International Journal of Research in Interdisciplinary Studies
Volume 3, Issue 12, December 2025
https://www.ijris.com | ISSN (Online): 2584-1017

Biometric Authentication Revolution: The Role of AI and UIDAI in Digital Payments

Karrn Kumar[1], Swati Kumari[2], Ashok Kumar[3], Chandan Kumar[4], Priya Kumari[5], Anuradha Sharma[6*], Kumar Amrendra[7]

[1,2,3,4,5]*Student, Department of Computer Science Engineering and Information Technology, Jharkhand Rai University, Ranchi, India*
[6,7]*Assistant Professor, Department of Computer Science Engineering and Information Technology, Jharkhand Rai University, Ranchi, India*

Abstract—Although UPI and Aadhaar have revolutionized the payments environment in India, QR codes, mobile applications, cash, and cards continue to play a significant role in retail transactions. At the point-of-sale (POS), a novel dual-factor authentication payment method that combines a user PIN with an Aadhaar-linked fingerprint has been suggested in this paper. With this approach, the consumer only has to touch a verified fingerprint scanner at the merchant's terminal, input a PIN, and use India's Aadhaar infrastructure to settle the payment from account to account. This makes advantage of the current AEPS (Aadhaar Enabled Payment System) and NPCI rails to transfer money in real time from the payer's bank to the payee's bank and authenticate the user using UIDAI. In addition to discussing security, privacy, consent, and reliability issues, the paper describes the system architecture in depth, including biometric hardware, PIN input, UIDAI connection, and AI fraud analytics. This paper shows how a similar idea with common fingerprint sensors might be implemented in India by taking inspiration from China's palm-vein payment terminals. There are discussion of implementation issues such device pricing and rural connection. We contend that India's transition to a fully cashless, inclusive, and secure digital payment ecosystem might be accelerated by using this fingerprint+PIN strategy.

***Index Terms*—Aadhaar Enabled Payment System (AEPS), Biometric Authentication, Fingerprint Scanner, UIDAI, NPCI, Fraud Detection, Privacy, Digital Payments, Financial Inclusion.**

1. Introduction

Billions of transactions are now routine thanks to India's digital payment revolution (UPI and Aadhaar) [3], [4]. Nonetheless, retailers continue to rely on consumers swiping their cards or scanning QR codes in numerous shopping situations. These techniques need cards or cellphones and create friction (opening applications, scanning codes). The paper suggest replacing these with a fingerprint-and-PIN system, in which the customer authenticates at the register by providing a PIN and a brief fingerprint scan on an Aadhaar-certified terminal. Instead of using app-based techniques for user authentication, this strategy makes use of the current Aadhaar biometric infrastructure, which is already connected to all bank accounts. In addition to a secret PIN, Aadhaar biometrics (inherence factor) can fulfill the Reserve Bank of India's current requirement for two-factor authentication for digital payments [5]. To connect a customer's Aadhaar biometric to a bank account or payment app, opt-in agreement is required at the time of enrollment. Only an Aadhaar-enabled point-of-sale device (micro-ATM or smartphone) with a PIN pad and a validated fingerprint reader is required for the business.

The design of such a system is presented in this paper. In short, a consumer chooses to pay a retailer using their fingerprint. The customer's fingerprint is taken, their Aadhaar number is retrieved (or read from a card), and a PIN is requested by the merchant's device. After then, NPCI's AEPS switch receives an encrypted authentication request and gets in touch with UIDAI for biometric verification. After a successful match, the system completes an account-to-account transfer by debiting the customer's bank account and crediting the merchants. We take use of the fact that cross-bank transfers using Aadhaar are already made possible by AEPS [6]. With the addition of the PIN for increased security and convenience, our innovation is expanding this concept to regular retail purchases. Similar to newly introduced biometric terminals in China [1], [2], biometric authentication enables cardless, tap-to-pay convenience; however, it has been modified for India's Aadhaar stack.

The paper is arranged as follows: Section II examines comparable systems, such as China's palm solution and India's AePS, as well as worldwide biometric payments. The suggested design and flow are described in depth in Section III. Security, privacy, and dependability are covered in Section IV. Implementation issues (cost, connection) are covered in Section V. The palm payment methodology in China is compared in Section VI. The possible effects on inclusive, cashless payments in India are finally covered in Section VII.

2. Background: Aadhaar and Biometric Payments

A. Aadhaar-Enabled Payment System (AEPS)

In remote locations, banking access has already been made possible by India's Aadhaar biometric ID. Through AEPS, people may use fingerprint/iris authentication to make cash withdrawals, deposits, and fund transfers through micro-ATM machines [6], [7]. AEPS operates as follows: the merchant obtains the client's Aadhaar number and biometric (fingerprint)

*Corresponding author: anuradha.shrama85@gmail.com

when the consumer requests a transaction at the merchant (who serves as a banking correspondent using a certified biometric device) [5]. The NPCI switch receives the encrypted fingerprint and transaction information before sending UIDAI an authentication request. After comparing the fingerprint to its database, UIDAI provides a yes/no response [8]. When it is successful, NPCI credits the merchant's bank account and debits the customer's bank [9].

Even in remote places where there are few other payment options, this complete process takes place in a matter of seconds. Crucially, AEPS only needs biometric identification from the client; no cards or smartphone apps are needed. For retail payments, we use this tested Aadhaar-based pipeline, which results in a digital transfer rather than a cash withdrawal to cover the cost of items.

B. UPI and Multi-Factor Authentication

Digital commerce has been accelerated by the Unified Payments Interface (UPI), which currently processes around 20 billion transactions monthly [10], [3]. Stronger authentication was recently enforced by authorities; the RBI now needs two different factors for all digital payments [5]. As an optional substitute for PINs, NPCI is allowing biometric (fingerprint/face) verification for UPI transactions [4], [5]. In this regard, the national drive for biometric security is consistent with our suggested fingerprint+PIN solution. Our approach leverages Aadhaar's centralized authentication, which means that any fingerprint, independent of phone capacity, may authenticate via UIDAI, in contrast to mobile-wallet biometrics, which confirm identification on a smartphone. This makes it extremely inclusive by eliminating the requirement that every consumer own a smartphone.

C. Biometric Payments Globally

Biometric checkout is becoming more and more popular worldwide. For instance, WeChat and Alipay have implemented palm vein scanners for payments in China [1], [11]. These gadgets provide a unique biometric template by mapping internal vein patterns using near-infrared imaging [2]. After creating an account and connecting their palm profile to a payment account, users may pay by only placing their palm close to the sensor. Similar technologies that permit no-phone, no-card transactions have been tested in university and transportation environments [11]. Due to the difficulty of spoofing the palm's subsurface patterns, these contactless palm devices are regarded as extremely secure [12]. Since fingerprint biometrics via Aadhaar are currently used for payments in India (e.g., AePS), our methodology is based on China's strategy but makes use of the more widely used fingerprint modality. This contrast is covered in Section VI.

3. Proposed System Architecture

The proposed system integrates biometric authentication hardware with the Aadhaar/NPCI infrastructure to enable direct bank-to-bank retail payments. Figure 1 shows the high-level architecture (described below).

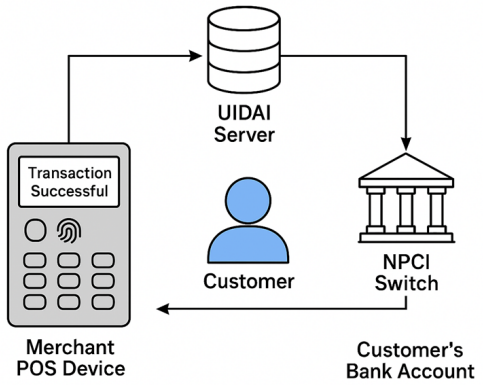

Fig. 1. A merchant's point-of-sale device equipped with an Aadhaar-certified fingerprint scanner and PIN pad directly connects to the NPCI switch and UIDAI servers. The customer is authenticated via UIDAI and funds are transferred from the customer's bank account to the merchant's account

A. Hardware Components

- *Fingerprint Scanner*: An optical or capacitive sensor that complies with Aadhaar and has received STQC certification, such as Mantra or SecuGen L1 devices [13]. These can take high-quality 10-fingerprint photos and cost a few thousand rupees. In accordance with UIDAI requirements, the gadget sends and encrypts the fingerprint instantly; it is not permitted to permanently keep any raw biometric data [14].
- *PIN Entry Device*: An integrated or connected secure keypad that allows the user to input a PIN in the form of numbers. The second factor is this PIN. It may be installed on a reliable smartphone or be a stand-alone hardware module. Both local (against a saved hash) and backend (as with ATM PIN verification) methods are used to verify the PIN.
- *Mobile POS / Micro-ATM Terminal*: A mobile device that runs the payment app, such as a ruggedized Android tablet, is called a mobile point-of-sale (POS) or micro-ATM terminal. This terminal has internet access (5G/4G/3G/Wi-Fi) and is connected to the scanner and keypad. It can sync when connectivity is available and save transactions offline in off-grid situations.
- *Connectivity*: The terminal connects to the NPCI AEPS switch via network access, either broadband or cellular. Internet is becoming more accessible in rural regions with poor connection thanks to BharatNet and cell coverage increases [15]. We also take store-and-forward into account, which allows the device to queue the transaction and push it later if it is offline.
- *Aadhaar-Linked Bank Accounts*: In accordance with the Jan Dhan/Aadhaar/UPI reforms, every user needs to have a bank account that is seeded with Aadhaar [16]. Every merchant, even micro-merchants, is required to keep a bank account under Jan Dhan initiatives. The transfer's endpoints are these accounts.

B. System Flow

The payment flow adapts the AePS process (Steps below) with a key difference: instead of cash withdrawal, the end result

is a transfer to the merchant. The steps are:

- *Initiation*: The merchant speaks or inputs the transaction amount into the POS system at the point of sale. Through input or card entry, the customer's Aadhaar number is verified.
- *Dual Authentication*: The client inputs their secret PIN on the keypad while placing a finger on the scanner.
- *Send Auth Request*: An encrypted request is generated by the terminal that includes the transaction amount, the Aadhaar ID, the encrypted fingerprint template, and the PIN (either hashed or encrypted). This is sent to the NPCI's AEPS platform via the acquiring bank's FI (Financial Inclusion) switch [17].
- *UIDAI Verification*: NPCI sends the customer's Aadhaar ID and fingerprint information together with a "Aadhaar-auth" request to UIDAI's server [8]. The fingerprint is compared to UIDAI's database. UIDAI replies with an authentication success if the user's account is legitimate and their biometrics match. To meet the criteria of two-factor authentication, the user's bank or the NPCI may additionally validate the PIN.
- *Transaction Settlement*: After successful authentication, the NPCI switch directs the payee's bank to credit the merchant's account while also instructing the payer's bank to debit the customer's account for the amount. The settlement mechanisms of NPCI are used for these interbank transfers. (This is comparable to an Aadhar-to-Aadhar money transfer that AePS now supports [18].)
- *Confirmation*: NPCI notifies the merchant banks as well as the client banks. The merchant's account is credited, and the consumer receives an SMS confirming the debit [19]. A receipt or an on-screen success message is printed or dispensed by the terminal. The money has been paid in full.
- It takes a few seconds to complete this process. Importantly, the Aadhaar biometric and PIN are sufficient; neither a QR code nor a UPI app on the customer's phone are needed. The device may wait for connectivity while in offline mode before completing the transaction.

C. Software and Integration

- The POS app uses NPCI to connect to the UIDAI Authentication API. According to UIDAI regulations, fingerprints can only be captured and sent by registered Aadhaar devices [14]. By leveraging Aadhaar's core SDK and removing biometrics, for example, the app guarantees compliance.
- *Security and Encryption*: Strong TLS is used to encrypt all data received to NPCI/UIDAI. Before being sent, the fingerprint template is encrypted on the device (UIDAI internally utilizes AES/RSA). We make sure that just Aadhaar ID and biometrics—no personally identifiable information, or PII—leave the device in plaintext.
- *AI-based Fraud Detection*: Machine-learning analytics are used on transaction data by the back-end network (NPCI or issuing banks) [20], [21]. AI is capable of analyzing patterns such as anomalous device IDs, transaction velocity, many unsuccessful PIN tries, unexpected spending amounts, and geographic anomalies. A model detects differences in user behavior and learns from it continually. The system may request more checks or reject the payment if a transaction appears suspicious (for example, a changing state, a new fingerprint pattern, or a high number of quick tries). It is possible to improve the model while protecting user data by using federated learning approaches [21]. Furthermore, liveness detection algorithms built into fingerprint sensors itself may verify that a finger is real (to avoid spoofing).

4. Security, Privacy, Consent

- Biometric payments raise important security and privacy questions. Our design adheres to UIDAI and RBI guidelines.
- *Encrypted Biometric Transmission*: The fingerprint is instantly encrypted on the scanner and transmitted to UIDAI in accordance with UIDAI protocol, no raw fingerprint pictures are saved locally [14]. Only an encrypted, transient template is stored on the device. The biometric information is deleted after authentication. This conforms with the Aadhaar Authentication Regulations' Regulation 17(1), which prohibits keeping fingerprint duplicates on file [14].
- *Dual-Factor Authentication*: By using both the fingerprint and the user's PIN, the dangers of the biometric being replayed are reduced. The transaction cannot be completed without the PIN, even if a fingerprint template were intercepted. The combination of fingerprint and PIN is now compliant due to the RBI's new demand for two factors [5]. The PIN itself may be generated by the bank or generated within the payment app. The bank hashes and verifies it; it is never delivered in clear.
- *Consent and Registration*: Using biometrics to make payments requires consent from the customer. This may be accomplished by upgrading UPI applications to permit biometric approval or by entering their fingerprint in the bank's database. Only anonymised biometric data is provided, and consent is specifically sought. A consent framework already governs the operation of UIDAI's e-KYC and authentication APIs. Explicit fingerprint re-authentication may be required for high-value transactions.
- *Data Localization and Regulation*: All authentication takes place on Indian servers, following China's lead. Government infrastructure does not lose access to UIDAI data. Only identification verification is done using Aadhaar data; NPCI does not receive any personal information other than "yes/no." We also adhere to data minimization: the merchant only ever receives an identification confirmation and never learns any biometric information. Transaction metadata belonging to the consumer is protected and utilized exclusively for fraud monitoring and dispute settlement.
- *User privacy*: We stress that the biometric picture is not used, just the fingerprint template. Customers can lock their Aadhaar biometrics (as permitted by UIDAI) to cancel their

biometric consent at any time. Because fingerprints cannot be altered if hacked, they are subject to strict security measures, unlike static tokens. Advanced techniques like tokenization, which is comparable to Tencent's claim [12], might be used for increased privacy. Replay attacks would be rendered useless if a device converted the fingerprint to a one-time token for UIDAI authentication.

- *Measures of Reliability*: The system has to be very accessible. Backup connectivity is built into POS equipment (e.g. SIM cards from several providers). In case of power disruptions, they feature a battery backup. Transactions are not lost due to temporary failures because to automated retry logic. For audit purposes, timestamps and transaction IDs are recorded for every interaction. The device should safely reverse any state and alert both parties in the event of a network outage during the transaction.

5. Implementation Challenges

While promising, deploying fingerprint-PIN payments at scale in India entails challenges:

- *Connectivity in Rural Areas*: According to banking authorities, there are internet gaps when implementing UPI in rural and tribal areas. Reliable data connectivity is still lacking in many communities. This is lessened by our system's use of tiny payloads and tolerance for sporadic networks. With approximately 214K village councils linked by 2024 [15], BharatNet has significantly increased the accessibility of internet; yet, issues with electricity and cell coverage still exist. In the short term, offline-capable modes—batch processing of transactions once they are online—are deemed crucial.
- *Cost of Biometric Terminals*: Compared to basic QR code installations, high-quality Aadhaar-certified fingerprint scanners and point-of-sale machines are more costly. An L1 Aadhaar fingerprint device, for instance, can cost between ₹2,000 and ₹3,000 (about $25 to $40 USD) per. It will cost a lot of money to install them in millions of stores. Dedicated scanners are more expensive than smartphones, which come with built-in fingerprint readers. The devices may be subsidized by governments or payment corporations, or hybrid terminals (POS machines that combine fingerprint scanning with card readers) may be used. One major obstacle to biometric payments, according to the Payments Journal, is equipment cost. Prices should eventually drop as a result of competition and economies of scale.
- *Infrastructure and Training*: Merchants need to have the necessary tools and training. It takes technological know-how to turn a kirana shop into a "biometric POS agent." User interfaces need to be very basic (maybe multilingual, icon-driven) because many shops are semiliterate or from rural areas. Another problem is power reliability; equipment may require battery backup. To register devices and troubleshoot, support centers or BC-networks (like those for AePS) will be required.
- *User Acceptance and Privacy Issues*: Following recent discussions over Aadhaar privacy, some customers could be hesitant to provide their fingerprints at the register. It is crucial to maintain openness by stating that fingerprints are only used for one-time authentication and are not retained by merchants. To establish trust, UI/UX design and client education initiatives would be required. Furthermore, additional accommodations must be provided for individuals who cannot provide their fingerprints (disabled) or who have worn fingerprints (elderly, workers); possibly alternate iris or facial modes might be offered.
- *Regulatory and Security Compliance*: Although biometric authentication is now encouraged by the RBI [4], official rules governing biometric payments may yet change. It will be crucial to make sure that proposed data protection regulations and cyber-security standards are followed. Device STQC certification and ongoing security audits will be required. Even hypothetical security or privacy flaws might compromise the application.
- *Competition with the Current Ecosystem*: India currently has cardless digital payments that are competitive. Banks and merchants need to be persuaded that this new approach offers benefits beyond UPI QR scans. To encourage adoption, it could be necessary to integrate with loyalty programs or offer simpler rewards free of transaction costs.

6. Comparison with China’s Palm Payment Model

Though there are some significant distinctions, our solution is essentially based on China's developing biometric checking systems. Tencent and Alipay have introduced palm-vein payment terminals in China [1], [11]. To scan users' palm vein patterns, authenticate against a connected wallet, and complete transactions, these devices employ contactless near-IR sensors (for instance, Alipay's PL1 gadget does away with the need for cards or PINs [1]). These palm systems are praised for their quickness and cleanliness and offer a very low false acceptance rate (one in a million).

Similarity: Our technology facilitates cardless, biometric checkouts, just like China's model. Both strive for a smooth experience in which the user does not have to show any tangible identification. We also adopt the dual-layer security concept: although we combine the fingerprint with a PIN, China's palm reader analyzes both surface palm prints and vein patterns . To preserve anonymity, both strategies make advantage of local template storage and safe encryption [12].

Differences: The technological stack and environment in India are different. Specialized, contactless, and costly technologies designed for high-volume events are palm scanners [1], [2]. On the other hand, hardware is more prevalent and fingerprints are already extensively enlisted (each person's

Aadhaar has 10 fingerprints). Instead than integrating a proprietary wallet, we make use of the already-existing Aadhaar database and NPCI network. In contrast to China's models, which now employ specialized terminals, our hardware (fingerprint scanner + keypad) is less expensive and flexible, allowing it to be added to any POS system. Regarding privacy, India's Aadhaar system likewise maintains data centralization but never provides merchants with raw biometrics, whereas China's systems tokenize and retain biometric data domestically [12].

Therefore, our fingerprint+PIN design is adapted to India's legal framework (Aadhaar legislation) and payment infrastructure (NPCI), even if Chinese palm payments show the user convenience and security potential. With technology that is currently approved and available in India, we expect many of the advantages (such as quick checkout and fraud protection).

7. Contribution to Cashless and Inclusive Payments

India's transition to a cashless economy might be greatly accelerated by this fingerprint-based technology. Nearly 90% of persons with bank accounts, even those without smartphones, may now use digital payments using Aadhaar-linked bank accounts. With just a fingerprint and PIN, even underbanked groups (such as farmers and daily wage laborers) may make digital payments at nearby stores, decreasing their need for cash. Security is further addressed by the dual-factor approach: biometrics linked to an individual's distinct physiology lower fraud, in contrast to phishable one-time OTPs [1].

Additionally, using AI fraud analytics gradually improves the ecosystem's intelligence [20], [21]. Each transaction improves the system's comprehension of typical behavior, assisting in the detection of counterfeits or stolen credentials. Additionally, the design expands upon India's Digital Public Infrastructure philosophy (Jan Dhan-Aadhaar-UPI) [16] by being open, interoperable, and governed by the public sector (NPCI/UIDAI), all of which promote confidence. If extensively used, it might legitimize more economic activity, reduce merchant MDR fees (no middlemen), and establish UPI as the biggest real-time payments system in the world [3].

8. Conclusion

To facilitate cashless, account-to-account retail transactions, this paper suggests a fingerprint-and-PIN payment authentication system that makes use of India's Aadhaar and AEPS infrastructure. By using pre-existing biometric identity data, this approach eliminates the requirement for QR code scans or cards. The technological architecture includes secure PIN entry, validated fingerprint sensors, NPCI's payment switch, UIDAI's Aadhaar auth APIs, and AI fraud detection. The research described the steps taken to address data privacy and security issues (permission procedures, encrypted templates, and the avoidance of storing raw biometrics) [14]. Biometric checkouts can operate at scale, as demonstrated by China's palm payments [1], [2], but India's extensive Aadhaar network offers us a remarkably wide base. Although there are still obstacles to overcome, such as user trust, device deployment costs, and connection in rural places, this is made possible by continuing infrastructural advancements like BharatNet [15] and regulatory assistance like RBI's dual-factor rule [5].

In conclusion, a fingerprint+PIN payment paradigm has the potential to greatly contribute to India's digital payment revolution by making routine payments quicker, safer, and more inclusive. This strategy, which builds on the successful Aadhaar/UPI systems, encourages a cashless economy in which even rural stores and street sellers may take digital payments with just a pin and fingerprint scan.

References

[1] ID Tech, "Alipay launches contactless palm print payment system in China," *IDTechWire*, Apr. 2025. [Online]. Available: https://idtechwire.com/alipay-launches-contactless-palm-print-payment-system-in-china/

[2] "Palm reading for payments: China's biometric leap and the legal maze ahead," *The Cashless Society*, 2025.

[3] Press Information Bureau, Government of India, "UPI: India's digital revolution goes global," *PIB Features*, Jun. 24, 2025. [Online]. Available: https://www.pib.gov.in/FeaturesDeatils.aspx?NoteId=155224&ModuleId=2

[4] W. Grant, "UPI is set to add biometric authentication for real-time payments," *Payments Journal*, 2025.

[5] J. McConvey, "India introduces face authentication for payments in UPI," *Biometric Update*, 2025.

[6] R. Garg, "Security challenges in Aadhaar-enabled payment systems," *Frugal Testing Blog*, Jul. 2025.

[7] Mantra Softech, "Biometric micro ATM for AePS," *Product Brief*, Mantratec, 2025.

[8] India Brand Equity Foundation (IBEF), "BharatNet unplugged: Transforming rural connectivity in India," *IBEF Reports*, 2025.

[9] TSYS, "AI & biometrics: A perfect match made in payment authentication?," *TSYS Insights*, Aug. 2025.

[10] "Financial inclusion still faces challenges in rural, tribal areas: Finance Secy M. Nagaraju," *The Tribune*, Oct. 2025.

[11] W. Grant, "Palm scanning gains ground as retail biometric of choice," *Payments Journal*, 2025.

[12] A. K. Komarraju, M. Ramprasad, and M. B. Rao, "Enhancing digital payment security with biometric authentication and AI: A big data approach," *Int. J. Eng. Comput. Sci.*, vol. 13, no. 4, 2024.

[13] A. Mittal, "Enhancing payment security: The role of biometric authentication and tokenization," *Int. J. Comput. Eng. Technol.*, vol. 16, no. 1, 2025.

[14] S. D. Adhiyamaan and R. K. Mishra, "The role of biometric authentication in securing digital identities," *Univ. Res. Rep.*, vol. 11, no. 4, 2025.

[15] G. K. Patra, S. K. Rajaram, and V. N. Boddapati, "AI and big data in digital payments: A comprehensive model for secure biometric authentication," *Educ. Admin.: Theory Pract.*, vol. 25, no. 4, 2019.

[16] C. Kuraku, H. K. Gollangi, and J. R. Sunkara, "Biometric authentication in digital payments: Utilizing AI and big data for real-time security and efficiency," *Educ. Admin.: Theory Pract.*, vol. 26, no. 4, 2020.

[17] D. Sadhya, "A critical survey of security and privacy aspects of the Aadhaar framework," *Comput. Secur.*, vol. 140, Art. no. 103782, 2024.

[18] Unique Identification Authority of India (UIDAI), *Authentication Ecosystem Overview*. UIDAI, Government of India, 2025.

[19] R. Brown, G. Bendiab, S. Shiaeles, and B. Ghita, "A novel multimodal biometric authentication system using machine learning and blockchain," *arXiv preprint*, arXiv:2109.03014, 2021.

[20] A. Ganmati, K. Afdel, and L. Koutti, "Deep learning-based multi-factor authentication: Biometric and smart card integration," *arXiv preprint*, 2025. (Identifier pending.)

[21] Unique Identification Authority of India (UIDAI), *Aadhaar Authentication and Offline Verification Regulations 2021*. Government of India, 2023.