International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901014

ATM Access Using Card Scanner and Face Recognition with AIML

Varshini. M[1], Chandrapathi. M[2], Manirekha. G[3], Balaraju. M[4], Afraz.MD[5]

Dr.Sarvanan. M[6], Dr. Prasad Dharnasi[7]

Student, B.Tech CSE 4th Year, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India[1-5]

Professor, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India[6]

Professor, Dept. of CSE, Holy Mary Inst. of Tech. and Science, Hyderabad, TG, India[7]

Publication History: Received: 15.01.2026; Revised: 12.02.2026; Accepted: 18.02. 2026; Published: 23.02.2026.

ABSTRACT: In recent years, the increasing number of ATM frauds has highlighted the limitations of traditional card-and-PIN–based authentication systems. To address these security challenges, this project proposes an enhanced ATM access system that combines card scanning technology with AI/ML-based face recognition to ensure secure and reliable user authentication. The system introduces a multi-layered verification mechanism aimed at preventing unauthorized access while maintaining ease of use for legitimate users.The proposed system is implemented using Python, with Tkinter used to design a graphical user interface that simulates ATM operations such as card scanning, authentication status, and transaction access. User card information and facial data references are maintained using CSV files, providing a lightweight and efficient method for structured data storage. File handling tasks, including storing and managing user images and logs, are performed using the os and shutil modules.

The authentication process begins with card verification, followed by AI/ML-based face recognition that compares the live facial image of the user with registered records. The time and datetime modules are utilized to record access timestamps and monitor suspicious activity patterns, such as repeated failed attempts. To strengthen security, random and string modules are used to generate unique session identifiers and temporary access tokens during each transaction.

To ensure smooth operation and real-time responsiveness, threading is employed to run facial recognition and verification processes concurrently without interrupting the GUI. System-level operations and exception handling are managed using the sys module to improve reliability and error control. In cases of suspicious or failed authentication attempts, the system automatically sends security alerts using smtplib and the email module to notify the account holder or bank authority. By integrating card-based verification with biometric authentication powered by AI/ML techniques, the proposed ATM system significantly enhances security, reduces fraud risk, and demonstrates a practical approach to intelligent and secure banking systems.

KEYWORDS: ATM Security, Card Scanner, Face Recognition, Artificial Intelligence, Machine Learning, Biometric Authentication, Two-Factor Authentication, Tkinter GUI, Python Programming, Fraud Detection, Secure Banking System, Real-Time Authentication, Email Alert System, Multithreading, Data Logging.

I. INTRODUCTION

The project focuses on Automated Teller Machines (ATMs) play a vital role in modern banking by enabling customers to access financial services conveniently and securely at any time. Services such as cash withdrawal, balance inquiry, fund transfer, and mini statements have become easily accessible due to the widespread deployment of ATMs.Traditional ATM authentication systems primarily depend on card-based access combined with Personal Identification Numbers (PINs). While these methods are simple and cost-effective, they are highly susceptible to various security threats. Card skimming, PIN theft, shoulder surfing, brute-force attacks, and unauthorized access are common vulnerabilities associated with conventional systems. Moreover, stolen or duplicated ATM cards can be misused easily if the PIN is compromised. These security limitations expose customers to financial fraud and reduce trust in ATM-based transactions, highlighting the need for a more advanced and reliable authentication mechanism.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901014

This project introduces an ATM System with Face Recognition, where users are authenticated using facial biometric data along with secure backend validation. The system is developed using Flask as a web framework, Python for backend processing, and machine learning libraries for
Facial recognition. The face recognition model analyzes facial features and compares them with stored encodings in the database. If the match is successful, the user is granted access to ATM functionalities. The goal of this system is to improve banking security, reduce fraud, and enhance user convenience. This solution aligns with modern banking trends that emphasize digital transformation and biometric verification.

II. LITERATURE REVIEW

Several researchers have explored the use of biometric authentication and intelligent systems to enhance the security of Automated Teller Machines (ATMs), aiming to overcome the limitations of traditional card- and PIN-based mechanisms. Ashwini C. et al. (2020) proposed a cardless multi-banking ATM system that replaces conventional authentication with a combination of fingerprint recognition, face recognition, and one-time passwords (OTP). Their three-factor authentication model significantly improves security by eliminating physical cards and static PINs. However, the system is primarily designed as an academic prototype, and critical aspects such as facial liveness detection, robustness against spoofing attacks, and scalability for real-world ATM deployment were not thoroughly evaluated. Additionally, usability under actual ATM operating conditions remains unclear.

Akshay Kumar et al. (2023) introduced a smart ATM transaction system that authenticates users using face recognition combined with OTP verification. The proposed model employs YOLO-based face detection and matching techniques, reducing dependency on ATM cards and PINs. The authors utilized a relatively large dataset of approximately 10,000 images, indicating promising recognition accuracy. Nevertheless, the study lacks real-world ATM testing, and issues related to dataset bias and protection against spoofing attacks using photographs or videos are not sufficiently addressed. This limits the system's reliability in uncontrolled environments.

Emad Afaq Khan and Sumaira Muhammad Hayat Khan presented a two-way authentication system for ATMs using Eigenface-based facial recognition. Their work demonstrated that integrating facial biometrics can enhance ATM security compared to traditional methods. However, Eigenfaces represent a classical approach to face recognition and are sensitive to variations in lighting, pose, and facial expressions. The absence of deep learning techniques and liveness detection mechanisms reduces the robustness of the system. Furthermore, the evaluation details and performance metrics provided in the study are limited.

Mehak Bhatia et al. proposed an architecture-level framework for integrating CNN-based face recognition into ATM systems, aiming to reduce or eliminate reliance on physical cards.
Their work highlights the potential of deep learning for improving ATM security and user convenience.
However, the study remains largely conceptual, lacking experimental validation, real-time performance analysis, and evaluation against common fraud scenarios such as spoofing or unauthorized access.

More recently, Dayana R. et al. (2025) presented a face biometric authentication system for ATMs using deep learning. Their approach combines traditional ATM card usage with deep CNN-based face recognition and incorporates liveness detection to prevent photo, video, and mask attacks. This work addresses a major limitation found in earlier studies by focusing on spoofing resistance. Despite this advancement, the system appears to have been tested mainly in controlled or laboratory environments. Large-scale deployment across ATM networks and performance evaluation under varying lighting conditions, camera angles, and user behavior require further investigation.

Overall, the literature indicates a clear shift toward AIML-based biometric authentication for ATM security. While face recognition combined with card detection and multi-factor authentication significantly enhances protection against fraud, existing studies often lack large-scale real-world validation, comprehensive liveness detection evaluation, and deployment feasibility analysis. These gaps motivate the need for a robust ATM authentication system integrating card detection, deep learning–based face recognition, and AIML techniques validated under real ATM operating conditions.

III. PROBLEM STATEMENT

Traditional ATM systems primarily rely on card-based authentication and PIN verification, which are vulnerable to security threats such as card skimming, PIN theft, shoulder surfing, and unauthorized access. With the increasing

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901014

number of financial fraud cases, there is a critical need for a more secure, reliable, and user-friendly authentication mechanism in banking systems. Users often face risks associated with lost or stolen cards, forgotten PINs, and identity theft, which compromise both personal data and financial assets.

The proposed ATM System with Face Recognition aims to enhance ATM security by integrating biometric authentication using facial recognition technology. The system is designed to verify a user's identity by capturing and analyzing facial features in real time, in addition to secure password handling and session management. By combining facial encoding, encrypted password storage, and transaction logging, the system ensures multi-layered authentication and improved access control.

This project addresses the problem of unauthorized ATM access by replacing or strengthening traditional authentication methods with a biometric-based solution.

The goal is to develop a secure, efficient, and scalable ATM system that minimizes fraud, improves user trust, and ensures safe banking transactions through advanced facial recognition and secure software architecture.

IV. METHODOLOGY

1.Card Scanning Module

The card scanning module is the first level of authentication in the proposed ATM system. When a user inserts or scans the ATM card, the system reads the card details such as card number and account identifier. These details are fetched and validated against stored records maintained using CSV files and Pandas for structured data handling. The OS and Shutil libraries support secure file access and management. If the scanned card information matches an existing account, the system generates a unique session ID using the Random and String modules and proceeds to the next authentication stage. If the card is invalid or unregistered, access is denied, and the session is terminated.

2. Face Verification Module

After successful card authentication, the system activates the camera for facial verification. Using OpenCV, Imutils, NumPy, and Pillow, the captured facial image is preprocessed by resizing, normalization, and noise reduction. Face detection is performed to extract the region of interest, followed by feature extraction using AIML-based techniques.

A trained machine learning model, implemented with scikit-learn and deep learning concepts, compares the real-time facial features with the stored facial templates linked to the scanned card. Threading ensures real-time processing without interrupting the user interface. This module ensures that only the genuine account holder proceeds further.

3. PIN Authentication Module

Once face verification is successful, the user is prompted with the PIN entry screen developed using Tkinter. The entered PIN is securely verified against encrypted records stored in the database. Time and DateTime modules are used to track login attempts and enforce time-based restrictions. Multiple incorrect PIN attempts trigger system warnings or temporary account blocking. This module adds an additional layer of security, strengthening the overall authentication mechanism.

4. Transaction Module

After successful completion of all authentication stages, the user is directed to the transaction module. This module provides banking services such as cash withdrawal, balance inquiry, and transaction history viewing. Tkinter is used to design interactive screens, while Pandas manages transaction data. ReportLab is utilized to generate printable transaction receipts. SMTP and Email modules send alerts or transaction confirmations to the registered email address. All transaction activities are logged with timestamps for auditing and security purposes.

5. Security and Monitoring Module

This module continuously monitors system activities, login attempts, and transaction behavior. System logs are maintained using CSV files, while OS and Sys modules manage runtime operations. Suspicious activities trigger alerts and session termination. This module ensures system reliability, fraud detection, and secure ATM operation.

- **Module 1 – Card Scanning Module**

The card scanning module starts ATM access by reading essential card details like the card number and account ID. It simulates card data with CSV files, which are accessed using pandas to quickly check user information. The module confirms that the card is valid and active before moving forward. File handling is managed with os to guarantee secure access. After successful verification, the system moves to the face recognition module, which allows for the next stage of AI-based authentication.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901014

Algorithm – Authentication

The card scanning module starts by launching the ATM application and setting up the needed libraries. The system shows the card scanning interface using Tkinter and reads card details from a CSV database using pandas. The system captures the user's card number as a simulated scan and checks it against the stored records. It verifies if the card is active or blocked. If the card is invalid, an error message appears and the process stops. If the card is valid, the system securely stores the user session details and grants access to the face recognition module for further authentication.

- **Module 2 – Face Verification**

After card authentication, the system captures the user's face with the camera. The image is preprocessed by being resized, normalized, and denoised. Then, the system detects the face. It extracts features and compares them with stored templates using an AI/ML model. Threading ensures smooth real-time verification. Only the verified account holder can proceed to the PIN screen.

Algorithm –

- Turn on the camera after verifying the card.
- Take the facial image.
- Process the image by resizing, normalizing, and removing noise.
- Find the face and extract features.
- Compare with stored facial templates using a machine learning model.
- If there is a match, proceed to the PIN module; otherwise, deny access.

- **Module 3 – PIN Authentication**

After the user verifies their face, they enter their PIN. The system checks it against encrypted records. The system tracks login attempts, and multiple failures may lead to warnings or temporary blocking.

Algorithm –

- Show the PIN entry screen.
- Enter the PIN and encrypt it.
- Compare it with stored records.
- If it's correct, proceed to the transaction module; if not, warn the user.
- Monitor login attempts and apply time-based restrictions.

- **Module 4 – Transcation**

Once the user is logged in, they can perform transactions such as withdrawing money, checking their balance, or viewing their history. Data is handled with Pandas, receipts are created using ReportLab, and email alerts are sent through SMTP.

Algorithm –

- Display transaction menu.
- Select operation (withdrawal, balance, history).
- Update and log transaction data in CSV.
- Generate receipt using ReportLab.
- Send email alerts if enabled.

- **Module 5 – Security and Monitoring**

This module tracks all activities, login attempts, and transactions. It keeps logs, and any suspicious activities trigger alerts or session termination to prevent fraud.

Algorithm -

- Monitor system and transaction logs continuously.
- Detect unusual activities.
- Log activities in CSV files.
- If something looks suspicious, send an alert and terminate the session.
- Make sure ATM operations are secure and reliable.

V. CONCLUSION

The ATM System with Face Recognition project successfully demonstrates how biometric technology can be integrated with traditional banking operations to enhance security, reliability, and user convenience. By combining facial recognition with secure password hashing and session management, the system introduces a multi-layered authentication mechanism that significantly reduces the risk of unauthorized access, card fraud, and identity theft. The implementation using Python, Flask, and image processing libraries ensures that the system remains efficient, scalable, and adaptable to real-world requirements.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901014

Through structured modules such as user authentication, face recognition, transaction management, and security control, the system maintains organized workflow and secure data handling. The use of facial encoding and comparison techniques strengthens identity verification, while transaction logging ensures transparency and accountability. Additionally, the system architecture supports smooth interaction between frontend, backend, and database components.

Overall, this project highlights the potential of biometric-enabled ATM systems in modern banking environments. It provides a practical solution to existing security challenges while improving user experience. Future enhancements may include advanced deep learning models, cloud-based storage, and integration with core banking systems to further increase accuracy, scalability, and real-time performance.

REFERENCES

1. Prasanna, D., Ahamed, N. A., Abinesh, S., Karthikeyan, G., & Inbatamilan, R. (2024, November). Cloud-based automatically human document authentication processes for secured system. In *2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS)* (pp. 1–7). IEEE.
2. Sugumar, R. (2025). Explainable AI-driven secure multi-modal analytics for financial fraud detection and cyber-enabled pharmaceutical network analysis. *International Journal of Advanced Research in Computer Science & Technology (IJARCST)*, 8(6), 13239–13249.
3. Lakshmi, A. J., Dasari, R., Chilukuri, M., Tirumani, Y., Praveena, H. D., & Kumar, A. P. (2023, May). Design and implementation of a smart electric fence built on solar with an automatic irrigation system. In *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 1553–1558). IEEE.
4. David, A. (2020). Air pollution control monitoring & delivery rate escalated by efficient use of Markov process in MANET networks: To measure quality of service parameters. *Test Engineering & Management*.
5. Karthikeyan, K., & Umasankar, P. (2025). A novel buck-boost modified series forward (BBMSF) converter for enhanced efficiency in hybrid renewable energy systems. *Ain Shams Engineering Journal*, 16(10), 103557.
6. Inbavalli, M., & Arasu, T. (2015). Efficient analysis of frequent item set association rule mining methods. *International Journal of Scientific & Engineering Research*, 6(4).
7. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep learning-driven visual analytics framework for next-generation environmental monitoring. *Journal of Applied Science and Technology Trends*, 114–122.
8. Saravanan, M., Kumar, A. S., Devasaran, R., Seshadri, G., & Sivaganesan, S. (2019). Performance analysis of very sparse matrix converter using indirect space vector modulation. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 4756–4762.
9. Poornima, G., & Anand, L. (2025). Medical image fusion model using CT and MRI images based on dual scale weighted fusion based residual attention network with encoder–decoder architecture. *Biomedical Signal Processing and Control*, 108, 107932.
10. Sakthivel, T. S., Ragupathy, P., & Chinnadurai, N. (2025). Solar system integrated smart grid utilizing hybrid coot-genetic algorithm optimized ANN controller. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, 1–24.
11. Ananth, S., Radha, D. K., Prema, D. S., & Nirajan, K. (2019). Fake news detection using convolution neural network in deep learning. *International Journal of Innovative Research in Computer and Communication Engineering*, 7(1), 49–63.
12. Vani, S., Malathi, P., Ramya, V. J., Sriman, B., Saravanan, M., & Srivel, R. (2024). An efficient black widow optimization-based faster R-CNN for classification of COVID-19 from CT images. *Multimedia Systems*, 30(2), 108.
13. Poornachandar, T., Latha, A., Nisha, K., Revathi, K., & Sathishkumar, V. E. (2025, September). Cloud-based extreme learning machines for mining waste detoxification efficiency. In *2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 1348–1353). IEEE.
14. Kumar, A. S., Saravanan, M., Joshna, N., & Seshadri, G. (2019). Contingency analysis of fault and minimization of power system outage using fuzzy controller. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 4111–4115.
15. Dharnasi, P. (2025). A multi-domain AI framework for enterprise agility integrating retail analytics with SAP modernization and secure financial intelligence. *International Journal of Humanities and Information Technology*, 7(4), 61–66.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 9, Issue 1, January-February 2026||

DOI:10.15662/IJRPETM.2026.0901014

16. Prasanna, D., & Manishvarma, R. (2025, February). Skin cancer detection using image classification in deep learning. In *2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1–8). IEEE.
17. Kiran, A., Rubini, P., & Kumar, S. S. (2025). Comprehensive review of privacy, utility and fairness offered by synthetic data. *IEEE Access*.
18. Yashwanth, K., Adithya, N., Sivaraman, R., Janakiraman, S., & Rengarajan, A. (2021, July). Design and development of pipelined computational unit for high-speed processors. In *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1–5). IEEE.
19. Aashiq Banu, S., Sucharita, M. S., Soundarya, Y. L., Nithya, L., Dhivya, R., & Rengarajan, A. (2020). Robust image encryption in transform domain using duo chaotic maps—A secure communication. In *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020* (pp. 271–281). Springer.
20. Madheswaran, M., Dhanalakshmi, R., Ramasubramanian, G., Aghalya, S., Raju, S., & Thirumaraiselvan, P. (2024, April). Advancements in immunization management for personalized vaccine scheduling with IoT and machine learning. In *2024 10th International Conference on Communication and Signal Processing (ICCSP)* (pp. 1566–1570). IEEE.
21. Saravanan, M., & Sivakumaran, T. S. (2016). Three phase dual input direct matrix converter for integration of two AC sources from wind turbines. *Circuits and Systems*, 7, 3807–3817.
22. Ananth, S., Radha, D. K., Prema, D. S., & Nirajan, K. (2019). Fake news detection using convolution neural network in deep learning. *International Journal of Innovative Research in Computer and Communication Engineering*, 7(1), 49–63.
23. Karthikeyan, K., Umasankar, P., Parathraju, P., Prabha, M., & Pulivarthy, P. Integration and analysis of solar vertical axis wind hybrid energy system using modified zeta converter.