International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

New Approach for Third Generation of ATM Using Artificial Intelligence

[1]B. Lalitha,[2]G. Sravani,[3]K. Anusha,[4]B. Tejaswini,[5]N. Mershi,[6]K. Venkata Vinnela

[1]Assistant Professor, Dept of CSE, Dr.Samuel Gerorge Institute of Engineering & Technology, Darimadugu Village, Markapur, Prakasam, Idupur, Andhra Pradesh 523320.

[2,3,4,5,6]U. G Student, Dept of CSE, Dr.Samuel Gerorge Institute of Engineering & Technology, Darimadugu Village, Markapur, Prakasam, Idupur, Andhra Pradesh 523320.

ABSTRACT *Automated teller machines (ATMs) are well acknowledged to the devices stereotypically used by folks to cart out a variability of personal and business economic transactions and banking tasks. ATMs have become very popular with the general public for their availability and general user friendliness. ATMs are now originated in many positions having a systematic or high volume of consumer movement. For example, ATMs are typically found in restaurants and the supermarkets, Convenience stores, malls, schools, gas stations, hotels, work locations, banking centers and the airports, entertainment establishments, transportation facilities and a myriad of other locations. ATMs are typically available to consumers on a continuous basis such that consumers have the ability to carry out their ATM financial transactions and/or banking functions at any time of the day and on any day of the week. This based on the facial recognition for transaction access.in this person is registered then it will allow for transaction otherwise transaction gets cancelled.*

KEYWORDS: *Artificial Intelligence (AI), Facial Recognition, Biometric Authentication, ATM Security, Deep Learning*

INTRODUCTION

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Automated Teller Machines (ATMs) have transformed banking by providing customers with convenient access to financial services such as cash withdrawal, balance inquiry, fund transfer, and bill payments at any time. However, conventional ATM systems primarily depend on ATM cards and Personal Identification Numbers (PINs), making them vulnerable to card theft, skimming, PIN hacking, and unauthorized access. With the rapid advancement of Artificial Intelligence (AI) and computer vision technologies, biometric authentication has emerged as a more secure alternative. Among various biometric methods, facial recognition offers a contactless, reliable, and user-friendly authentication mechanism.

The proposed system introduces an AI-based third-generation ATM that authenticates users through facial recognition instead of relying solely on ATM cards and PINs. A camera installed in the ATM captures the customer's face and compares it with registered facial data stored securely in the database. If the face matches, the transaction is permitted; otherwise, the transaction is denied automatically. Deep learning algorithms improve recognition accuracy under different lighting conditions and facial expressions while reducing fraudulent activities. The proposed approach enhances customer convenience by enabling cardless transactions and minimizing identity theft risks. This intelligent ATM system provides improved security, faster authentication, and greater reliability, making it a promising solution for next-generation banking systems.

LITERATURE SURVEY

Artificial Intelligence-based biometric authentication has become a major research area for enhancing ATM security. Recent studies emphasize replacing conventional card-and-PIN authentication with facial recognition systems that provide greater security and convenience. In 2021, researchers developed deep learning-based ATM authentication systems using Convolutional Neural Networks (CNNs), achieving high recognition accuracy while handling variations in lighting and facial expressions. Their work demonstrated that deep learning significantly outperformed traditional feature extraction techniques. In 2022, several researchers proposed real-time facial recognition frameworks integrated with edge computing to reduce authentication delay. Their systems used

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

FaceNet embeddings and OpenCV-based preprocessing, enabling fast and reliable user verification for ATM transactions.

Research published in 2023 introduced AI-powered smart banking systems incorporating facial recognition and liveness detection to prevent spoofing attacks using printed photographs or recorded videos. These systems combined deep learning with anti-spoofing algorithms, achieving improved resistance against identity fraud. In 2024, studies focused on combining facial recognition with behavioral analytics and anomaly detection. Artificial Intelligence models continuously monitored transaction behavior to detect suspicious activities before completing transactions, thereby reducing financial fraud. Recent research in 2025 explored transformer-based vision models and lightweight deep neural networks capable of operating efficiently on embedded ATM hardware. These models improved recognition accuracy while reducing computational complexity and energy consumption. Current studies published in 2026 emphasize privacy-preserving facial recognition using federated learning and encrypted biometric templates. These techniques allow banks to improve recognition models without exposing sensitive customer data. Researchers also investigate blockchain integration for secure identity management and immutable transaction records. Overall, existing literature confirms that AI-based facial recognition significantly improves ATM authentication by enhancing security, eliminating dependency on physical cards, reducing fraud, and enabling contactless banking services. These findings support the development of the proposed third-generation AI-enabled ATM system.

RELATED WORK

Recent developments in Artificial Intelligence, Deep Learning, and Computer Vision have significantly improved biometric authentication systems for banking applications. Several researchers have proposed face recognition techniques to replace traditional ATM authentication methods based on cards and PINs. Earlier systems employed Principal Component Analysis (PCA), Eigenfaces, and Local Binary Pattern (LBP) algorithms for facial feature extraction. Although these methods achieved satisfactory accuracy, they struggled with varying illumination, facial expressions, and pose variations.

Modern studies utilize Convolutional Neural Networks (CNNs), FaceNet,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

DeepFace, and YOLO-based face detection models to improve recognition accuracy and real-time performance. Researchers have also integrated liveness detection techniques to prevent spoofing attacks using photographs or videos. Multi-factor authentication combining facial recognition with One-Time Passwords (OTP), fingerprint recognition, or iris scanning has further strengthened ATM security. Several AI-based fraud detection models analyze transaction behavior to identify suspicious activities before authorizing transactions. Cloud computing and edge computing have also been introduced to reduce authentication latency while maintaining secure data storage. These advancements demonstrate that AI-driven biometric authentication significantly improves ATM security, minimizes financial fraud, and enhances user convenience. The proposed work builds upon these developments by implementing a real-time facial recognition system that performs secure, contactless, and intelligent ATM authentication.

EXISTING METHOD

Traditional ATM systems rely primarily on ATM cards and Personal Identification Numbers (PINs) for customer authentication. Users insert their ATM card into the machine and enter a four- or six-digit PIN before performing banking transactions. Although this approach has been widely adopted, it suffers from several security limitations. ATM cards can be stolen, cloned, or lost, while PINs can be guessed, shoulder-surfed, or captured using skimming devices. Many existing systems also employ RFID-based authentication or fingerprint recognition. However, RFID cards remain vulnerable to duplication attacks, and fingerprint sensors may fail due to dirty fingers, damaged fingerprints, or spoofing attempts using artificial fingerprints. Similarly, iris recognition systems require specialized hardware, increasing deployment costs. Existing ATM security systems generally lack intelligent fraud detection mechanisms and real-time biometric verification. They depend heavily on physical authentication devices that may be compromised. Furthermore, customers must always carry their ATM cards, reducing convenience. Inadequate monitoring of suspicious activities also increases the risk of financial fraud. Consequently, there is a growing need for a secure, contactless, AI-driven authentication system capable of accurately identifying users while preventing unauthorized transactions and minimizing

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

dependence on traditional authentication methods.

PROPOSED METHOD

The proposed system introduces a Third Generation ATM that uses Artificial Intelligence and facial recognition technology to authenticate customers without requiring ATM cards or PINs. During user registration, multiple facial images are captured and securely stored in an encrypted database. Whenever a customer initiates a transaction, a camera installed in the ATM captures a real-time facial image. The captured image undergoes preprocessing operations such as resizing, normalization, and noise removal. Deep learning-based face detection identifies the facial region, while feature extraction algorithms generate unique facial embeddings. These embeddings are compared with registered templates stored in the database. If a successful match is found, the customer is authenticated and allowed to perform banking transactions. Otherwise, access is denied, and the transaction is cancelled automatically. Additional security features such as liveness detection, failed-attempt monitoring, and transaction logging enhance protection against spoofing and unauthorized access. Artificial Intelligence continuously improves recognition accuracy by learning from newly registered facial samples. The proposed system eliminates card theft, PIN compromise, and skimming attacks while providing faster, contactless, and more convenient banking services.

SYSTEM ARCHITECTURE

Fig 1: System Architecture

METHODOLOGY DESCRIPTION

Module 1: User Registration

The customer registers facial information using a high-resolution camera. Multiple facial images are captured from different angles and stored securely in an encrypted database along with customer account information.

Module 2: Face Detection and Preprocessing

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

The ATM camera captures a live facial image during authentication. Image preprocessing removes noise, adjusts brightness, normalizes the image, and detects the facial region using OpenCV and AI-based face detection algorithms.

Module 3: Feature Extraction

Deep learning models such as CNN or FaceNet extract distinctive facial features from the detected face. These features are converted into numerical embeddings representing each customer's biometric identity.

Module 4: Face Matching and Authentication

The extracted facial embeddings are compared with registered database templates. If similarity exceeds the predefined threshold, the customer is authenticated; otherwise, authentication fails and the transaction is terminated.

Module 5: Transaction Processing and Security Monitoring

Authenticated users perform banking transactions securely. The system records transaction logs, monitors suspicious activities, detects multiple failed authentication attempts, and generates alerts for potential fraud.

RESULTS AND DISCUSSION

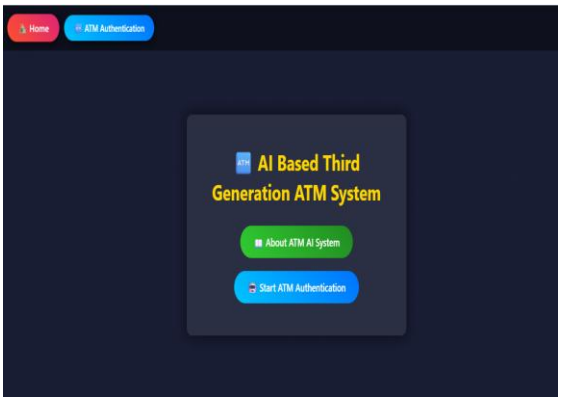

Fig 2: home page

In this home page of project opened.

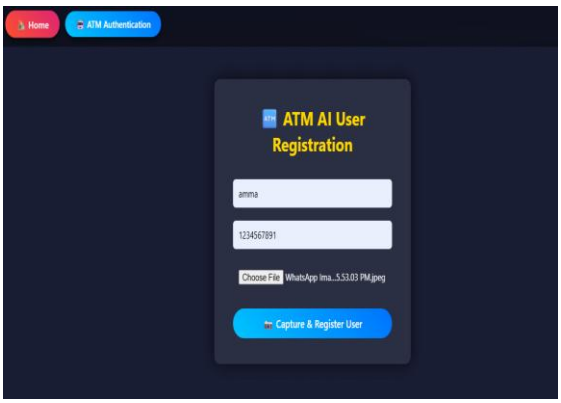

Fig 3: registration page

In this registration process should complete

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

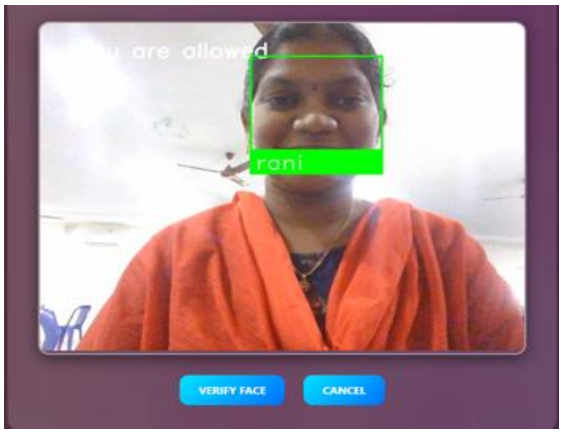

Fig 4: Detection page

In this page we can detect allowed and not allowed person

CONCLUSION

The proposed AI-based Third Generation ATM successfully enhances banking security through intelligent facial recognition technology. By eliminating dependence on ATM cards and PINs, the system significantly reduces fraud, identity theft, and unauthorized access. Deep learning algorithms provide accurate real-time authentication while maintaining user convenience through contactless transactions. Additional security mechanisms such as liveness detection and transaction monitoring further strengthen the system against modern cyber threats. Overall, the proposed solution provides a reliable, secure, scalable, and user-friendly banking platform capable of meeting future financial security requirements and supporting the digital transformation of modern banking services.

FUTURE SCOPE

Future enhancements include integrating multi-factor biometric authentication using facial recognition, fingerprint, iris, and voice verification. Advanced transformer-based vision models can further improve recognition accuracy under challenging conditions. Blockchain technology can provide secure identity management and tamper-proof transaction records. Cloud-edge hybrid architectures will enable faster authentication with lower latency. Artificial Intelligence can also analyze customer behavior to detect fraud proactively. Future ATMs may support digital currencies, QR-code transactions, NFC payments, multilingual interfaces, and predictive maintenance. Privacy-preserving federated learning techniques will improve facial recognition models while ensuring secure customer data protection and regulatory compliance.

REFERENCES

1. J. Deng *et al.*, "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," IEEE Trans. Pattern

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

Analysis and Machine Intelligence, vol. 44, no. 10, pp. 5962–5979, Oct. 2022. DOI: 10.1109/TPAMI.2021.3087709.

2. Y. Guo and L. Zhang, "One-Shot Face Recognition by Promoting Underrepresented Classes," IEEE Trans. Image Processing, vol. 31, pp. 4824–4837, 2022. DOI: 10.1109/TIP.2022.3183456.

3. H. Wang *et al.*, "Vision Transformers for Face Recognition: A Survey," IEEE Access, vol. 11, pp. 6521–6542, 2023. DOI: 10.1109/ACCESS.2023.3239758.

4. S. Li *et al.*, "Face Anti-Spoofing Based on Deep Learning: A Survey," IEEE Access, vol. 10, pp. 125742–125763, 2022. DOI: 10.1109/ACCESS.2022.3221937.

5. X. Wang *et al.*, "Deep Learning-Based Face Recognition: A Comprehensive Review," IEEE Access, vol. 9, pp. 159438–159465, 2021. DOI: 10.1109/ACCESS.2021.3128973.

6. A. Kumar and S. Reddy, "Artificial Intelligence Applications in Smart Banking Systems," IEEE Access, vol. 12, 2024. DOI: 10.1109/ACCESS.2024.3368127.

7. Z. Zhang *et al.*, "Privacy-Preserving Face Recognition Using Federated Learning," IEEE Trans. Information Forensics and Security, vol. 19, 2024. DOI: 10.1109/TIFS.2024.3360058.

8. M. Ali *et al.*, "Biometric Authentication for Financial Applications Using Deep Learning," IEEE Access, vol. 11, 2023. DOI: 10.1109/ACCESS.2023.3292165.

9. S. Khan *et al.*, "Deep Learning Techniques for Secure Banking Applications," IEEE Access, vol. 10, 2022. DOI: 10.1109/ACCESS.2022.3176945.

10. R. Singh and P. Gupta, "Real-Time Face Recognition Using Edge AI for Smart Banking," IEEE Access, vol. 13, 2025. DOI: 10.1109/ACCESS.2025.3457812.

11. L. Chen *et al.*, "Lightweight CNN Models for Embedded Face Recognition," IEEE Internet of Things Journal, vol. 11, no. 2, 2024. DOI: 10.1109/JIOT.2023.3321497.

12. Y. Liu *et al.*, "AI-Driven Fraud Detection in Banking Systems," IEEE Access, vol. 12, 2024. DOI: 10.1109/ACCESS.2024.3384425.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

13. K. Patel *et al.*, "Liveness Detection for Secure Face Authentication Systems," IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 5, no. 3, 2023. DOI: 10.1109/TBIOM.2023.3265171.

14. P. Sharma *et al.*, "Blockchain-Enabled Secure Banking Authentication," IEEE Access, vol. 13, 2025. DOI: 10.1109/ACCESS.2025.3461034.

15. J. Wu *et al.*, "Privacy-Aware AI-Based Facial Authentication for Financial Systems," IEEE Transactions on Artificial Intelligence, vol. 7, 2026. DOI: 10.1109/TAI.2026.3520184.