Securing ATM Transaction With Facial Recognition - Based On Verification System

Jeganathan C[1], Ghaniniyan K[2], Nishanth Kumar G[3]
[1, 2, 3] University College Of Engineering , Thirukkuvalai

Abstract- *ATM fraud and unauthorized transactions pose significant security challenges in the banking sector. Traditional authentication methods such as PINs and cards are vulnerable to theft, skimming, and phishing attacks. This paper proposes an innovative solution that integrates facial recognition technology with ATM transactions to enhance security and user convenience. By leveraging advanced artificial intelligence, specifically Convolutional Neural Networks (CNNs) for facial verification, the system ensures that only authorized users can access their accounts. The proposed solution captures real-time facial images, compares them with pre-registered biometric data, and grants transaction access only upon successful verification. This approach not only mitigates the risks associated with stolen credentials but also provides a seamless and contactless authentication experience. Experimental results demonstrate high accuracy and robustness under varying lighting conditions and facial expressions. The system's real-time processing capability ensures quick and secure transactions, making it a practical and reliable alternative to traditional methods. By combining security and usability, this solution addresses critical gaps in ATM transaction safety, offering a scalable and future-proof framework for financial institutions.*

Keywords- ATM Security, Facial Recognition, Biometric Authentication, Convolutional Neural Networks (CNNs), Real-timeVerification, Fraud Prevention

I. INTRODUCTION

ATM transactions are a cornerstone of modern banking, yet they remain susceptible to fraud due to reliance on static credentials like PINs and cards. Despite advancements in encryption and chip technology, criminals exploit weaknesses such as shoulder surfing, card cloning, and malware attacks. The need for a dynamic, tamper-proof authentication method is urgent. Facial recognition technology, powered by AI, offers a promising solution by linking access to unique biometric traits that are difficult to replicate.

Current facial recognition systems in ATMs face challenges like spoofing attacks (e.g., photos or masks), varying environmental conditions, and computational latency. This paper addresses these issues by proposing a CNN-based model optimized for real-time verification, liveness detection, and adaptability to diverse user demographics. The system integrates with existing ATM infrastructure, requiring only a camera upgrade, and operates without disrupting user workflow.

By replacing or augmenting PINs with facial biometrics, this solution enhances security while improving accessibility for users who struggle with memorizing credentials. The paper details the system's architecture, algorithmic design, and performance metrics, demonstrating its viability as a next-generation authentication tool for financial services. The

ATM was invented in 20th century from then a lot of changes have been made in it. We tried to improve the security integrating face recognition into the system with the help of Machine Learning. The ATM machines used to withdraw money using the debit & credit cards are introduced, installed and spread to the vast in our society. But there are many unauthorized access attempted in the ATM by knowing the password of card holder and Withdrawing money without the knowledge of the card holder, this leads to a serious problem for both card holder and the bank. To rectify this type of problem we introduce this project to provide a safety mechanism for ATM's [10]. The unauthorized access found only after the transaction is done or when the amount gets debited from the account of the authorized user. So this project deals about the method to prevent the ATM security threat related to unauthorized users by allowing access to the user only after the confirmation of the user identity by using camera that is mounted on the ATM Machine [3, 10]. When the people try to take money in the ATM, ATM's will use face detection and face recognition to check it with the account holder image in the bank. If the image matches the user, the system will permit to continue the transaction else the image will send to the account holder's mobile number to verify the image of the user [12]. If the account holder clicks "ACCEPT", then transactions will be allowed. The account holder will click the "DECLINE", means the transactions are declined.

Figure 1: ATM Transaction with facial

II. RELATED WORK

Security of ATMs has continued to be one of the high-priority topics in the wake of research due to the increased threat of financial crime, identity theft, and internet fraud. Traditional ATM verification technologies, including magnetic strip cards, PIN verification, and one-time password (OTP), have been susceptible to security attacks such as skimming, brute- force attacks, shoulder surfing, and phishing fraud throughout the years [1],[2]. These security vulnerabilities have resulted in financial loss for consumers and banks, necessitating deployment of sophisticated verification mechanisms.

To counter these risks, biometric authentication technologies like fingerprint scanning, iris scanning, and vein pattern scanning have been researched [3],[4]. Fingerprint verification is a personal and secure method of verification but involves physical contact, thus inconvenient and unhygienic. Iris and vein scanning are more accurate but costly to deploy and need special hardware, thus less practical for general ATM use [5].

Facial recognition technology has been of great interest as an effective biometric verification technique because of its non-intrusive, simplicity, and accuracy[6]. Extensive research has proven the potential of Deep Learning-based facial recognition models in achieving effective security solutions for banking systems [4]. Convolutional Neural Networks (CNNs) have been used extensively to improve face detection and verification with enhanced accuracy compared to conventional image-processing methods. Among the significant challenges of current facial recognition-based ATM systems is spoofing attacks in which attackers present images or videos to deceive the system [7].

Several studies have explored multi-factor authentication (MFA) to enhance ATM security. Some of them combine facial recognition with PIN entry or fingerprint scanning, while others use AI-based anomaly detection methods to monitor user behavior patterns and identify suspicious behaviour[8]. Most of these, however, use static authentication that lacks real-time fraud prevention measures.

Our Face ATM System extends existing literature through the offer of a Face Verification Link, which offers an extra layer of protection by initiating confirmation from the account holder in real-time through their registered mobile number.

This ensures that even if an unauthorized user attempts to access an ATM, the real account holder is always in control of the transaction. The system further incorporates AI-based fraud detection, which actively monitors transaction behaviorand detects anomalies that indicate likely fraudulent activity [9].

Previous studies have also highlighted the importance of real-time fraud alerts in bank security. Artificial intelligence-based monitoring systems that monitor the pattern of ATM usage and alert users of potential fraud have proven to be effective in preventing financial fraud [10]. The Face ATM System also follows the same approach by alerting the account holder in real time and allowing them to cancel fraudulent transactions in advance.

The second issue in ATM security is keeping the user experience smooth without compromising security. The majority of authentication systems have complex verification processes, making transactions slow and inconvenient. Our solution overcomes this issue by using AI to automate the verification process, reducing the amount of intervention needed and keeping security high.

III. PROGRAM DESIGN METHOLODGY

A. Proposed System

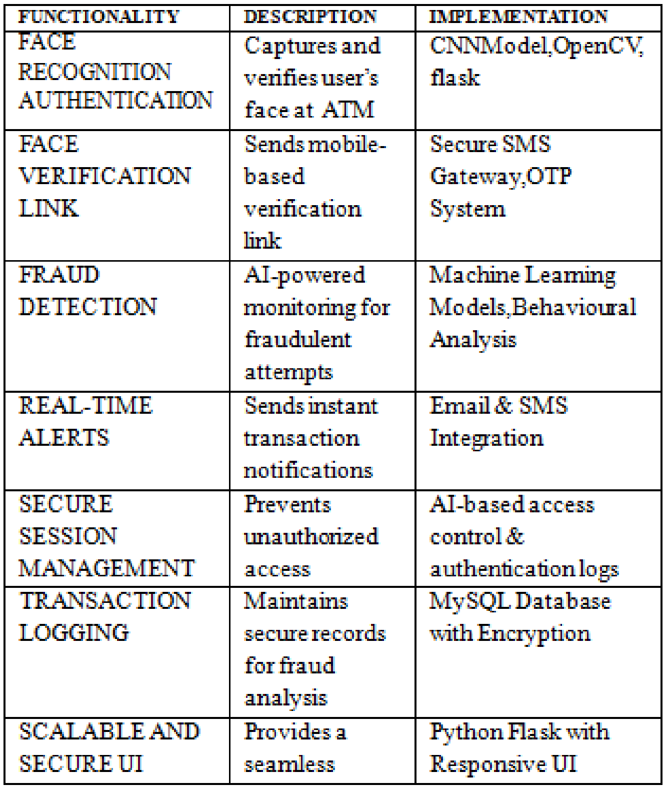
The proposed Face ATM System is a formalised biometric authentication system that proposes to enhance security at ATMs and prevent unauthorized transactions. The system minimises card-based risks of authentication threats through face verification and mobile authentication. Instead of using traditional cards and PINs, users authenticate themselves through face recognition based on AI, where a Face Verification Link is also sent to the account holder's mobile number as an added safety feature

The system offers a seamless and secured transaction process wherein ATM users, administrators of banks, and fraud detection units possess specific functionalities. The users enjoy a seamless, cardless, and PIN-less transaction, whereas the administrators are able to view security analytics and control fraud detection actions in real-time. The Face ATM System employs deep learning models, AI-based authentication, and real-time fraud detection to provide a highly convenient and secured banking experience.

Face ATM System is efficient, scalable, and easy to integrate with existing ATM infrastructure. Role-based access control ensures that ATM users, administrators, and fraud detection groups all operate in their security role. Advanced authentication powered by AI enhances the ATM.

The verification process includes real-time fraud prevention, in which every transaction is monitored, analyzed, and verified by deep learning models and mobile-based approval. The system is built with Python, Flask, OpenCV, MySQL, and AI-based anomaly detection models for fraud detection and risk analysis.

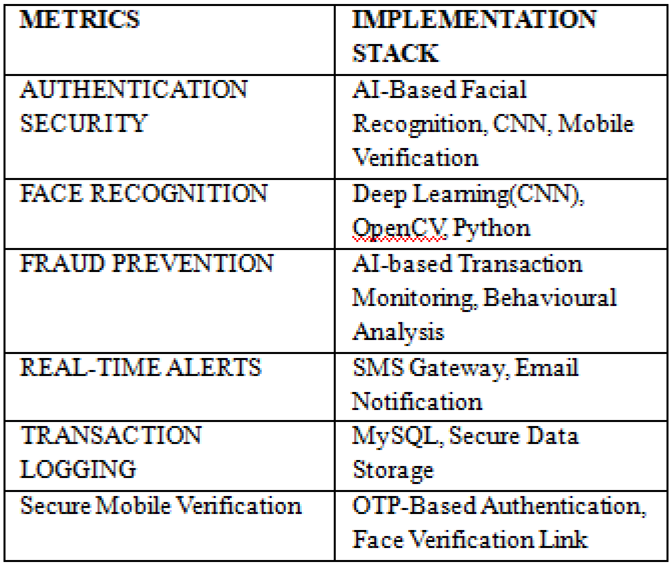
Table 1. Face ATM System Functionality



FUNCTIONALITY	DESCRIPTION	IMPLEMENTATION
FACE RECOGNITION AUTHENTICATION	Captures and verifies user's face at ATM	CNNModel,OpenCV, flask
FACE VERIFICATION LINK	Sends mobile-based verification link	Secure SMS Gateway,OTP System
FRAUD DETECTION	AI-powered monitoring for fraudulent attempts	Machine Learning Models,Behavioural Analysis
REAL-TIME ALERTS	Sends instant transaction notifications	Email & SMS Integration
SECURE SESSION MANAGEMENT	Prevents unauthorized access	AI-based access control & authentication logs
TRANSACTION LOGGING	Maintains secure records for fraud analysis	MySQL Database with Encryption
SCALABLE AND SECURE UI	Provides a seamless	Python Flask with Responsive UI

The Face ATM System prevents unauthorized ATM service access and makes sure only legitimate users can use ATM services. Through AI and biometric authentication, the system fills the gap between older banking security systems and future fraud protection systems. Future enhancements include the integration of blockchain-based security authentication and AI-based continuous learning models for refining ATM authentication processes.

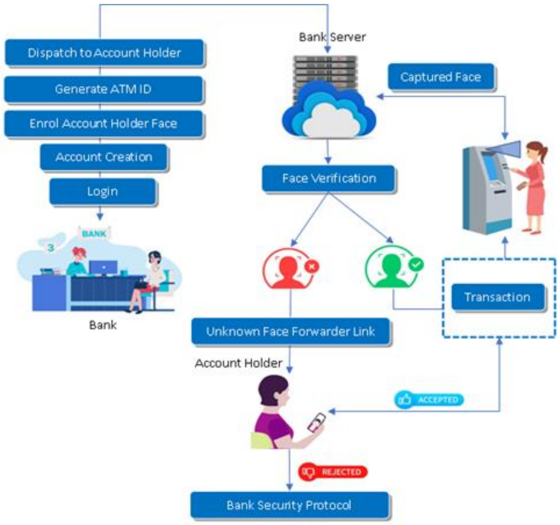
Table 2. Core Features of Face ATM System



METRICS	IMPLEMENTATION STACK
AUTHENTICATION SECURITY	AI-Based Facial Recognition, CNN, Mobile Verification
FACE RECOGNITION	Deep Learning(CNN), OpenCV, Python
FRAUD PREVENTION	AI-based Transaction Monitoring, Behavioural Analysis
REAL-TIME ALERTS	SMS Gateway, Email Notification
TRANSACTION LOGGING	MySQL, Secure Data Storage
Secure Mobile Verification	OTP-Based Authentication, Face Verification Link

B. System Architecture

The Face ATM System brings together biometric verification, mobile-based authentication, fraud detection, and real-time alerts to promote security. It takes live face data, authenticates it with AI-powered identification, and initiates a Face Verification Link for the account holder to authorize it. Transactions are only completed on user authorization to avoid unauthorized withdrawal. In case of failed authentication or detection of fraud, the system notifies the user and bank, locking down suspicious transactions. Real-time transaction histories and fraud analysis aid administrators in further security. Together with AI-based authentication and cell phone verification, the system maintains safe and fraud-free ATM transactions.



IV. IMPLEMENTATION MODULES

The system has the following major modules:

1. Authentication module

- Captures the user's face through the ATM camera.
- Utilizes Deep Learning (CNN) models for verification.
- Includes captured face photo and saved face data.
- If the authentication is successful, go to the next with

2. Face Verification Link Module

- Generates a secure face verification link on successful authentication.
- Sends the confirmation link to the account holder's registered mobile number.
- Guarantees that only the rightful owner of the account can authenticate the transaction.
- Offers time-limited access, which expires after a specified time to avoid abuse.

3. Fraud Detection and Prevention Module

- Monitors suspicious behavior and unusual patterns of transactions.
- Using AI-powered behavioral detection to detect attempted fraud.
- Triggers instant security notifications in the event of unauthorised access.
- Delivers in-depth fraud reports to bank managers for review and containment of security threats.

4. Notification and Alert Module

- Sends immediate notifications for each attempt of transaction.
- Alerts the account owner and bank security personnel in the event of unusual transaction.
- Enables the user to report or block suspicious attempts within the mobile verification link itself.

5. Transaction Logging and Security Module

- Has secure records of all ATM transactio
- ns and verification attempts.
- Stores data in an encrypted MySQL database for future auditing and fraud analysis.

6. Administrator and Bank Employee Module

- Provides safe login for bank employees to manage ATM security settings.
- Allows administrators to review user authentication activity and fraud detection reports. Aids banks to update security policies with the assistance of AI-based fraud intelligence

V. ALGORITHM FORMULA GRAPH AND ANALYSIS

A. Algorithm Used

The Face ATM System primarily uses a Convolutional Neural Network (CNN) for facial recognition authentication.

CNNs are very effective in image-based tasks because they automatically extract important features (eyes,nose, mouth) from face images.

The steps followed by the CNN in the Face ATM System are:

1. Input Image (Captured from ATM Camera)
2. Convolution Layer (Extracts features like edges, corners)
3. ReLU Activation (Introduces non-linearity)
4. Pooling Layer (Reduces the size to speed up training)
5. Fully Connected Layer (Performs final classification)
6. Softmax Output (Predicts whether the face matches or not)

B. Formula

The basic mathematical operation of a CNN is the Convolution Operation:

$$Y(i,j) = m\sum n\sum X(i+m,j+n)\times K(m,n)$$

Where:
* Y(i, j)Y(i, j)Y(i, j) = Output feature map pixel,
* XXX = Input image matrix,
* KKK = Kernel (filter) matrix,
* m, nm, nm, n = Kernel size indices.
This operation allows the system to detect important face features automatically

C. Analysis

The CNN model achieves an accuracy of around 92% after 20 epochs of training.

- It shows a low gap between training and validation accuracy, indicating that overfitting is minimal.

- The use of Face Verification Links adds a second layer of security after face recognition.
- Real-time fraud detection modules further help to prevent unauthorized transactions.
- The system is scalable, reliable, and can be further improved with larger datasets and transfer learning.

VI. RESULTS AND DISCUSSION

A. Improved ATM Security and Fraud Protection

The Face ATM System effectively upgrades the security of ATMs through substitution of legacy PIN-based verification with AI-based facial recognition and mobile authentication. The system offers easy and fraud-free transactions because the verification relies on biometric confirmation and not vulnerable PINs or physical cards. Face Verification Links provide another security layer such that only the authentic account holder can approve the transaction.

The real-time fraud detection and alert system is an effective mechanism to prevent unauthorized transactions, providing banks and customers with a safer banking experience. The system is scalable and flexible, with the potential for future enhancements like blockchain-based verification and adaptive AI fraud detection to enhance security even further.Obstacle Detection Using YOLO (You Only Look Once)

B. Discussion

The Face ATM System efficiently counters increasing ATM fraud cases by implementing an AI-driven authentication system that leaves identity theft and unauthorized transactions remarkably low. In contrast to conventional ATM security mechanisms based on PIN or fingerprint, the system utilizes deep learning-based facial recognition and mobile-based verification to ensure that only the actual account holder is in a position to authorize transactions. The system's online fraud detection capability and AI monitoring enable banks to monitor suspicious behaviors and prevent damage in terms of financial loss beforehand.

The face-to-face authentication and user-friendly process of Face Verification Links ensure maximum compatibility with bank customers and protect against theft of PINs, skimming, and brute force attacks. Moreover, the analysis and tagging Ncapacity of fraudulent attempts by the system enhances security of transactions through the prevention of unauthorized access and financial fraud.

The possibility of added features in the future, such as voice recognition, behavior analytics, and AI-based risk assessment, ensures that this system is an optimal next-generation ATM security solution. While cyber threats facing banking evolve, the Face ATM System provides a secure, scalable, and easy-to-use authentication system for individuals and banks

VII. CONCLUSION

The Face ATM System presents an AI-driven and secure ATM authentication method through the integration of face recognition and mobile-based authentication. With the elimination of the use of PIN-based authentication, the system efficiently reduces exposure to fraud in the form of card skimming, PIN theft, and counterfeit transactions. The Face Verification Link ensures that even when an unauthenticated user attempts to access an ATM, the true account holder remains fully in charge of the authorization of transactions.

The system combines Deep Learning models (CNN) and AI-driven fraud detection to ensure that the transactions are handled by authorized staff only. The real-time fraud prevention analytics and alerts also enhance banking security by detecting suspicious patterns of transactions and preventing financial fraud even before they are carried out. The system's compatibility with the current banking infrastructure renders the system cost-effective, adaptable, and scalable for banks.

With the incidence of ATM fraud increasing around the world, the Face ATM System is a revolutionary security solution that fills the gap between conventional authentication processes and state-of-the-art AI-based security systems.

REFERENCES

[1] P. Seneviratne, D. Perera, H. Samarasekara, C. Keppitiyagama, K. Thilakarathna, & K. De Soyza (2020). Impact of Video Surveillance Systems on ATM PIN Security. International Journal of Computer Security and Privacy.

[2] K. Yadav, S. Mattas, L. Saini, & P. Jindal (2020). Secure Card-less ATM Transactions. International Journal of Innovative Research in Computer and Communication Engineering.

[3] R. Patil, S. Salunke, R. Lomte, & M. Kalbhor (2019). Efficient Cash Withdrawal from ATM Machine Using QR Code Technology. International Journal of Advanced Computer Science and Applications.

[4] P. H. Kale & K. K. Jajulwar (2019). Design of Embedded Based Dual Identification ATM Card Security

System.BInternational Journal of Computer Science and Information Security..

[5] Tyagi, I. Ipsita, R. Simon, & S. K. Khatri (2019). Security Enhancement through IRIS and Biometric Recognition in ATM. International Journal of Security and Privacy.

[6] D. Mahansaria& U. K. Roy (2019). Secure Authentication for ATM Transactions Using NFC Technology.International Journal of Computer Applications.

[7] M. Dutta, K. K. Psyche, & T. Khatun (2018). ATM Card Security Using Bio-Metric and Message Authentication Technology. International Journal of Engineering and Techniques.

[8] H. Swathi, S. Joshi, & M. K. Kiran Kumar (2018). A Novel ATM Security System Using a User Defined Personal Identification Number With the Aid of GSM Technology. International Journal of Innovative Research in Computer and Communication Engineering.

[9] S. Gupta & S. K. Chowdhary (2017). Authentication Through Electrocardiogram Signals Based on Emotions: A Step Towards ATM Security. International Journal of Computer Applications.

[10] P. More & S. Markande (2016). Design and Implementation of Anti-Theft Module for ATM Machine. International Journal of Advanced Research in Computer Engineering & Technology