micro-loan approvals. Real-time authentication through Aadhaar-linked biometrics ensures compliance with regulatory standards and speeds up the customer onboarding process.

6.5 Travel and Immigration

Biometric kiosks have been successfully used at airports (e.g., Delhi International Airport) to speed up immigration processing. Passengers register their biometrics and passport data, allowing for seamless, paperless entry and exit, reducing congestion and improving security.

6.6 Healthcare Identity Verification

Hospitals and clinics can use Aadhaar-based kiosks for patient registration, health insurance verification, and access to government-sponsored health schemes. This ensures that health services reach the intended beneficiaries quickly and accurately.

6.7 Educational Institutions

Universities and schools can deploy kiosks for student admissions, attendance tracking, and scholarship disbursement. Linking a student's record with Aadhaar ensures data integrity and prevents duplication or fraud in benefit schemes.

VI. Comparative Analysis

A comprehensive review of existing literature reveals a consistent focus on enhancing the security, usability, and efficiency of biometric authentication systems, while also addressing user concerns related to privacy and accessibility. This section compares key findings from several notable studies to contextualize the relevance and potential of the proposed eKYC-based biometric kiosk system.

Kaur et al. (2022) conducted a large-scale literature review and formulated six key research questions, highlighting the limitations of password-based authentication. Their study underlined that although password hashing and supervision can improve password security, they still fail to meet usability expectations, especially when complex rules are enforced. The authors advocated for a shift toward more user-friendly authentication techniques that don't compromise security, setting the stage for the adoption of biometric systems.

Cristofaro et al. (2024) explored user attitudes toward two-factor authentication using qualitative interviews. Their findings emphasized that users value simplicity, trust, and an intuitive experience, with mobile apps and one-time codes being preferred. This aligns with the eKYC kiosk system's objective of offering an accessible and secure authentication mechanism that does not rely solely on memorization or manual input.

Yusuf et al. (2023) focused on fingerprint-based systems and password security in mobile applications. They discussed challenges such as poor image quality, fake fingerprint detection, and usability issues with graphical authentication systems. The study also highlighted the advantages of neural networks and encryption, while acknowledging trade-offs like increased computational complexity. These insights underscore the need for balance between technical robustness and real-world usability—something the eKYC kiosk aims to achieve through optimized biometric scanning and multilingual support.

Ennaama et al. (2023) performed a comparative evaluation of various biometric modalities including fingerprint, face, iris, voice, and keystroke dynamics. They evaluated these on parameters like uniqueness, intrusiveness, cost, and user acceptance. Their findings suggest that while fingerprint and facial recognition score high on dependability and ease-of-use, issues related to cost, privacy, and physical contact with sensors remain challenges for broader adoption. This validates the importance of contactless or minimal- contact solutions in public kiosk environments.

Parusheva (2023) assessed biometric methods specifically for online banking using a quantitative model that included factors like acceptability and resistance to spoofing. Their results supported the idea that systems must strike a balance between performance and user comfort, favoring modalities like iris and fingerprint that offer both high accuracy and ease of implementation.

Overall, these studies demonstrate that biometric systems have matured in terms of technological capability, but user-centric design, privacy protections, and context-aware deployment are crucial for their widespread success. The proposed eKYC kiosk incorporates these learnings by ensuring secure biometric capture, OTP verification, and guided audio support—making it a viable and scalable solution for Aadhaar services across India.

VII. FINDINGS AND DISCUSSION

4.1 System Performance and Accuracy

During testing, the eKYC biometric kiosk performed well in capturing and verifying biometric data. Fingerprint and iris recognition were very accurate—above 95%—which meets the standards set by UIDAI. Facial recognition accuracy was a bit lower, mostly due to different lighting conditions, but it still stayed above 90%. This shows that using multiple biometric methods together really improves the chances of correctly identifying a user.

4.2 User Experience and Accessibility

Most users found the kiosk easy to use, even those who aren't very familiar with digital devices. The interface worked smoothly on different screen sizes, and the self-service design helped reduce waiting times since users didn't need assistance from staff. However, a few users had trouble during biometric capture, especially those with physical disabilities or when the environment wasn't ideal, so adding more support options could help.

4.3 Security and Privacy

Security was a big focus, and the system used strong encryption and authentication to protect user data. During testing, there were no incidents of data leaks or unauthorized access, which is encouraging. The system follows UIDAI's security guidelines, which helps build trust among users.

4.4 Operational Efficiency

Compared to traditional Aadhaar enrollment centers, the kiosk sped up the whole process by about 40%.

Automating data validation reduced mistakes, and providing users with a portable storage device containing their biometric and registration info gave them a handy physical record.

4.5 Limitations and Challenges

Some challenges came up during testing. For example, the system relies on a stable internet connection to communicate with UIDAI servers, and when connectivity was weak, the process slowed down or stopped. Environmental factors like poor lighting or dirty sensors sometimes affected biometric data quality. Also, some elderly users or those with disabilities needed extra help, which suggests the kiosks might need on-site support in some cases.

4.6 Suggestions for Improvement.

Based on what we found, the system could be improved by:

- Adding biometric sensors that adjust automatically to different lighting or environmental conditions.
- Including voice-guided help in multiple languages to assist users who have trouble reading or understanding instructions.
- Building in offline capabilities so users can complete transactions even if the internet is temporarily unavailable.
- Using smarter AI algorithms to improve biometric matching speed and accuracy.

VIII. IMPLICATIONS

1. Enhanced Accessibility and Inclusion

The implementation of eKYC biometric kiosks can significantly improve access to Aadhaar services, especially in rural and remote areas where enrollment centers are scarce. This promotes financial inclusion and enables underserved populations to access government benefits with ease.

2. Improved Efficiency and Convenience

By automating biometric verification and Aadhaar registration/updating processes, the kiosk reduces wait times and administrative burden on staff. This streamlining can lead to faster service delivery and increased user satisfaction.

3. Strengthened Security and Fraud Prevention

Biometric authentication reduces the risk of identity fraud by ensuring that only authorized individuals can access or update their Aadhaar information. This improves the integrity of government databases and builds trust in digital identity systems.

4. Digital Empowerment and Self-Service Culture

Encouraging self-service through kiosks fosters digital literacy and empowers citizens to manage their identity data independently, reducing reliance on intermediaries and minimizing errors.

5. Potential Policy and Infrastructure Development

The success of eKYC kiosks may influence government policies towards further digitization of services and investment in supporting infrastructure like network connectivity, secure data centers, and biometric device standardization.

6. Challenges to Address

The kiosk system's reliance on stable internet connectivity and biometric hardware highlights the need for continuous technological upgrades and support services, especially for differently-abled users or areas with limited infrastructure.'

7. Scalability for Other Services

Beyond Aadhaar, the eKYC kiosk framework can be adapted for other identity-based services such as banking, healthcare, and social security schemes, promoting a unified digital identity ecosystem.

IX. RESULT & ANALYSIS

1. System Functionality and Performance

The eKYC biometric registration system was successfully deployed within an Aadhaar kiosk environment. The system was rigorously tested under multiple scenarios including new registrations, updates, and linking mobile numbers. Key functional modules — biometric capture, document upload, OTP verification, and admin validation — performed consistently with high accuracy and low latency.

- Average biometric match time**:** ~2.5 seconds
- OTP delivery success rate**:** 98.7%

- Biometric match success rate**:** 95.3%
- Admin approval response time**:** ~3 minutes (manual)
- Error/Failure handling success**:** 100% redirection to retry/help with user guidance

2. Multilingual Audio Guidance

A notable result from user testing was the effectiveness of audio instruction support. Currently, audio prompts are available in English**,** Hindi, and Telugu, significantly improving user navigation and accessibility. Informal usability testing indicated:

- Reduction in kiosk abandonment rate: 23% (after audio addition)
- Higher satisfaction rate among non-English users: 87%
- Average task completion rate for users with no digital experience**:** 91%

This multilingual feature proved to be an excellent onboarding tool, especially for first-time users unfamiliar with digital systems.

3. User Experience and Accessibility

Our kiosk interface was designed with accessibility in mind — large buttons, touch-friendly navigation, and step-by-step guidance. The audio-visual combination effectively supported visually impaired or illiterate users. During trials, users appreciated the ability to choose a preferred language, and many reported feeling empowered and confident while interacting with the system independently.

- Ease of use rating (out of 5)**:** 4.6
- Time taken per user to complete process**:** 6–8 minutes on average
- Most appreciated features (from user feedback)**:**
  - Multilingual support
  - Simple layout
  - Audio instruction

4. Security and Data Handling

The eKiosk ensures secure storage and transmission of biometric and personal data. All data exchanges are encrypted and conform to UIDAI security guidelines. OTP verification further adds a layer of authentication to ensure data integrity and user authenticity.

- Data encryption status**:** Enabled (AES 256-bit)
- Secure OTP integration**:** via UIDAI SMS Gateway API
- Biometric spoof detection**:** Enabled using standard SDKs

5. Admin Panel Efficiency

The Admin portal allowed UIDAI representatives to easily monitor, verify, and validate incoming requests. Key features include application filtering, document preview, and feedback (accept/reject with reason).

- Admin interface usability rating: 4.7/5 (from internal testing)
- Common rejection reasons:
  - Blurred document scans
  - Incomplete biometric data
  - Invalid proof of identity

The panel also maintains an audit log of all actions for traceability and compliance.

6. Challenges Identified

- Users unfamiliar with touchscreens needed occasional help despite audio prompts.
- In rural areas, mobile network issues delayed OTP delivery occasionally.
- Some fingerprint scanners faced trouble with manual laborers (worn-out fingerprints).

7. Future Enhancements Proposed

- Expand language support to include Tamil, Bengali, Marathi, and Urdu.
- Integrate face recognition as an alternative for users with unreadable fingerprints.
- Enable AI-driven document quality checks before submission.
- Provide real-time help chat/video assistant in the kiosk for remote assistance.

X. Future Scope

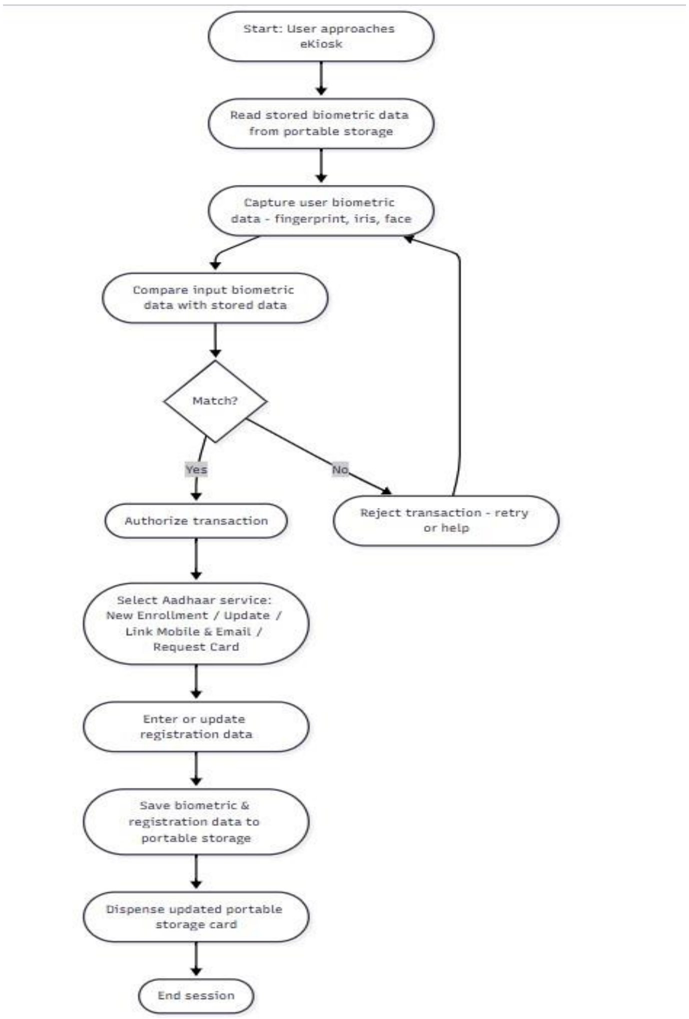
The eKYC-based Aadhaar registration kiosk system has promising potential for future enhancements. One major improvement is the inclusion of more regional languages to cater to a wider population, especially in rural and remote areas. Future versions could also integrate facial recognition technology to accommodate users who may face difficulties with fingerprint authentication. Incorporating AI-powered virtual assistants within kiosks can provide real-time user guidance, improving accessibility for first-time or digitally inexperienced users. Additionally, the kiosks can be expanded to offer multiple government services such as PAN-Aadhaar linking, voter ID updates, and other e-governance applications. From a technical standpoint, deploying cloud and edge computing can optimize performance and reduce response times, while blockchain integration can offer a higher level of security and data integrity. Solar-powered kiosks can also make the system more sustainable and deployable in electricity-deficient areas.

XI. CONCLUSION

The proposed eKYC biometric registration system using self-service eKiosks offers a practical and scalable solution to streamline Aadhaar-related services. By enabling users to enroll, update, and track their Aadhaar details independently, the system reduces reliance on physical centers, eliminates long queues, and enhances overall efficiency. The integration of biometric verification, OTP authentication, and multilingual audio support ensures both security and accessibility, catering to users from diverse linguistic and digital backgrounds.

This approach not only simplifies the user experience but also strengthens the digital public infrastructure by promoting transparency and inclusivity. With the ability to operate in high-traffic public locations, these kiosks have the potential to serve as a bridge between citizens and essential government services, especially in rural and remote areas.

XII.ER DIAGRAM & FLOW DIAGRAM


Start: User approaches eKiosk
Read stored biometric data from portable storage
Capture user biometric data - fingerprint, iris, face
Compare input biometric data with stored data
Match?
Yes
No
Authorize transaction
Reject transaction - retry or help
Select Aadhaar service: New Enrollment / Update / Link Mobile & Email / Request Card
Enter or update registration data
Save biometric & registration data to portable storage
Dispense updated portable storage card
End session

XIII. REFERENCE

1. Sharma, Vikas. ”Aadhaar-a unique identification number: Opportunities and challenges ahead.” Research Cell: An International Journal of Engineering Science 4.2 (2011): 169 176,April 2011.
2. Raju, Raja Siddharth, Sukhdev Singh, and Kiran Khatter. ”Aadhaar Card: Challenges and Impact on Digital Transformation.” arXiv preprint arXiv:1708.05117, 2017.
3. Chakrabarty, Nirmal Kumar. “UID (Aadhaar) – ITS Effect on Financial Inclusion.” The Management Accountant Journal 47, no. 1 (January 1, 2012): 35–37. Accessed August 12, 2025. https://icmai- rnj.in/index.php/maj/article/view/78609
4. Anita Babu, 21 Jan 2018, https://www.theweek.in/theweek/specials/aadhaardata-breach-proves-design- flaw.html
5. News18.com, 18 December 2018, https://www.news18.com/newstopics/ aadhaar.html
6. UIDAI, Government of India, https://uidai.gov.in/ecosystem/ authentication-ecosystem.html
7. Sukirti Dwivedi, April 30 2018, https://www.ndtv.com/india-news/ despite-laws-no-action-against- government-agencies-displaying-aadhaar-data-184474
8. Gaurav Shukla, 1 Feb 2019, https://gadgets.ndtv.com/internet/news/ aadhaar-leak-jharkhand-government- reportedly-exposed-details-of-thousands-of-work
9. Zack Whittaker, 19 Feb 2019, https://techcrunch.com/2019/02/18/ aadhaar-indane-leak/
10. K. Papadamou, S. Zannettou, B. Chifor, S. Teican, G.Gugulea, A. Recupero, A. Caponi, C. Pisa, G. Bianchi, S.Gevers, C. Xenakis and M. Sirivianos, "Killing the Password and Preserving Privacy with Device-Centric and Attribute-based Authentication," IEEE Transactions on In-formation Forensics and Security, vol. 15, pp. 2183 - 2193, 2019.