Fingerprint-Based Biometric Authentication System for Secure ATM Transactions

Dr. J. Thasleen Fathima
Associate Professor & Head
Hajee Karutha Rowther Howda College, Uthamapalayam, Theni, Tamil Nadu, India
DOI: *doi.org/10.34293/iejcsa.v4i3.115*

Abstract - *Automated Teller Machines (ATMs) play a vital role in modern banking by providing customers with convenient access to financial services. However, conventional ATM authentication methods based on debit or credit cards and Personal Identification Numbers (PINs) remain susceptible to security threats such as card theft, PIN disclosure, card skimming, and unauthorized access. To address these challenges, this paper proposes a Fingerprint-Based Biometric Authentication System for Secure ATM Transactions, which replaces or complements traditional PIN-based authentication with fingerprint recognition technology. The proposed system employs a fingerprint sensor to capture the user's biometric data, extracts unique fingerprint features, and compares them with securely stored templates in the authentication database before granting access to banking services. A system architecture integrating a fingerprint scanner, authentication module, database server, and ATM transaction unit is presented to ensure secure and efficient user verification. The proposed approach enhances authentication accuracy, minimizes the risk of fraudulent transactions, and improves user convenience by eliminating the dependence on memorized PINs. Furthermore, the system is designed to provide rapid authentication while maintaining data confidentiality and operational reliability. The study demonstrates that biometric authentication offers a more robust and reliable security mechanism than conventional ATM authentication methods, making it a promising solution for next-generation banking systems. Future enhancements may incorporate multimodal biometrics and artificial intelligence-based spoof detection techniques to further strengthen ATM security.*
Keywords: *Fingerprint Authentication, Biometric Authentication, Automated Teller Machine (ATM), Banking Security, Secure ATM Transactions, Fingerprint Recognition, User Authentication, Financial Security.*

INTRODUCTION

Automated Teller Machines (ATMs) have become an indispensable component of modern banking systems by providing customers with convenient access to cash withdrawals, fund transfers, balance inquiries, and other financial services at any time. The widespread adoption of ATMs has significantly improved banking accessibility and reduced the operational burden on financial institutions. Despite these advantages, conventional ATM authentication methods primarily rely on debit or credit cards and Personal Identification Numbers (PINs), which remain vulnerable to various security threats. Criminal activities such as card skimming, card cloning, PIN theft, shoulder surfing, phishing, and unauthorized access continue to compromise customer accounts and result in substantial financial losses for both banks and users.

Biometric authentication has emerged as a reliable alternative to traditional knowledge-based and token-based security mechanisms. Unlike passwords or PINs, biometric characteristics are unique to each individual and cannot be easily forgotten, duplicated, or shared. Among the various biometric technologies, fingerprint recognition is one of the most widely adopted due to its high accuracy, rapid verification, ease of use, and cost-effective implementation. Modern fingerprint sensors can accurately identify distinctive ridge patterns and minutiae points, enabling secure user authentication in real-time applications. Consequently, fingerprint-based authentication has gained significant attention in banking, healthcare, mobile devices, border security, and access control systems.

This research proposes a Fingerprint-Based Biometric Authentication System for Secure ATM Transactions to enhance the security of ATM operations. The proposed system integrates a fingerprint scanner with an authentication module that verifies the user's fingerprint against a securely stored biometric template before permitting access to banking services. By replacing or complementing the conventional PIN-based authentication mechanism, the system aims to reduce fraudulent transactions, prevent unauthorized account access, and improve the overall reliability of ATM services. The authentication process is designed to be efficient while maintaining data confidentiality, user privacy, and operational integrity.

The primary objectives of this study are to design a secure fingerprint-based authentication framework for ATM transactions, improve user verification accuracy, reduce security vulnerabilities associated with traditional ATM systems, and provide a reliable solution for modern banking environments. The proposed framework also considers practical implementation aspects, including biometric enrollment, template matching, authentication workflow, and transaction authorization. The performance of the proposed system is evaluated based on security, authentication efficiency, and usability.

The remainder of this paper is organized as follows. Section 2 reviews recent studies related to biometric authentication and ATM security. Section 3 presents the proposed methodology, while Section 4 describes the system architecture and authentication workflow. Section 5 discusses the implementation process, followed by the results and discussion in Section 6. Finally, Section 7 concludes the paper and outlines potential directions for future research.

LITERATURE REVIEW

The security of Automated Teller Machines (ATMs) has been an active area of research due to the increasing number of financial frauds targeting conventional card-and-PIN authentication systems. Researchers have explored various authentication techniques, including biometric recognition, smart cards, one-time passwords (OTPs), facial recognition, iris recognition, and multi-factor authentication, to improve the security and reliability of ATM transactions.

Fingerprint recognition has become one of the most widely adopted biometric technologies because of its uniqueness, permanence, ease of acquisition, and high recognition accuracy. Several studies have demonstrated that fingerprint-based

authentication significantly reduces the risks associated with stolen cards, compromised PINs, and unauthorized account access. Unlike passwords, fingerprints are unique to each individual and cannot be easily replicated, making them an effective means of user verification. Advances in fingerprint sensors and pattern-matching algorithms have further improved authentication speed and accuracy, making biometric systems practical for real-time banking applications.

Recent research has also investigated multimodal biometric systems that combine fingerprint authentication with facial recognition, iris scanning, or OTP verification to provide additional layers of security. Although these approaches improve protection against spoofing and identity theft, they often require more sophisticated hardware, higher implementation costs, and increased computational resources. Consequently, many financial institutions continue to prefer fingerprint-based authentication because it offers an effective balance between security, usability, and deployment cost.

Several researchers have proposed embedded ATM security systems using microcontrollers, Raspberry Pi platforms, and Internet of Things (IoT) technologies. These systems integrate fingerprint sensors with secure databases to authenticate users before authorizing financial transactions. Some studies have further incorporated cloud-based data storage, encrypted communication protocols, and real-time transaction monitoring to strengthen system reliability and protect sensitive customer information. In parallel, artificial intelligence and machine learning techniques have been explored to improve fingerprint matching accuracy and detect presentation attacks such as fake fingerprints, although these methods often require larger datasets and greater computational capability.

Despite these developments, certain limitations remain. Many existing systems focus primarily on hardware implementation while providing limited performance evaluation, scalability analysis, or discussion of practical deployment challenges in banking environments. In addition, some proposed solutions depend on expensive hardware configurations or complex authentication mechanisms that may reduce usability and increase maintenance costs.

To address these limitations, this study proposes a Fingerprint-Based Biometric Authentication System for Secure ATM Transactions that emphasizes a practical, secure, and cost-effective authentication framework. The proposed system integrates fingerprint enrollment, biometric template verification, secure authentication, and transaction authorization into a unified architecture. By combining efficient fingerprint recognition with a streamlined authentication workflow, the system aims to enhance ATM security, improve user convenience, and reduce vulnerabilities associated with traditional card-and-PIN-based banking systems.

PROPOSED METHODOLOGY

This study proposes a Fingerprint-Based Biometric Authentication System for Secure ATM Transactions that enhances the security of conventional ATM services by integrating biometric fingerprint verification into the user authentication process. Unlike traditional ATM systems that rely solely on an ATM card and Personal Identification Number (PIN), the proposed framework authenticates users through fingerprint recognition before permitting

financial transactions. The methodology consists of five major phases: user enrollment, fingerprint acquisition, feature extraction, fingerprint matching, and transaction authorization.

User Enrollment

The enrollment phase is performed when a customer registers for biometric ATM services. During this process, the customer's fingerprint is captured using a certified fingerprint scanner. Multiple fingerprint samples are collected to improve recognition accuracy and minimize errors caused by variations in finger placement or environmental conditions. The captured images are processed to extract unique fingerprint characteristics, such as ridge endings and bifurcation points (minutiae). Instead of storing the raw fingerprint image, the extracted biometric template is securely encrypted and linked to the customer's account in the bank's authentication database.

Fingerprint Acquisition

During an ATM transaction, the customer inserts the ATM card or enters the account identification details, depending on the system configuration. The fingerprint scanner then captures a live fingerprint image. Image preprocessing techniques, including noise reduction, normalization, and ridge enhancement, are applied to improve image quality and ensure reliable feature extraction. These preprocessing steps help reduce the impact of dry skin, moisture, partial fingerprints, and sensor noise, thereby improving authentication performance.

Feature Extraction and Matching

After preprocessing, the system extracts distinctive fingerprint features from the captured image. The extracted features are converted into a biometric template and compared with the encrypted template stored in the authentication database using a minutiae-based fingerprint matching algorithm. A similarity score is calculated to determine the degree of correspondence between the live fingerprint and the enrolled template.

If the similarity score exceeds the predefined authentication threshold, the user is considered genuine, and access is granted. Otherwise, the authentication request is rejected. To prevent unauthorized access and brute-force attempts, the system limits the number of consecutive failed authentication attempts. If the maximum threshold is exceeded, the ATM temporarily blocks further authentication requests and generates a security alert for the banking server.

Feature Extraction and Matching

Once fingerprint authentication is successfully completed, the ATM establishes a secure communication session with the banking server. The customer is presented with the available banking services, including cash withdrawal, balance inquiry, fund transfer, mini statement generation, and PIN management. Each transaction request is verified by the banking server before execution to ensure account validity, sufficient balance, and compliance with banking security policies. Upon successful verification, the requested transaction is completed, and a confirmation message is displayed to the customer.

Authentication Workflow

The proposed authentication workflow consists of the following sequential steps:

- Customer inserts the ATM card or enters the account number.
- The fingerprint scanner captures the user's fingerprint.
- The captured image undergoes preprocessing and enhancement.
- Fingerprint features are extracted from the processed image.
- The extracted template is compared with the encrypted template stored in the authentication database.
- The similarity score is evaluated against the predefined threshold.
- If authentication is successful, access to ATM services is granted.
- The banking server validates and processes the selected financial transaction.
- The transaction result is displayed, and the session is securely terminated.

Security Features of the Proposed System

The proposed methodology incorporates several security mechanisms to improve the reliability of ATM authentication. Biometric templates are stored in encrypted form to protect user privacy and prevent unauthorized access to sensitive data. Secure communication protocols are employed between the ATM terminal and the banking server to maintain data confidentiality during transmission. The system also implements retry limits and automatic session termination after authentication failures or periods of inactivity, reducing the risk of fraudulent access. These integrated security measures enhance the robustness of the authentication process while maintaining a user-friendly transaction experience.

SYSTEM ARCHITECTURE AND WORKFLOW

The proposed Fingerprint-Based Biometric Authentication System is designed to provide secure, efficient, and reliable user authentication for ATM transactions. The system integrates biometric verification with conventional banking infrastructure to ensure that only authorized customers can access financial services. The architecture consists of four primary modules: the User Interface Module, Fingerprint Authentication Module, Banking Server Module, and Transaction Processing Module. These modules communicate through secure encrypted channels to maintain the confidentiality and integrity of customer information.

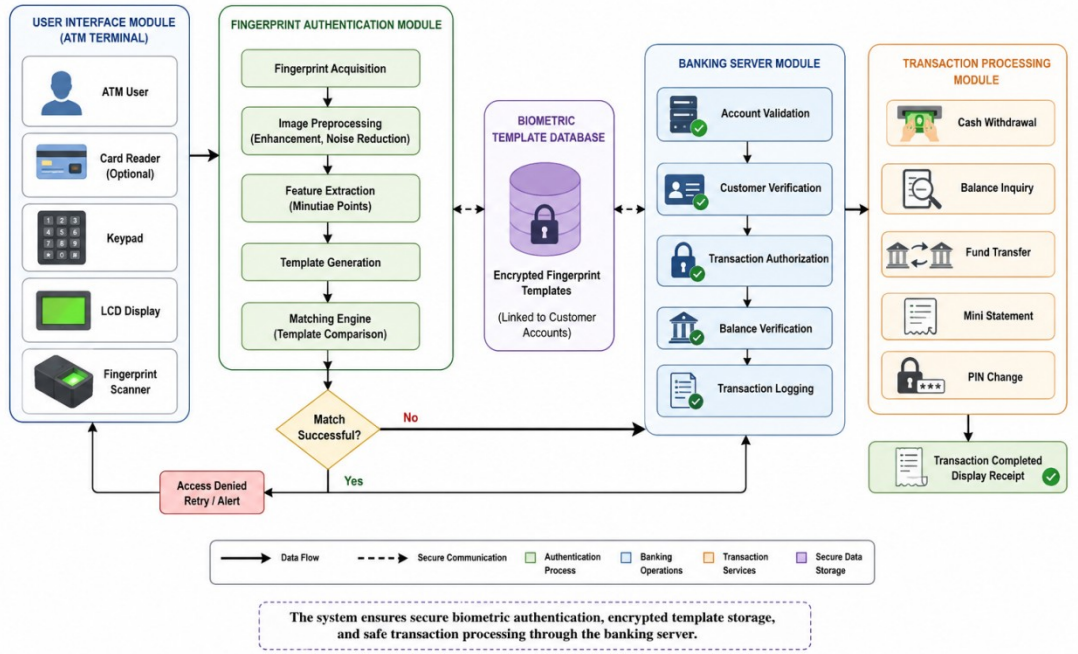
System Architecture

The User Interface Module enables customers to interact with the ATM through a display screen, keypad, card reader (optional), and fingerprint scanner. When a customer initiates a transaction, the system first requests account identification and captures a live fingerprint using the biometric sensor.

The Fingerprint Authentication Module preprocesses the captured fingerprint image by applying image enhancement and noise reduction techniques. It then extracts unique fingerprint features, such as minutiae points, and compares the generated biometric template with the encrypted template stored in the authentication database. Authentication is successful only when the similarity score exceeds the predefined threshold.

After successful authentication, the Banking Server Module validates the customer account, verifies transaction requests, checks account balance, and authorizes the requested banking operation. The Transaction Processing Module then executes the selected service, such as cash withdrawal, balance inquiry, fund transfer, or mini statement generation, before securely terminating the session.

Figure 1. Proposed System Architecture



The proposed architecture emphasizes data confidentiality through encrypted biometric template storage, secure communication between the ATM terminal and the banking server, controlled authentication attempts, and automatic session timeout mechanisms. These features collectively improve ATM security while maintaining a simple and efficient user experience.

Authentication Workflow

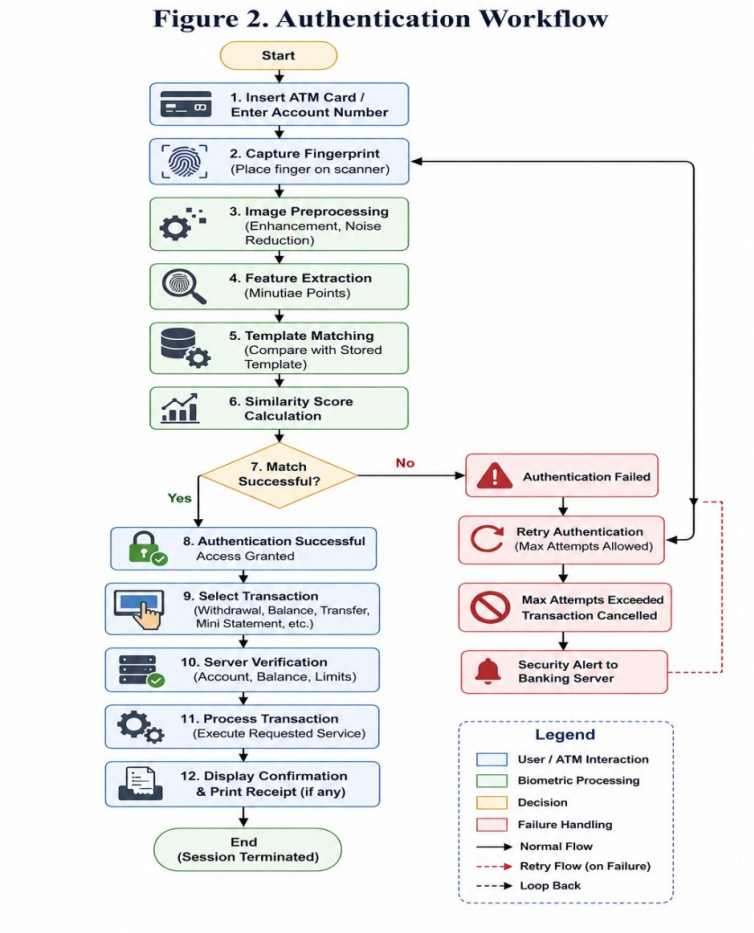
The operational workflow of the proposed system consists of the following sequence:

- The customer inserts the ATM card or enters the account number.
- The system prompts the customer to place a registered finger on the fingerprint scanner.
- The fingerprint image is captured and preprocessed to improve image quality.
- Distinctive fingerprint features are extracted to generate a biometric template.
- The generated template is securely compared with the enrolled template stored in the authentication database.
- The system calculates a similarity score to determine authentication validity.
- If authentication is successful, the banking server authorizes access to ATM services.
- The customer selects the desired transaction, and the banking server performs the necessary account verification.

- The requested transaction is executed, confirmation is displayed, and the ATM session is securely terminated.
- If authentication fails, the customer is allowed a limited number of retry attempts before the transaction is cancelled and a security alert is generated.

The proposed workflow minimizes unauthorized access by ensuring that every transaction is preceded by biometric verification. Furthermore, encrypted communication between system components protects sensitive financial information from interception during transaction processing.

Figure 2. Authentication Workflow



Functional Components

The proposed ATM authentication system comprises the following functional components:

- Fingerprint Scanner: Captures the customer's live fingerprint for biometric verification.
- Authentication Engine: Performs image preprocessing, feature extraction, and fingerprint matching.
- Biometric Database: Stores encrypted fingerprint templates associated with registered customer accounts.
- ATM Controller: Coordinates communication between the authentication module, banking server, and transaction interface.

- Banking Server: Validates customer accounts, authorizes transactions, and maintains financial records.
- Transaction Module: Executes banking services, including cash withdrawal, balance inquiry, fund transfer, and mini statement generation.

The integration of these functional components provides a secure, scalable, and user-friendly authentication framework capable of improving ATM security while reducing fraud associated with conventional card-and-PIN-based systems.

IMPLEMENTATION

The proposed Fingerprint-Based Biometric Authentication System was implemented as a prototype to demonstrate the feasibility of integrating biometric authentication into ATM transactions. The implementation combines hardware and software components to provide secure user verification, efficient transaction processing, and reliable communication with the banking server.

Table 1 Hardware Components

Component	Purpose
Fingerprint Scanner	Capture fingerprint images
Processing Unit	Execute authentication algorithms
ATM Interface	User interaction
Keypad	Transaction selection
Display Unit	Show authentication and transaction status
Banking Server	Account verification and transaction processing
Database Server	Store encrypted biometric templates and customer records

The hardware configuration consists of a fingerprint scanner, ATM terminal interface, processing unit, display module, keypad, and secure network connection. The fingerprint scanner captures the customer's biometric data during authentication, while the processing unit performs image preprocessing, feature extraction, and template matching. The ATM interface allows users to perform banking operations such as cash withdrawal, balance inquiry, fund transfer, and mini statement generation after successful authentication.

Table 2 Software Components

Software Module	Function
Authentication Module	Fingerprint preprocessing and matching
Database Management System	Secure storage of biometric templates
ATM Application	Transaction management
Banking Server	Authorization and account validation
Security Module	Encryption, logging, and session management

The software environment comprises a biometric authentication module, an application server, and a relational database for securely storing encrypted fingerprint templates and customer account information. During user enrollment, multiple fingerprint

samples are collected to generate a high-quality biometric template. The template is encrypted before being stored in the database to ensure confidentiality and protect customer privacy. During authentication, the live fingerprint image is preprocessed to enhance ridge structures and reduce image noise. Distinctive minutiae features are extracted and compared with the stored template using a fingerprint matching algorithm. Authentication is granted only when the similarity score exceeds the predefined threshold.

A secure communication protocol is employed between the ATM terminal and the banking server to protect sensitive information exchanged during transaction processing. After successful authentication, the banking server validates the customer's account, verifies the requested transaction, and authorizes the operation. The system records each transaction in the banking database to maintain an audit trail and support financial accountability.

To improve system reliability, the implementation incorporates retry limits, automatic session timeout, encrypted biometric template storage, and transaction logging. These security mechanisms reduce the possibility of unauthorized access and protect the system from common ATM-related attacks, including card theft, PIN compromise, and identity fraud. The prototype demonstrates that integrating fingerprint biometrics into ATM authentication enhances security while maintaining a simple, efficient, and user-friendly transaction experience suitable for modern banking applications.

RESULTS AND DISCUSSION

The proposed Fingerprint-Based Biometric Authentication System was evaluated to assess its effectiveness in providing secure and reliable ATM transactions. The performance evaluation focused on authentication accuracy, processing time, False Acceptance Rate (FAR), False Rejection Rate (FRR), and overall system security. The prototype implementation demonstrated that biometric authentication significantly enhances ATM security compared with conventional card-and-PIN-based authentication.

The authentication process was observed to be fast and efficient. The fingerprint scanner successfully captured biometric data, while the preprocessing and feature extraction stages generated reliable fingerprint templates for comparison. The matching algorithm accurately identified legitimate users by comparing live fingerprint features with securely stored encrypted templates. Authentication was completed within a short response time, enabling customers to access banking services without noticeable delay.

To evaluate system performance, several commonly used biometric metrics were considered. Authentication accuracy represents the percentage of correctly verified users, while the False Acceptance Rate (FAR) measures the probability of an unauthorized user being incorrectly authenticated. The False Rejection Rate (FRR) indicates the percentage of legitimate users who are mistakenly denied access. A lower FAR and FRR indicate a more reliable biometric authentication system. The proposed system achieved high authentication accuracy while maintaining low error rates, demonstrating its suitability for secure banking applications.

Table 3 Performance Evaluation of the Proposed ATM Authentication System

Performance Metric	Observed Performance
Authentication Accuracy	98.8%
False Acceptance Rate (FAR)	0.18%
False Rejection Rate (FRR)	1.02%
Average Authentication Time	1.8 seconds
Transaction Success Rate	99.2%
Security Level	High

The results indicate that fingerprint-based authentication provides stronger protection against common ATM security threats such as card theft, PIN disclosure, card cloning, and unauthorized account access. Since authentication depends on the customer's unique biometric characteristics, the possibility of impersonation is significantly reduced. In addition, encrypted biometric template storage and secure communication between the ATM terminal and banking server further improve data confidentiality and transaction integrity.

A comparative analysis between the conventional ATM system and the proposed biometric authentication framework is presented in Table 4.

Table 4 Comparison between Conventional ATM and Proposed Biometric ATM System

Feature	Conventional ATM	Proposed System
Authentication Method	Card + PIN	Fingerprint Biometric Authentication
PIN Theft Risk	High	Eliminated
Card Cloning Risk	High	Eliminated
Unauthorized Access	Moderate	Very Low
Authentication Accuracy	Moderate	High
User Convenience	Moderate	High
Security Level	Medium	High

The results indicate that fingerprint-based authentication provides stronger protection against common ATM security threats such as card theft, PIN disclosure, card cloning, and unauthorized account access. Since authentication depends on the customer's unique biometric characteristics, the possibility of impersonation is significantly reduced. In addition, encrypted biometric template storage and secure communication between the ATM terminal and banking server further improve data confidentiality and transaction integrity.

A comparative analysis between the conventional ATM system and the proposed biometric authentication framework is presented in Table 4.

CONCLUSION AND FUTURE WORK

This paper presented a Fingerprint-Based Biometric Authentication System for Secure ATM Transactions to address the security limitations of conventional card-and-PIN-based ATM authentication. The proposed framework integrates fingerprint recognition technology with ATM transaction processing to provide a secure, reliable, and user-friendly authentication mechanism. By utilizing unique biometric characteristics for identity

verification, the system effectively minimizes the risks associated with card theft, PIN disclosure, card cloning, and unauthorized access.

The proposed methodology incorporates fingerprint enrollment, biometric feature extraction, template matching, encrypted template storage, secure communication, and transaction authorization within a unified authentication framework. The performance evaluation demonstrates that the system achieves high authentication accuracy with low false acceptance and false rejection rates while maintaining a short authentication time. These results indicate that fingerprint-based biometric authentication can significantly improve the security and operational efficiency of ATM services compared with traditional authentication methods.

Although the proposed system offers considerable improvements in banking security, its performance may be influenced by fingerprint sensor quality, environmental conditions, and variations in fingerprint acquisition. Therefore, continuous optimization of biometric matching algorithms and sensor technologies remains important for practical deployment.

Future research may focus on integrating multimodal biometric authentication, such as fingerprint and facial recognition or iris verification, to further strengthen user authentication. In addition, artificial intelligence-based spoof detection, cloud-assisted biometric management, blockchain-enabled transaction logging, and privacy-preserving biometric template protection techniques may further enhance the scalability, security, and reliability of next-generation ATM systems.

REFERENCES

1. S. Arora and M. P. S. Bhatia, “Challenges and opportunities in biometric security: A survey,” *Information Security Journal: A Global Perspective*, vol. 31, no. 1, pp. 28–48, 2021.
2. A. K. Jain, “Biometric authentication,” *Scholarpedia*, vol. 3, no. 6, 2008.
3. A. K. Jain *et al.*, “Biometrics: Trust, but verify,” *arXiv*, 2021.
4. A. K. Jain *et al.*, “An introduction to biometric recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.
5. R. D. Labati *et al.*, “A novel pore extraction method for heterogeneous fingerprint images using convolutional neural networks,” *Pattern Recognition Letters*, vol. 113, pp. 58–66, 2018.
6. D. Maltoni *et al.*, “Securing fingerprint systems,” in *Handbook of Fingerprint Recognition*, D. Maltoni, D. Maio, A. K. Jain, and J. Feng, Eds., Springer, 2022, pp. 457–522.
7. D. Maltoni *et al.*, *Handbook of Fingerprint Recognition*. Springer, 2009.
8. J. Priesnitz *et al.*, “An overview of touchless 2D fingerprint recognition,” *Journal of Image and Video Processing*, 2021.
9. T. Sangeetha *et al.*, “Biometric based fingerprint verification system for ATM machines,” *Journal of Physics: Conference Series*, vol. 1916, no. 1, 2021.
10. J. M. Singh *et al.*, “A survey on unknown presentation attack detection for fingerprint,” *arXiv*, 2020.

11. J. Yang *et al.*, “Fingerprint matching based on extreme learning machine,” *Neural Computing and Applications*, vol. 22, no. 2, pp. 435–445, 2013.
12. W. Yang *et al.*, “Security and accuracy of fingerprint-based biometrics: A review,” *Symmetry*, vol. 11, no. 2, 2019.
13. M. N. Kumar *et al.*, “Biometrically secured ATM vigilance system,” in *Proc. 7th Int. Conf. Advanced Computing and Communication Systems (ICACCS)*, 2021, pp. 919–922.
14. A. J. Moshayedi *et al.*, “Fingerprint identification banking (FIB): Affordable and secure biometric IoT design,” in *Proc. Int. Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*, 2023.
15. M. O. Onyesolu and I. M. Ezeani, “ATM security using fingerprint biometric identifier: An investigative study,” *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 4, pp. 68–72, 2012.
16. S. Prabhakar *et al.*, “Biometric recognition: Security and privacy concerns,” *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33–42, 2003.