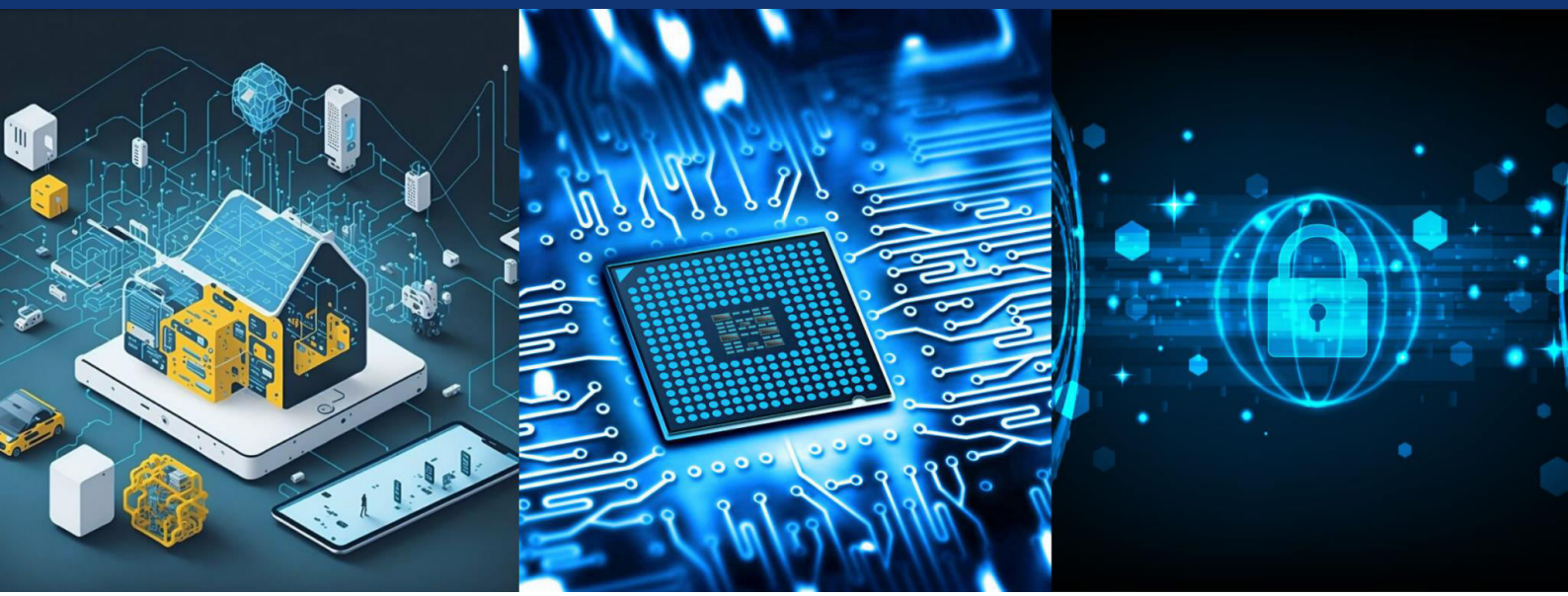
IJIRCCE

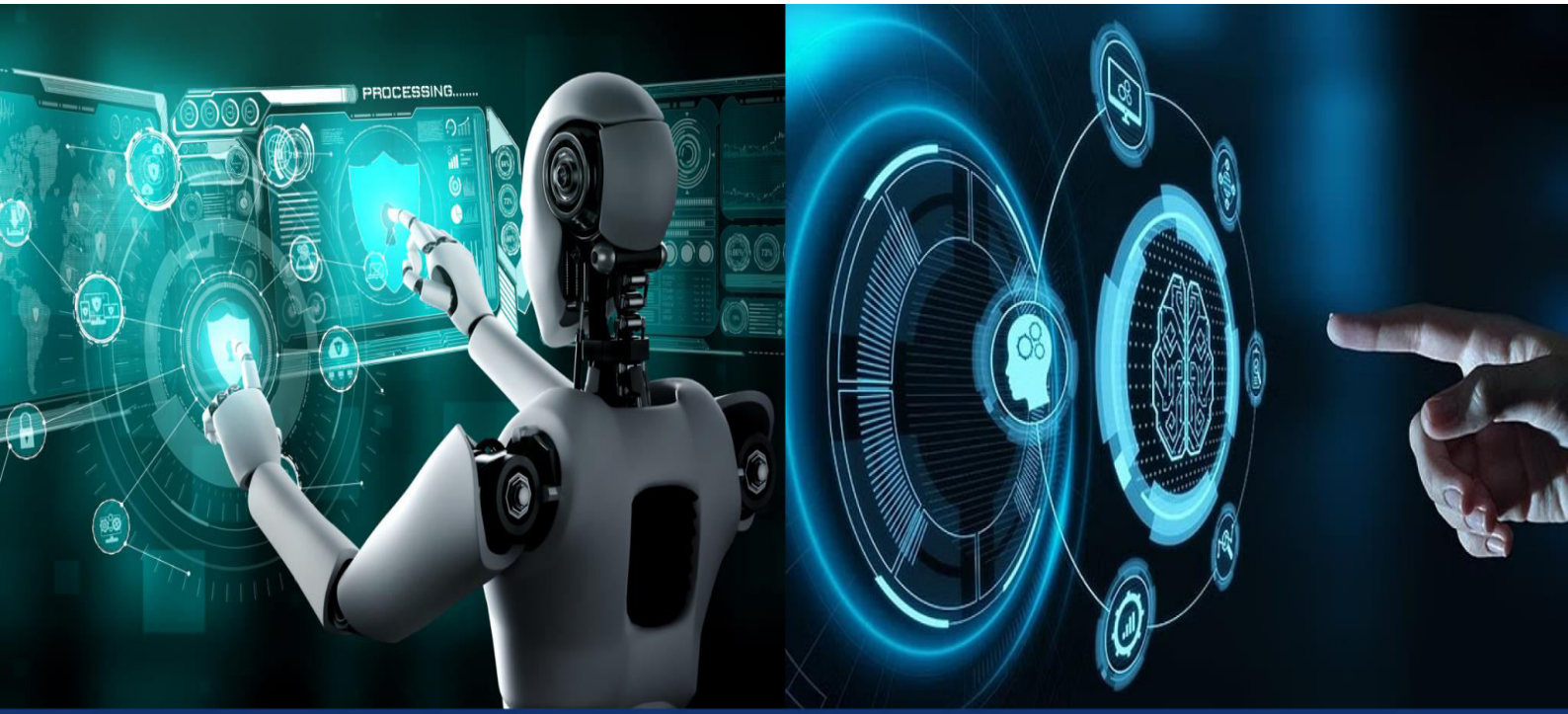
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 5, May 2026

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405070

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Secure Facial Authentication for Multi-Bank ATM Access

R.Gayathri[1], S.Priyadharshini[2]

Assistant Professor, Department of Master of Computer Applications, Vivekanandha Institute of Information and Management Studies Tiruchengode, Namakkal Tamil Nadu, India[1]

PG Scholar, Department of Master of Computer Applications, Vivekanandha Institute of Information and Management Studies, Tiruchengode, Namakkal, Tamil Nadu, India[2]

ABSTRACT: Automated Teller Machines (ATMs) are widely used for quick cash withdrawal and essential banking operations, but they are increasingly targeted by card theft, skimming, shoulder surfing, and unauthorized withdrawals. These frauds occur mainly because traditional ATM systems depend on physical debit cards and PINs, which can be stolen, duplicated, shared, or misused. Existing ATM security systems fail to verify the true identity of the person using the card, lack real-time user validation, and cannot prevent situations where another person performs transactions on behalf of the account holder.

To overcome these limitations, this project introduces a deep learning–based ATM security framework that integrates biometric identity verification with multi-bank transaction access. During account creation, the user's face is captured, processed using MTCNN for detection and alignment, validated by a Liveness CNN, and embedded using FaceNet to generate a secure facial template stored in the bank database.

A debit card is inserted at the ATM, the camera captures the live face, which is aligned, checked for liveness, and compared with the stored FaceNet embedding for authentication. If matched, the ATM retrieves and displays all bank accounts linked to the user, allowing seamless multi-bank withdrawals and operations. The system generates a secure verification link showing the live captured face and sends it to the account holder.

KEYWORDS: Facial Authentication, Automated Teller Machines (ATM) Security, Multi-Bank Access, Deep Learning, FaceNet, Liveness Detection, Biometric Verification, Remote Authorization.

I. INTRODUCTION

Automated Teller Machines (ATMs) have become an essential component of modern banking by providing customers with convenient, fast, and 24×7 access to financial services such as cash withdrawals, deposits, and fund transfers. [1] Despite their widespread adoption, traditional ATM systems primarily rely on debit cards and Personal Identification Numbers (PINs) for user authentication. [2] This approach exposes the system to significant security threats including card theft, skimming, shoulder surfing, PIN compromise, cloning, and unauthorized withdrawals. [3]

These vulnerabilities arise because conventional authentication mechanisms verify possession of a card and knowledge of a PIN, but fail to confirm the true identity of the person performing the transaction. With advancements in biometric technologies and deep learning, facial recognition has emerged as a robust and reliable authentication mechanism. [10] [11] Unlike physical cards and PINs, biometric traits are unique, non-transferable, and difficult to replicate. Integrating facial authentication into ATM systems enhances identity verification by ensuring that only the legitimate account holder can perform financial transactions.

This project, titled "**Secure Facial Authentication for Multi-Bank ATM Access,**" proposes a deep learning–based ATM security framework that incorporates facial recognition, liveness detection, and remote user authorization. [12] [13] The system utilizes Multi-task Cascaded Convolutional Neural Networks (MTCNN) for face detection and alignment, a Convolutional Neural Network (CNN)-based liveness detection model to prevent spoofing attacks, and FaceNet to generate high-dimensional facial embeddings for accurate identity verification.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

In addition to strengthening security, the proposed system introduces multi-bank account integration, enabling users to access multiple linked bank accounts through a single verified facial identity. Furthermore, in scenarios where an unrecognized individual attempts a transaction, the system generates a secure remote approval mechanism, allowing the registered account holder to authorize or deny the transaction in real time. [14] This approach significantly reduces ATM fraud, enhances authentication reliability, and improves user convenience while maintaining banking security standards.

II. LITERATURE REVIEW

Several research studies have attempted to enhance ATM security using machine learning and intelligent fraud detection techniques. Domashova and Kripak (2021) proposed a machine learning–based system to identify non-typical international transactions, helping to detect fraudulent banking activities. Similarly, Domashova and Mikhailina (2021) introduced methods for early detection of money laundering schemes using data-driven approaches. In addition, Sharma and Singh (2024) developed an AI-based fraud detection system that improves the accuracy of identifying suspicious transactions.

Biometric authentication techniques have been widely explored to improve ATM security. Rtayli and Enneya (2020) applied support vector machine methods for credit card risk identification, enhancing fraud detection efficiency. Veena et al. (2022) implemented SVM and KNN algorithms for cyber-crime detection, demonstrating the effectiveness of machine learning in security applications.

Recent advancements in ATM systems have focused on facial recognition technology. Selvakumar et al. (2022) proposed a face biometric authentication system for ATM access using deep learning, ensuring secure and user-friendly transactions. Similarly, Kowshika et al. (2022) developed a face-based ATM authentication system that eliminates the need for physical cards and PINs, reducing fraud risks.

To further enhance system reliability, liveness detection and anti-spoofing techniques have been introduced. Yu et al. (2023) presented a survey on deep learning–based face anti-spoofing methods, which help prevent fake identity attacks using photos or videos.

Traditional authentication systems have also been improved using innovative approaches. Hari Krishna et al. (2021) proposed a PIN authorization method using eye tracking and dynamic keypad generation. Guerar et al. (2020) developed secure PIN-based authentication techniques. Das et al. (2020) introduced an eye pupil movement-based authentication system for enhanced security.

Despite these advancements, existing systems still rely on single-layer authentication or additional hardware requirements. Therefore, there is a need for an integrated system that combines facial recognition, liveness detection, and multi-bank access into a unified ATM security framework.

III. METHODOLOGIES

System Architecture

The proposed ATM security framework is designed as a software-based ATM simulator integrated with biometric authentication, multi-bank access, and remote authorization mechanisms. The system is developed using Python, Flask, MySQL, Bootstrap, and WAMP server environment to simulate real-time ATM operations without physical hardware deployment.

The architecture consists of interconnected modules including ATM interface control, face enrollment and authentication, multi-bank account management, remote authorization, transaction processing, alert generation, and security logging. Each module collaboratively ensures secure, reliable, and user-centric banking operations.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405070

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

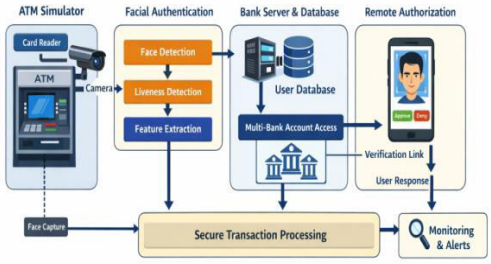


Figure 1: System Architecture of the Proposed ATM Security System

Figure 1: System Architecture

ATM Simulator and System Control

The ATM Simulator module replicates real-world ATM functionality in a controlled software environment. It manages debit card insertion simulation, camera activation, authentication workflow initiation, bank selection interface, and transaction execution.

This module acts as the central coordination layer, establishing communication between facial recognition models, bank servers, and remote authorization services. It ensures proper session handling and secure data transmission during ATM operations.

User and Administrative Interaction

The system supports three primary interaction levels: ATM system control, account holder interaction, and bank employee management.

The ATM control unit handles card detection, face capture, authentication processing, and transaction initiation. The account holder interaction module manages on-screen guidance and remote verification procedures when authentication discrepancies occur.

Additionally, a dedicated administrative interface enables bank employees to manage account registration, facial enrollment, transaction monitoring, and security maintenance. This ensures proper oversight and fraud prevention.

Face Enrollment Module

The face enrollment module is responsible for registering and training the biometric model during account creation. Initially, a short video of the account holder's face is captured to generate a diverse dataset containing multiple facial angles and expressions.

The recorded video is converted into image frames, which undergo preprocessing techniques such as resizing, normalization, and noise removal. Face detection is performed to isolate the facial region and eliminate background interference.

Subsequently, distinctive facial features are extracted and organized into identity-specific embeddings. The facial recognition model is trained using this processed dataset and deployed securely on the bank server for real-time authentication during ATM transactions.[12]

Facial Authentication Module

During ATM operation, once a card is inserted, the system captures live facial input using the integrated camera. The MTCNN algorithm performs accurate face detection and alignment to standardize facial orientation.

To prevent spoofing attacks, a CNN-based liveness detection mechanism analyzes eye blinking patterns and facial texture variations.

Only after successful liveness verification is the image passed to the FaceNet model for embedding generation.

The generated embedding is compared with stored biometric templates using cosine similarity measurement. [13] If the similarity score exceeds a predefined threshold, the user is authenticated; otherwise, access is denied and appropriate security actions are triggered.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Multi-Bank Account Access

The proposed framework enables unified access to multiple bank accounts using a single verified facial identity. After successful authentication, the system retrieves all bank accounts linked to the authenticated user from the centralized database.

These accounts are displayed on the ATM interface, allowing the user to select the desired financial institution for transaction execution. This approach eliminates the need to carry multiple debit cards and enhances cross-bank usability while maintaining strong identity verification controls.

Remote Authorization Mechanism

In cases where facial authentication fails or detects an unknown face, the remote authorization module is activated. The system generates a secure, time-limited verification URL containing transaction details, ATM location, timestamp, and the captured facial image.

The verification link is transmitted to the registered mobile number or email address of the account holder. Through a secure web interface, the account holder can review the transaction request and either approve or deny it.

If approved, the transaction proceeds; if denied, the request is blocked and security alerts are generated. This mechanism provides an additional security layer while maintaining user convenience.

Transaction Processing Module

Once authentication or remote authorization is completed successfully, the transaction processing module executes the selected banking operation. The module communicates securely with the bank server to validate account balance, update transaction records, and authorize cash dispensation.

It ensures transactional integrity, reliability, and proper exception handling in case of system errors or interruptions. Upon completion, confirmation messages are displayed to the user.

Alert and Notification System

The alert module provides real-time communication between the ATM system and the account holder.

Notifications are generated for authentication failures, verification requests, approvals, denials, and suspicious activity detection.

Secure communication channels such as SMS and email are utilized to ensure timely delivery of alerts, thereby enhancing transparency and user trust.

Security Logging and Monitoring

All authentication attempts, transaction activities, timestamps, and ATM location details are continuously recorded in secure log storage. The logging mechanism protects records from unauthorized modification and supports auditing and fraud investigation.

By analyzing repeated failures or abnormal transaction patterns, the system assists administrators in detecting potential security threats and ensuring compliance with banking security standards.

IV. ALGORITHM

1. **Start**
2. User inserts the ATM debit card into the ATM system.
3. The ATM camera captures the **live facial image** of the user.
4. **Face detection and alignment** are performed using MTCNN to locate and normalize the face.
5. **Liveness detection** is applied using a CNN model to verify that the captured face belongs to a live person and not a spoof attempt.
6. If liveness detection **fails**, the system immediately triggers the **remote authorization mechanism** and terminates the local authentication process.
7. If liveness detection **succeeds**, facial features are extracted using the **FaceNet model** to generate a facial embedding.
8. The generated embedding is compared with the **stored facial template** in the bank database using cosine similarity.
9. If the similarity score exceeds the predefined threshold: The user is successfully authenticated. The system retrieves and displays all **linked bank accounts**. The user selects the required bank and proceeds with the transaction.
10. If the similarity score is below the threshold: The system activates the **remote authorization module**. A secure verification request containing the captured face and transaction details is sent to the registered account holder.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405070

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

11. Based on the account holder's approval or denial:
Approved: Transaction is allowed.
Denied: Transaction is blocked and security alerts are generated.
12. **End**

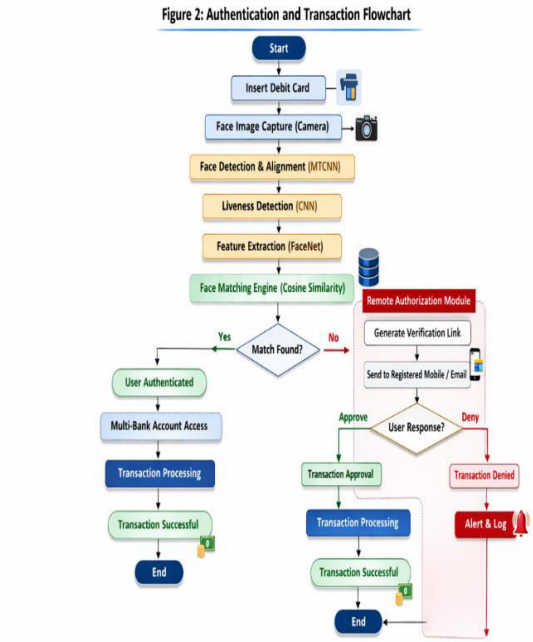


Figure 2: Flowchart

Image capturing
To create the database, an image of each user's face is captured using a webcam. This image serves as a primary data point within the database, essential for efficient face recognition during verification. When a user initiates a transaction, the system references this stored image to compare with the live image captured.
By using facial images as the main identifier, the database allows quick and accurate identity verification, ensuring only authorized individuals can access the system. This approach strengthens security by integrating biometric data, providing a reliable foundation for the face recognition verification process.

Pre-processing
The system employs pre-processing techniques to enhance the quality of images for effective face recognition. Image acquisition captures high-quality images, while image resizing standardizes dimensions and speeds up processing. Histogram equalization improves image clarity, and normalization adjusts pixel intensity levels for consistency.
Additionally, grayscale conversion transforms color images into shades of grey, simplifying the data by focusing on intensity rather than color. Together, these techniques refine the captured images, ensuring uniformity and clarity before analysis. This pre-processing stage is crucial for reliable and accurate face recognition, as it provides standardized inputs that improve the recognition model's performance.

Liveness detection
Liveness detection is actually a biometric security feature meant to confirm that the biometric sample is from the live person instead of one displaying a photograph or video or with respect to the fake person. It uses liveness detection techniques such as blinking in the eyes or reflection in the eyes or head movement detection to confirm that it is indeed the user there and not trying to play a trick on the system.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405070

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

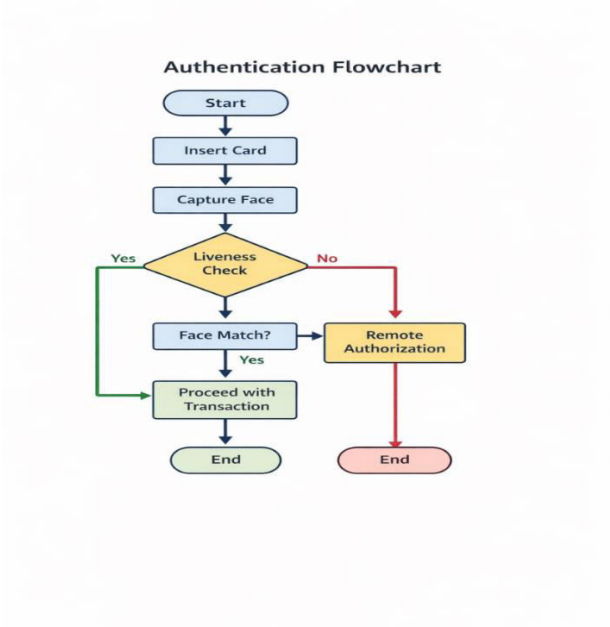


Figure 3: Authentication Flowchart

V. RESULT ANALYSIS

S.NO	EXISTING	PROPOSED
1	Relies on debit card and PIN authentication	Uses deep learning–based facial authentication
2	Vulnerable to card theft, skimming, and PIN attacks	Prevents unauthorized access using biometric verification
3	No real-time identity verification mechanism	Performs real-time facial recognition and authentication
4	Unable to detect spoofing attacks using photos or videos	Uses Liveness CNN for anti-spoofing detection
5	Supports only single-bank operations	Supports secure multi-bank account access
6	OTP-based verification may suffer from delays and phishing attacks	Uses secure remote authorization mechanism
7	CCTV surveillance is limited to post-event	Prevents fraud before transaction execution

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

	investigation	
8	Requires users to remember PINs	Provides secure PIN-less transactions
9	Limited fraud monitoring capabilities	Provides real-time alerts and security logging
10	Existing systems are reactive to fraud attempts	Proposed system is proactive and fraud-resistant

VI. CONCLUSION

In conclusion, the comprehensive design and development of the project is centered on enhancing both security and user convenience through advanced biometric technologies. The system employs Python and Flask for back-end efficiency, OpenCV and Tensor Flow for real-time facial recognition and liveness detection, and MySQL for structured and secure storage of user and transaction data. Key functionalities, such as face enrollment, multi-bank account access, remote authorization, transaction processing, alert notifications, and security logging, work together to provide a seamless, PIN-less, and fraud-resistant ATM experience. These modules ensure accurate identity verification, prevent unauthorized access, enable controlled delegated transactions, and facilitate transparent monitoring of all ATM activities.

REFERENCES

[1] K. Riad and M. Elhoseny, "A Blockchain-Based Key-Revocation Access Control for Open Banking," Wireless Communications and Mobile Computing, vol. 2022, pp. 1–10, 2022.
[2] K. Lee, S.-Y. Lee, and K. Yim, "Classification and Analysis of Security Techniques for the User Terminal Area in the Internet Banking Service," Security and Communication Networks, vol. 2020, pp. 1–16, 2020.
[3] J. Domashova and E. Kripak, "Identification of Non-Typical International Transactions on Bank Cards Using Machine Learning Methods," Procedia Computer Science, vol. 190, pp. 178–183, 2021.
[4] J. Domashova and N. Mikhailina, "Usage of Machine Learning Methods for Early Detection of Money Laundering Schemes," Procedia Computer Science, vol. 190, pp. 184–192, 2021.
[5] N. Rtayli and N. Enneya, "Selection Features and Support Vector Machine for Credit Card Risk Identification," Procedia Manufacturing, vol. 46, pp. 941–948, 2020.
[6] K. Veena, K. Meena, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, "SVM and KNN Techniques for Cyber-Crime Detection," Wireless Communications and Mobile Computing, vol. 2022, pp. 1–9, 2022.
[7] S. M. Hari Krishna et al., "Development of PIN Authorization Using Eye Tracking and Dynamic Keypad," in Proc. I2CT, 2021, pp. 1–6.
[8] M. Guerar et al., "Securing PIN-Based Authentication in Smartwatches," Concurrency and Computation: Practice and Experience, vol. 32, no. 18, 2020.
[9] I. Das et al., "Eye Pupil Movement-Based PIN Authentication System," in Proc. IEEE VLSI, 2020, pp. 1–6.
[10] M. Selvakumar et al., "Face Biometric Authentication System for ATM Using Deep Learning," in Proc. ICESC, 2022, pp. 647–655.
[11] P. Kowshika et al., "Face Biometric Authentication System for ATM," NVEO Journal, pp. 1859–1872, 2022.
[12] J. Deng et al., "ArcFace: Deep Face Recognition Using Angular Margin Loss," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 10, pp. 5962–5979, 2023.
[13] Z. Yu et al., "Deep Learning for Face Anti-Spoofing: A Survey," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 125–139, 2023.
[14] A. Sharma and P. K. Singh, "AI-Based Fraud Detection in Banking Systems," IEEE Access, vol. 11, pp. 45872–45885, 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details