Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Energizing ATM Security by Sending OTP to Aadhar Card-Linked Mobile Number and Using Fingerprint

K. Vasuki Devi [1], P. Vidhya Lakshmi [2], P. Vajila [3], A. TharikNazeem [4], RebeccaFernamdo. I.M.S.B [5], R. Subha [6]

[1] *Chennai Institute of Technology, Kundrathur, Chennai, Tamil Nadu, India. Email: k.vasukidevi@gmail.com*
[2] *Chennai Institute of Technology, Kundrathur, Chennai, Tamil Nadu, India. Email: vidhyapl1992@gmail.com*
[3] *Loyola Institute of Technology and Science, Kanyakumari, Tamil Nadu, India. Email: vajilavaji.p@gmail.com*
[4] *PSN Engineering College, Melathediyoor, Tirunelveli, Tamil Nadu, India. Email: thariknaims@gmail.com*
[5] *Grace College of Engineering, Mullakkadu, Thoothukudi, Tamil Nadu, India. Email: rebecca270496@gmail.com*
[6] *PSN Engineering College, Melathediyoor, Tirunelveli, Tamil Nadu, India. Email: rtsubha@gmail.com*

ARTICLE INFO

Received: 15 Mar 2025

Revised: 10 May 2025

Accepted: 18 May 2025

ABSTRACT

ATMs are utilized by everyone to withdraw and transfer money in today's environment. The implementation of fingerprint mechanisms in the ATM system served as the basis for this study. We chose this location in order to make transactions easier and safer for all clients. Each person's fingerprints have unique minute characteristics. You don't have to have your ATM card with you at all times, and you don't have to worry about losing it. It is shown that fingerprint technology outperforms and is safer than other technologies when compared to other technologies used for ATM security. It makes transactions simple and safe while preserving an environment that is easy to use for both users and ATMs. When it comes to electronic money transactions, this technology is the most promising. Sending OTP to Aadhaar-linked Phone Number. Aadhaar Linking: The user must have their mobile number linked to their Aadhaar card for this process to work. This number is stored in the bank's system as part of their KYC (Know Your Customer) records. OTP Generation: After fingerprint authentication, the ATM will trigger the bank's system to generate a one-time password (OTP).☐ SMS Delivery: The generated OTP is then sent via SMS to the mobile phone number linked with the user's Aadhaar account.

Keywords: Enhancing ATM, Security System for ATM, Biometric Base ATM, and Fingerprint Based ATM.

INTRODUCTION

Our primary goal is to use fingerprint-based ATMs to create a more secure system. Biometrics is a technique that helps make your data very safe and unique for each user based on their bodily attributes. Using a person's fingerprint, face, voice, iris, handwriting, hand geometry, and other biometric characteristics, biometric information is utilized to accurately identify them. There are a number of benefits of using biometric identification over existing and conventional techniques. Physical keys, smart cards, and magnetic stripe cards are examples of tokens that may be lost, stolen, copied, or left behind; passwords can be shared, forgotten, compromised, or unintentionally seen by a third party. Two primary purposes are provided by a biometric system. Identification is one method, and verification is the other. The most widely used and developed biometric technology is fingerprint technology, which is also the most straightforward to create and offers the highest degree of protection at the fingers. Getting one's fingerprints registered with a fingerprint identification device is simple to do and requires little time or work. Fingerprint recognition is therefore regarded as one of the least invasive biometric verification techniques. Thousands of years ago, officials utilized thumbprints to seal papers. Since the late 1800s, law enforcement has been employing fingerprint identification. The same method is used on digital platforms. Despite being first taken, fingerprint pictures are not stored anywhere in the system. Rather, the actual fingerprints were transformed into templates. not make it again. Therefore, it is impossible to misuse the system [1].

These days, self-service banking systems are quite popular since they provide outstanding client assistance around-the-clock. It is fairly usual to use the ATM (Automatic Teller Machine), which gives clients quick banknote

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

exchanging.However, financial fraud has been on the rise recently. Many thieves interfere with the ATM terminal and steal users' credit card and password using illicit ways. The thief takes all money in the shortest amount of time once the user's bankcard is lost and the password is stolen, causing the consumer to suffer a significant financial loss. In the current financial cycle, the attention shifts to how to maintain the customer's authentic identification. Conventional ATM systems typically use a credit card and password for authentication, however this approach has several drawbacks. The client's identity cannot be precisely verified using a credit card and password. The original password authentication method combined with biometric identification technology validates the clients' identities more effectively and accomplishes the goal of using ATMs to increase safety. In recent years, the algorithm that recognizes fingerprints has been updated continuously and sends the four-digit code by the controller, which has given us new verification means. [2].

EXISTING SYSTEM

Everyone used to conduct banking operations like depositing and withdrawing money in the modern world. Customers will be waiting in line to take out cash from the bank for this. Every consumer wanted to wait to withdraw money. As a result, that bank offers an automated teller machine (ATM) to facilitate speedy cash withdrawals. Customers can use CARDS (Credit, Debit, Master, Visa) to withdraw cash from such ATM system. The main benefit is the instant cash that the ATM system provides. The consumer is satisfied and won't spend time withdrawing money. However, there are drawbacks, such as the possibility of physical keys and smart cards being stolen, misplaced, copied, or abandoned; passwords being shared, forgotten, compromised, or inadvertently seen by a third party. For the customers to conduct transactions in their banks, the banks needed a better method to ensure security. They created this fingerprint-based ATM in order to solve these issues.

PROPOSEDSYSTEM

By using a fingerprint system, the suggested solution will increase safety and security. Accuracy is the benefit of finger-scan technology. The fingerprint approach quickly reduces a number of drawbacks. Numerous clients are pleased with our system due to its speedy and improved service. These include the fact that you don't need to carry your ATM card in your wallet and that there is no possibility of losing it. Additionally, we first save the bank manager's fingerprint, which is then compared to the one we provide during authentication. The ATM cashbox will open if the fingerprints match; if not, an alert will sound from the buzzer. A safe way to verify a user's identity is to utilize fingerprint authentication in an ATM and an OTP (One-Time Password) sent to the phone number associated with their Aadhar card**.**

OBJECTIVES

1. Compared to ATM cards, fingerprint-based ATM systems are more secure.
2. The user does not need to carry an ATM card in order to conduct transactions; he can use his fingerprint anywhere, at any time.
3. In an emergency, the user can transfer funds to many accounts by giving the account number.
4. The system is applicable to a number of banks.
5. People with low incomes can readily obtain
6. If our ATM card is lost, nobody can use or access it. It blocks on its own.
7. The pincode cannot be hacked. The four-digit pin code is easily guessed by hackers.
8. The fingerprint match with the Aadhar card and send the OTP to the registered phone number with aadhar card for verification.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

STEPS FOR THE VERIFICATION METHOD

Fingerprint authentication in an ATM machine combined with OTP (One-Time Password) sent to the Aadhaar card-linked phone number is a secure method of ensuring the authenticity of the user. Here's an outline of how such a system could work:

1. Fingerprint Authentication Process:

User Enrollment: The user must first register their fingerprint in the bank's system. This is typically done at the time of account opening or during a subsequent update process at a bank branch or through an authorized machine.

Fingerprint Capture: At the ATM, the user places their finger on the fingerprint scanner.

Matching: The ATM machine captures the fingerprint and compares it with the previously stored fingerprint data in the bank's central server. Authentication Outcome: If the fingerprint matches the record, the system proceeds to the next step. If there is no match, access is denied, and the user may be asked to try again.

2. Sending OTP to Aadhaar-linked Phone Number:

Aadhaar Linking: The user must have their mobile number linked to their Aadhaar card for this process to work. This number is stored in the bank's system as part of their KYC (Know Your Customer) records.

OTP Generation: After fingerprint authentication, the ATM will trigger the bank's system to generate a one-time password (OTP).SMS Delivery: The generated OTP is then sent via SMS to the mobile phone number linked with the user's Aadhaar account.

3. OTP Verification:

OTP Input: The user will receive the OTP on their phone and enter it on the ATM screen. Verification: The ATM machine verifies the OTP with the central server. If the OTP is correct and matches the one sent to the user's phone, the transaction is authenticated and processed. Transaction Completion: If the verification is successful, the user can proceed with their withdrawal, transfer, or any other desired banking activity.

4. Security Considerations:

Biometric Security: Fingerprint authentication provides a high level of security by ensuring that only the registered user can access the ATM.OTP as a Second Factor: OTP serves as an additional layer of security, ensuring that even if someone were to have access to the user's fingerprint data, they cannot complete transactions without the OTP.

Aadhaar Linkage: By linking the user's mobile number to their Aadhaar card, it ensures that the OTP is sent to the correct phone number, reducing the risk of fraud.

5. Benefits:

Integrating OTP (One-Time Password) sent to an Aadhaar-linked mobile number and using fingerprints for ATM security can offer several benefits:

1. **Enhanced Security:** Multi-Factor Authentication (MFA): This approach requires two forms of authentication: something the user knows (OTP) and something the user has (fingerprint). This makes unauthorized access more difficult. Unique Fingerprint Identification: Fingerprints are unique to every individual, making it almost impossible for someone to fraudulently access an account using another person's fingerprint.
2. **Reduced Fraud and Identity Theft:** Aadhaar Linking: Since the Aadhaar card is linked to the user's biometric data and phone number, it provides a higher level of authentication, making it harder for fraudsters to use stolen cards or identities.OTP Verification: Sending an OTP to the registered mobile number ensures that only the account holder can complete the transaction, preventing unauthorized users from accessing the account, even if they have the physical ATM card.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3. **Improved User Convenience:** No Need to Remember PIN: Users no longer need to remember a PIN for accessing their ATM. The fingerprint and OTP combination provides a quicker and more convenient way to authenticate the transaction. Faster Transactions: With OTP and fingerprint authentication, transactions can be processed more quickly compared to traditional PIN-based systems.
4. **Real-Time Fraud Detection:** Immediate Notifications: OTPs sent to mobile numbers can alert users of attempted fraudulent activities in real-time. This instant notification can help them take quick action to protect their accounts. Aadhaar Database Verification: Using Aadhaar data can help verify the user's identity through central databases, making it easier for banks to detect unusual activities and intervene faster.
5. **Improved Access Control:** Mobile Number Authentication: Linking the ATM to an Aadhaar card ensures that only the phone number registered with the Aadhaar database is authorized for OTPs, further increasing security by reducing chances of SMS interception. Biometric Control: Biometrics provide a more precise and personalized access control mechanism, ensuring that only the cardholder can access the account.
6. **Compliance with Regulations:** Alignment with Government Initiatives: The use of Aadhaar for authentication aligns with government mandates and regulations for secure, reliable, and easily accessible public services. Better Data Protection: The biometric data used in this system would be encrypted and stored securely, aligning with privacy and data protection laws.
7. **Lower Risk of Skimming and Shoulder Surfing:** No Need for Physical PIN Input: Since the system relies on OTP and fingerprints, users don't need to enter a PIN on the ATM keypad, making it much harder for fraudsters to intercept PINs via skimming devices or shoulder surfing.
8. **User Trust and Confidence:** Increased User Confidence: As more people become familiar with biometric systems, they may feel more secure using ATMs because of the added layers of protection, increasing trust in the banking system.

6.Challenges:

Fingerprint Accuracy: Some users may have fingerprint data that is difficult to capture, especially in cases of worn fingerprints or certain skin conditions.

Aadhaar Privacy Concerns: There may be concerns regarding privacy and data security associated with linking Aadhaar and using it for financial transactions.

Figure 1

Explanation of the Diagram:

Fingerprint Capture: The user places their finger on the fingerprint scanner in the ATM machine.

Fingerprint Match: The ATM sends the captured fingerprint to the bank's central server to match it against the stored fingerprint data.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

OTP Generation: Upon successful fingerprint authentication, the bank's system triggers an OTP generation process and links the OTP to the phone number associated with the user's Aadhaar card.

OTP Sent to User's Phone: The OTP is sent to the phone number registered with the user's Aadhaar through an SMS service.

User Inputs OTP: The user receives the OTP on their phone and enters it into the ATM machine.

Transaction Confirmation: The ATM verifies the OTP. If correct, the transaction proceeds, and the user is able to complete the withdrawal or other banking activity.

RESULTS AND DISCUSSIONS

In this research, we are mainly concentrated about the end- user and a poor literacy people. In this way we were created simpleloginpage. Using thisl oginpage, we have two option, they are going to use the option card and fingerprint (Fig.6).

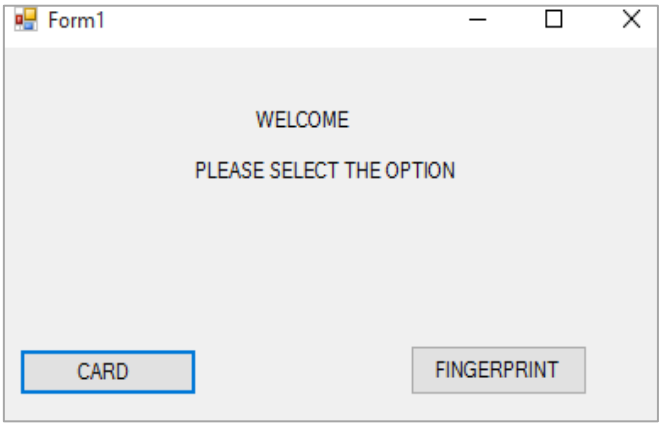

Figure 2. Fingerprint system welcome module

The end-user and those with low literacy levels are the primary focus of this study. We designed the simple login page in this manner. We have two options using this login page; they will utilize their fingerprint and choice card.

The consumer should choose the specific choice if they wish to utilize the card option. If not, he or she want to choose another fingerprint option.

The next module is the standard account and transaction selection module for the banking system. His or her action will depend on their choice in this phase.We have three choices. Checking their balance comes first, then taking money out of their account, and then moving money from one account to another.

Figure 3. Finger placing module

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

To confirm identity, the user must insert his or her finger in the scanner after choosing a fingerprint (Fig.7). The user's fingerprint will be recognized at this phase with the aid of a fingerprint scanner.

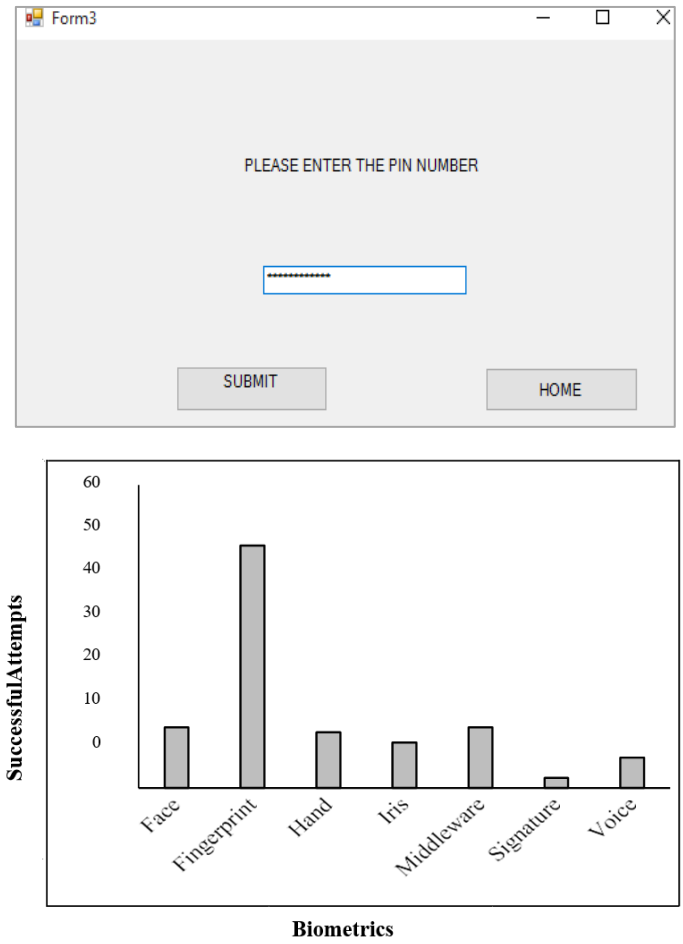

Figure 4. Survey of fingerprint with other Biometrics

CONCLUSIONS

The use of fingerprints to accomplish ATM security also includes the original methods of verification, which involved entering the customer's fingerprints and having them correctly validated by the controller. For the stability and dependability of owner recognition, the security features were significantly improved. The fingerprint technology that underpins the entire system makes it dependable, user-friendly, and safer. When it comes to electronic money transactions, this technology is the most promising. Because it combines biometric identity with a safe, one-time password technique, fingerprint authentication with an OTP texted to a mobile phone connected to Aadhaar is a potential method for protecting ATM transactions. However, strong infrastructure, user knowledge, and privacy protections will be necessary for a successful adoption.

REFERENCES

[1] A.K.Ojha,"ATM Security using Fingerprint Recognition", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 5, No. 6, pp. 170- 175, 2015.

[2] R.Banu Priya, P.Kavitha, T.Ashok, N.Logesh Kumar and M.Chandrasekar, "Smart ATM Access and Security System using RFID and GSM Technology", *International Journal of Scientific Research and Education*, Vol.2, No.5, pp.446 - 453, 2013.

[3] G.Eason, B.Noble and I.N.Sneddon,"On Certain Integrals of Lipschitz-Hankel Type Involving Products of Bessel Functions", *Philosophical Transactions of the Royal Society A*, Vol. A247, pp. 529-551, 1955.

[4] G. Sambasiva Rao, C. Naga Raju, L.S.S. Reddy and E.V. Prasad, "A Novel Fingerprints Identification System Based on the Edge Detection", *International Journal of Computer Science and Network Security*, Vol. 8, No.12, pp.394-397, 2008.
[5] M.R. Girgis, A.A. Sewisy and R. F. Mansour, "Employing Generic Algorithms for Precise Fingerprint Matching based on Line Extraction", *Graphics, Vision and Image Procession Journal*, Vol. 7, No. 1, pp. 51-59, 2007.
[6] Duresuoquian Miao, Qingshi Tang and Wenjie Fu, "Fingerprint Minutiae Extraction Based on Principal Curves", *Pattern Recognition Letters*, Vol. 28, pp. 2184- 2189, 2007.
[7] Pranali Ravikant Hatwar and Ravikant B Hatwar, "Bio- Signal based Biometrics Practices", *International Journalof Creative Research Thoughts*, Vol. 1, No. 4, pp. 1-9, 2013.
[8] Edmund Spinella, "Biometric Scanning Technologies: Finger, Facial and Retinal Scanning", Available at: https://www.sans.org/reading-room/whitepapers/authentication/biometric-scanning-technologies-finger-facial-retinal-scanning-1177.
[9] J.Swann,"Teaching Ethics:It's the Right Thing to Do", Available at: https://www.informs.org/ORMS-Today/Archived-Issues/2004/orms-6-04/Teaching-Ethics-It-s-the-Right-Thing-to-Do.
[10] O.W. Fatai, J.B. Awotunde and O.E. Matluko, "A Novel System of Fingerprint Recognition Approach for Immigration Control", *IOSR Journal of Computer Engineering*, Vol. 16, No. 3, pp. 39-42, 2014.
[11] N. Selvaraj and G. Sekar, "A Method to Improve the SecurityLevel of ATM Banking Systems using AES Algorithm", *International Journal of Computer Applications*, Vol. 3, No. 6, pp. 5-9, 2010.
[12] T.C.Glaessner,T.KellermannandV.McNevin,"Electronic Security: Risk Mitigation in Financial Transactions: Public Policy Issues",Working Paper,World Bank Publications, pp.3-5,2002.
[13] W.W.N. Wan, C.L. Luk and C.C. Chow, "Customers Adoption of Banking Channels", *International Journal of Bank Marketing*, Vol. 23, No. 3, pp. 255-272, 2005.
[14] B. Richard and M. Alemayehu, "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons", *Journal of Internet Banking and Commerce*, Vol.11, No.2, pp.1-6,2006.
[15] N.K. Ratha, J.H. Connell and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems", *IBM Systems Journal*, Vol. 40, No. 3, pp. 614- 634, 2001.
[16] J.Yang, N.Xiong, A.V.Vasilakos, Z.Fang, D.Park, X.Xu, S. Yoon, S. Xie and Y. Yang, "A Fingerprint Recognition Scheme Based on Assembling Invariant Moments for Cloud Computing Communications", *IEEE Systems Journal*, Vol. 5, No. 4, pp. 574-583, 2011.
[17] J.Leon,G.Sanchez,G.Aguilar,L.Toscano,H.PerezandJ.M.Ramirez,"FingerprintVerificationApplyingInvariant Moments", *Proceedings of IEEE International Midwest Symposium on Circuits and Systems*, pp. 751-757, 2009.
[18] L. O'Gorman, "Overview of Fingerprint Verification Technologies", *Information Security Technical Report*, Vol. 3, No. 1, pp. 21-32, 1998.
[19] G.B. Iwasokun, O.C. Akinyokun, B.K. Alese and O. Olabode, "Fingerprint Image Enhancement: Segmentation toThinning", *International Journal of Advanced Computer Science and Applications*, Vol. 3, No. 1, pp. 15-24., 2012.