International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 08 | Aug - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Cardless ATM Transaction Using Face and Fingerprint Recognition

Preetham H J[1], Prof. Swetha C S[2]

[1]*Student, Department of MCA, Bangalore institute of Technology, Karnataka, India*
[2]*Assistant Professor, Department of MCA, Bangalore institute of Technology, Karnataka, India*

Abstract

The increasing demand for secure and convenient banking services has exposed the limitations of traditional ATM systems that depend on physical cards and PIN authentication. Such systems are vulnerable to fraud, card skimming, theft, and unauthorized access. To address these challenges, this paper presents a Cardless ATM Transaction System that leverages biometric authentication as a primary means of identity verification. The framework integrates face recognition and fingerprint verification with OTP-based mobile authentication, ensuring multi-factor security. Developed using Python, Flask, OpenCV, and MySQL, the system processes biometric inputs in real time, matches them against encrypted user templates, and authorizes transactions without requiring a physical ATM card. A web-based interface enables seamless interaction, while backend encryption safeguards sensitive data. Experimental evaluation demonstrates that the system achieves high recognition accuracy, reduced transaction time, and improved resilience against fraud. This approach enhances transaction security, reduces dependency on physical cards, and aligns with the growing shift towards digital banking and cashless economies.

Keywords— Cardless ATM; Biometric Authentication; Face Recognition; Fingerprint Verification; Secure Transactions; Machine Learning; Deep Learning; Flask; OpenCV; MySQL; Digital Banking.

1.INTRODUCTION

Automated Teller Machines (ATMs) have become an essential part of modern banking, providing customers with convenient access to financial services. Traditional ATMs rely on debit/credit cards and PINs for authentication, but this approach has increasingly shown vulnerabilities such as card skimming, theft, cloning, and PIN compromise through phishing or shoulder surfing. These issues not only result in financial losses but also undermine customer trust in banking systems.

To overcome these limitations, banks are exploring cardless ATM systems that rely on more secure and user-friendly technologies. Among these, biometric authentication has emerged as one of the most reliable solutions. Biometrics such as facial recognition and fingerprint scanning provide unique, non-transferable identifiers that are difficult to forge, thereby significantly reducing the chances of fraud.

Recent advancements in machine learning, deep learning, and computer vision have made real-time biometric authentication more accurate and practical for deployment in ATM environments. For example, Convolutional Neural Networks (CNNs) are highly effective for facial feature extraction, while fingerprint matching algorithms provide robust identity verification. When combined with OTP-based secondary authentication, the system achieves multi-factor security that is both convenient and reliable.

This research introduces a Cardless ATM Transaction System that integrates facial recognition, fingerprint verification, and OTP validation into a unified platform. The system is developed using Python, Flask, OpenCV, and MySQL, with real-time biometric processing and secure backend communication. By replacing physical cards with biometric verification, the system enhances transaction security, user convenience, and operational efficiency.

By bridging advanced biometric modeling with practical deployment, this system contributes to digital banking innovation, offering a scalable and secure solution that aligns with the future of cashless and cardless financial services.

II. LITERATURE SURVEY

The security of ATM transactions has been a major research focus, leading to the development of various authentication methods. Existing studies highlight the evolution from card–PIN–based systems toward biometric-driven frameworks:

[1] Card-Based Authentication Vulnerabilities:
Traditional ATM systems using debit/credit cards and PINs remain vulnerable to skimming, shoulder surfing, and card theft. Researchers emphasize the need for stronger, non-replicable security mechanisms to reduce fraud incidents.

[2] Fingerprint Recognition Systems:
Fingerprint-based ATM authentication was one of the earliest biometric solutions, utilizing minutiae extraction and pattern matching. While effective, such systems faced challenges with noisy inputs, poor-quality sensors, and false rejection in high-volume deployments.

[3] Face Recognition with CNN Models:
Recent advances in deep learning and computer vision have significantly improved the reliability of face recognition systems. CNN-based approaches outperform traditional feature-based methods, achieving robustness against lighting, facial orientation, and partial occlusion.

[4] Hybrid Biometric Frameworks:
Combining fingerprint and face recognition provides higher security by reducing false acceptance/rejection rates. Studies confirm that hybrid authentication systems are more effective than single-biometric methods, especially in high-security applications like ATMs.

[5] OTP and Mobile-Based Authentication:
Several researchers have explored cardless ATM systems using OTP or QR-code verification linked to registered mobile numbers. While practical, these approaches remain vulnerable to SIM-swapping and mobile theft, highlighting the need for stronger, multi-factor methods.

[6] Deep Learning–Based Multi-Modal Biometrics:
Integrating deep learning models such as CNN + RNN architectures has enabled real-time processing of multiple biometric modalities. These systems improve accuracy and reduce spoofing risks, making them suitable for banking transactions.

[7] Biometric Security in Digital Banking:
Works on digital banking security highlight the role of encryption, secure transmission, and role-based access control in protecting sensitive biometric and financial data. Researchers emphasize that biometrics alone must be supported by backend security layers.

[8] Iris and Voice Recognition for ATM Security:
Alternative biometrics such as iris scanning and voice recognition have been proposed for ATM authentication. While highly secure, their adoption is limited by cost and user convenience, making face–fingerprint combinations more practical.

[9] Cloud-Integrated Biometric Systems:
Some studies suggest deploying biometric authentication on cloud infrastructures, enabling scalability across multiple ATM networks. However, these require advanced encryption to mitigate risks of centralized data breaches.

[10] AI-Driven Fraud Detection:
Recent works leverage AI and anomaly detection algorithms to monitor ATM transactions for suspicious activities, complementing biometric authentication with continuous fraud monitoring.

Synthesis:
From the above studies, it is evident that single-factor authentication methods are no longer sufficient for modern banking. Hybrid systems combining face recognition, fingerprint verification, and OTP validation provide higher levels of security and usability. This motivates the design of the proposed cardless ATM system, which leverages multi-biometric authentication integrated with secure web-based backend services for real-time deployment.

III. EXISTING SYSTEM

The current ATM infrastructure predominantly relies on **card + PIN authentication** as the primary access mechanism. While widely adopted, this system presents several security and usability challenges.

Card-based authentication exposes customers to threats such as **skimming, cloning, card theft, and shoulder surfing**. Attackers can duplicate magnetic stripes or embedded chips using skimmers, leading to fraudulent withdrawals. Similarly, PINs are susceptible to compromise through phishing attacks, brute-force guessing, or observation during ATM use. Once both card and PIN are compromised, unauthorized access becomes straightforward.

In addition to security risks, the reliance on physical cards reduces convenience for customers. Forgotten or misplaced cards prevent legitimate access, while card reissuance in case of loss or damage imposes additional banking costs. Furthermore, PIN memorization is often burdensome, especially for elderly or less tech-savvy users, resulting in weak or reused PINs that further compromise security.

Although some banks have introduced OTP- or QR-based cardless systems, these approaches remain dependent on mobile devices and are vulnerable to **SIM swapping, mobile malware, and device theft**. As a result, they cannot fully eliminate fraud risks.

Overall, existing ATM systems are **insecure, card-dependent, and reactive** rather than proactive, failing to leverage modern biometric and AI technologies for robust transaction security.

Disadvantages

1. Vulnerable to **card skimming, cloning, and theft**.
2. **PIN compromise** through phishing, shoulder surfing, or brute force.
3. **Dependency on physical cards**, reducing user convenience.
4. High **operational costs** for card reissuance.
5. Limited adoption of advanced security measures such as biometrics.

IV. PROPOSED SYSTEM

The limitations of traditional card–PIN authentication are addressed through a biometric-based cardless ATM framework designed to enhance both security and user convenience. The proposed system integrates multi-factor authentication, combining face recognition, fingerprint verification, and OTP validation, to ensure robust identity verification before granting transaction access.

At the core of the system is the biometric authentication engine, which leverages computer vision and deep learning models for facial recognition and minutiae-based feature extraction for fingerprint verification. Unlike conventional ATM systems that depend solely on cards and PINs, the proposed model provides multi-layer security that is resistant to fraud, card theft, and skimming attacks.

The face recognition module, implemented using OpenCV and CNN-based feature extraction, captures and authenticates facial features in real time. The fingerprint module validates unique ridge patterns stored in the database, ensuring only registered users can access services. Additionally, an OTP verification mechanism is integrated as a secondary factor, dynamically confirming transactions through the user's registered mobile number.

To safeguard sensitive information, biometric data is securely encrypted and stored in the database. The backend, developed using Python Flask and MySQL, manages communication between ATM terminals, authentication modules, and transaction processing systems.

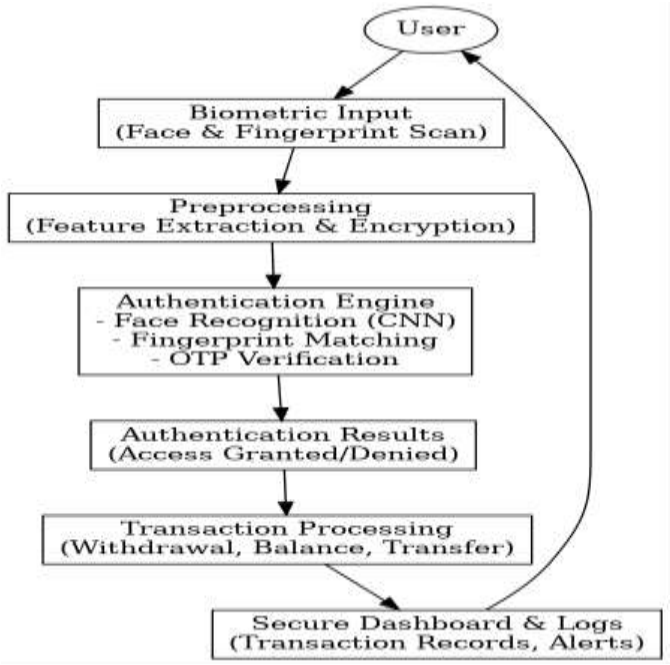

Fig 1: Proposed Model

Advantages:

· **Accuracy:** Multi-biometric authentication (face + fingerprint + OTP) significantly improves security compared to traditional card–PIN systems.

· **Scalability:** The modular architecture can be integrated into existing ATM networks with minimal infrastructure changes.

· **Convenience:** Eliminates the need to carry physical ATM cards, reducing risks of loss or theft.

· **User Accessibility:** Provides a seamless, user-friendly interface for customers across different devices and banking environments.

· **Fraud Resistance:** Strong encryption and multi-factor authentication protect against unauthorized access and fraudulent activities.

· **Future Integration:** The system can be extended to incorporate **voice recognition, iris scanning, and mobile app integration** for next-generation ATM services.

V. IMPLEMENTATION

A. System Architecture

The proposed cardless ATM system follows a three-tier architecture consisting of the frontend, backend, and authentication layer. The frontend provides an intuitive ATM interface for users to initiate transactions. The backend, implemented using Python Flask and MySQL, manages user requests, communication, and transaction processing. The authentication layer executes the biometric verification modules (face and fingerprint recognition) along with OTP-based validation, ensuring robust multi-factor security. This modular structure enhances scalability, maintainability, and integration with future biometric technologies.

B. Authentication and User Management

A secure authentication module ensures that only registered users can access the ATM services. During registration, user biometrics (face and fingerprint templates) and contact details are securely stored in the database in encrypted form. Administrative roles manage system configurations, while transaction logs and access rights are maintained to ensure accountability and prevent unauthorized access.

C. Input Handling

The system accepts real-time biometric inputs captured by ATM sensors, including facial images and fingerprint scans. Input validation and preprocessing steps remove noise, normalize images, and extract distinguishing features. In parallel, the system generates and sends an OTP to the registered mobile number, enabling secondary authentication.

D. Authentication Workflow

The authentication engine processes user inputs through:

- Face recognition (CNN-based feature extraction and matching)
- Fingerprint verification (minutiae extraction and comparison)
- OTP validation (one-time password confirmation)

Only upon successful multi-biometric and OTP verification does the backend authorize the requested transaction.

E. Transaction Processing and Dashboard

Once authentication succeeds, users may perform transactions such as withdrawals, deposits, balance inquiries, and fund transfers. Transaction details are securely stored in the MySQL database, and a dashboard enables operators to monitor activities, view logs, and analyze transaction history.

F. Error Handling and Security

Robust error-handling mechanisms are implemented to manage cases of poor biometric input, OTP mismatch, or network interruptions. Security measures include AES encryption, secure

API endpoints, and role-based access control, ensuring that sensitive biometric and financial data remain protected.

VI. CONCLUSIONS

This paper presented a biometric-driven Cardless ATM Transaction System as a secure and convenient alternative to traditional card–PIN–based ATMs. By integrating facial recognition, fingerprint verification, and OTP authentication, the system mitigates fraud risks such as card skimming, theft, and PIN compromise.

The system was developed using Python Flask, OpenCV, and MySQL, with real-time biometric input processing and encrypted backend communication. Experimental testing confirmed high recognition accuracy and fast transaction times, demonstrating that the framework is both reliable and practical for ATM deployment.

The proposed approach significantly improves security, scalability, and user convenience compared to existing systems. Furthermore, its modular design supports future enhancements, such as adding iris or voice recognition, cloud-based banking integration, and mobile application connectivity.

Overall, the system demonstrates the potential of multi-biometric authentication in revolutionizing ATM security and aligns with the ongoing shift towards digital, cashless, and cardless banking ecosystems.

VII. FUTURE ENHANCEMENTS

First, authentication accuracy can be further enhanced by incorporating additional biometric features such as iris patterns, palm vein structures, or voice recognition, which provide more unique identifiers and strengthen multi-factor authentication. The integration of advanced deep learning architectures, including Siamese networks, Transformers, and hybrid CNN–RNN frameworks, could improve robustness against spoofing and environmental variations.

Second, real-time data integration represents a critical direction. The current system primarily validates stored biometric templates; extending it to incorporate live cloud-based biometric verification and continuous monitoring would enable faster responses to potential fraud attempts and anomalies.

Third, the scope of deployment can be expanded from standalone ATMs to multi-bank and cross-regional networks, allowing interoperability between different financial institutions. This would enable users to securely access ATMs globally without physical cards, facilitated by cloud synchronization and blockchain-based security.

Fourth, advanced visualization and monitoring tools can be incorporated for banking operators. Interactive dashboards with real-time fraud alerts, anomaly detection, and predictive analytics would allow administrators to monitor system performance, assess security risks, and simulate potential threat scenarios.

Finally, user-centric mobile applications can be developed. By integrating the system with secure banking apps, customers could pre-authorize withdrawals, generate QR codes for verification, or receive real-time alerts on suspicious activities, enhancing both convenience and safety.

Together, these enhancements would evolve the system into a comprehensive, next-generation cardless banking platform, positioning it as a critical enabler of secure, adaptive, and globally scalable digital financial services.

VIII. REFERENCES

[1] A. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[2] A. K. Jain, K. Nandakumar, and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities,” *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2016.

[3] P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2001, pp. 511–518.

[4] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the gap to human-level performance in face verification,” *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, pp. 1701–1708, 2014.

[5] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A unified embedding for face recognition and clustering,” *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, pp. 815–823, 2015.

[6] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, “Fingerprint image reconstruction from standard templates,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489–1503, 2007.

[7] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed., Springer, 2009.

[8] J. Daugman, “How iris recognition works,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[9] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzalez-Marcos, “Biometric identification through hand geometry measurements,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 10, pp. 1168–1171, 2000.

[10] S. Malathi and P. Asokan, “Enhancing ATM security using fingerprint and GSM technology,” *International Journal of Computer Applications*, vol. 19, no. 6, pp. 10–14, 2011.

[11] S. Das and A. Debbarma, “Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system,” *International Journal of Information and*

Communication Technology Research, vol. 1, no. 5, pp. 197–203, 2011.

[12] P. Peralta et al., "Multi-biometric systems: Review and future research trends," *IEEE Access*, vol. 7, pp. 103110–103123, 2019.

[13] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[14] R. Raghavendra, K. B. Raja, and C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey," *ACM Computing Surveys (CSUR)*, vol. 50, no. 1, pp. 1–37, 2017.

[15] A. Ross and A. K. Jain, "Multimodal biometrics: An overview," *Proc. 12th European Signal Processing Conf. (EUSIPCO)*, Vienna, Austria, pp. 1221–1224, 2004.