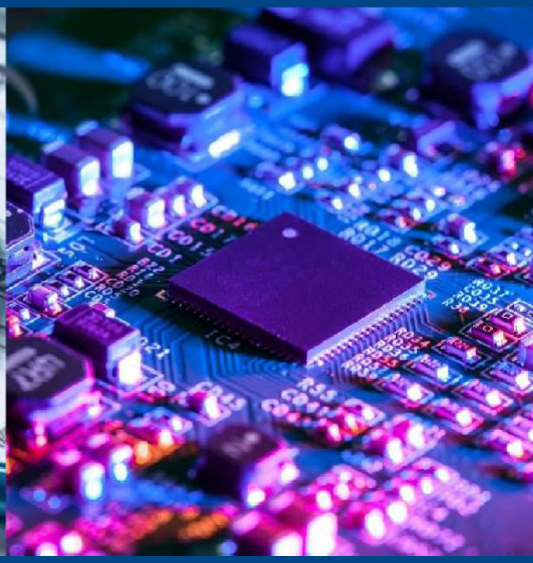
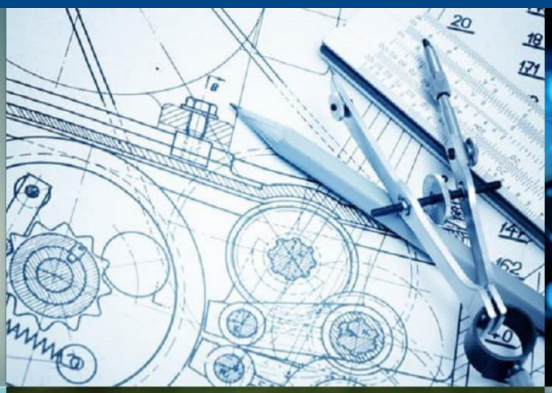
ISSN: 2582-7219

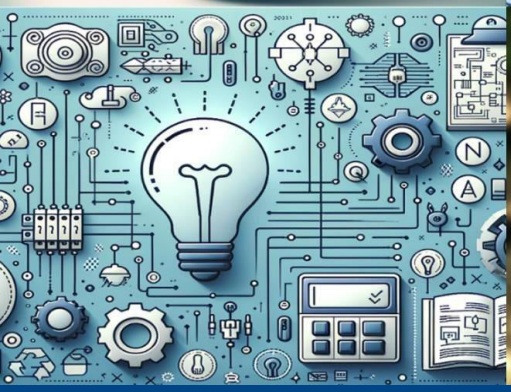




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 8, Issue 7, July 2025**

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807050

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Securing ATM Transactions with Facial Recognition Based Verification Systems

K. Nivetha[1], Ms. C. Vaneesa[2]

PG Scholar, Department of Master of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India[2]

ABSTRACT: Automated Teller Machines (ATMs) have become an essential component of daily financial operations across the globe. However, the increasing dependence on ATM services has led to a surge in security vulnerabilities, with debit card fraud accounting for approximately 270,000 cases of identity theft in 2021. To address these concerns, this paper proposes a secure ATM transaction model utilizing facial recognition-based biometric verification, supported by advanced deep learning techniques. The proposed system integrates a Convolutional Neural Network (CNN) to train a FaceNet model during account creation, and employs a Temporal Convolutional Network (TCN) at the time of transaction to authenticate users by comparing live ATM camera input with stored face data. This dual-model framework ensures accurate, real-time verification while enhancing user experience and transaction security. In the event of unauthorized access attempts, the system triggers a verification protocol wherein a facial confirmation link is dispatched to the registered user for immediate identity verification via artificial intelligence agents. This approach mitigates the risks associated with ATM card theft and duplication, thereby ensuring that only the legitimate account holder can perform transactions. The system demonstrates significant potential in elevating the safety and reliability of ATM operations. The model is designed with scalability and efficiency in mind, offering high accuracy across different lighting conditions, facial angles, and user movements. Furthermore, by eliminating the dependence on physical cards, the system reduces operational costs and enhances user convenience. Experimental results demonstrate the effectiveness of the hybrid CNN-TCN model in achieving secure, contactless, and user-specific ATM interactions. This facial biometric-based ATM framework significantly advances the state-of-the-art in transaction security, paving the way for intelligent, fraud-resistant banking systems.

I. INTRODUCTION

In the evolving landscape of digital banking, Automated Teller Machines (ATMs) continue to serve as a critical channel for financial transactions. Their widespread deployment offers customers 24/7 access to cash withdrawals, balance inquiries, and other essential banking services. However, the increasing reliance on ATMs has also exposed significant vulnerabilities in conventional authentication mechanisms. The most used methods—such as magnetic stripe cards combined with Personal Identification Numbers (PINs)—have become increasingly prone to security breaches. Card skimming, duplication, shoulder surfing, and stolen credentials are among the most frequently reported forms of ATM-related fraud. These growing threats necessitate a shift toward more secure, i and mobile technologies. Biometric authentication methods, including fingerprint and iris recognition, offer enhanced security by verifying ntelligent, and user-centric authentication systems. Biometric technologies, particularly Facial Recognition Technology (FRT), have emerged as promising alternatives. Unlike passwords or cards that can be forgotten, lost, or stolen, a person's face provides a unique and permanent identifier. Facial recognition systems offer a non-intrusive, contactless, and real-time method of identity verification, making them highly suitable for ATM environments. This research proposes the development of an ATM security model that incorporates facial recognition powered by Convolutional Neural Networks (CNN). The proposed system captures the user's facial features at the point of access and compares them with pre-registered templates for authentication. In the case of a mismatch or an unknown face, an "Unknown Face Forwarder" module is triggered, initiating an additional verification layer to prevent unauthorized access.

Furthermore, real-time alert notifications are generated and sent to the account holder's registered mobile number or email, thereby enhancing awareness and control over transaction activity. By integrating artificial intelligence with traditional ATM infrastructure, this study aims to significantly strengthen transaction security while enhancing

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

customer trust. The model not only addresses current limitations in ATM authentication but also lays the foundation for future enhancements in biometric-driven financial technologies.

II. EXISTING SYSTEM

Current ATM authentication systems predominantly rely on traditional security mechanisms such as card-based access and Personal Identification Number (PIN) entry. In this widely adopted approach, users insert their ATM card into the machine's reader and input their PIN, which is then matched with the data stored on the card's magnetic stripe or chip. Despite its ubiquity, this method remains vulnerable to various forms of identity theft and unauthorized access. To address these limitations, though their adoption is still limited. Two-Factor Authentication (2FA) has also been implemented in certain banking environments requirmg users to provide both a PIN and a One-Time Password (OTP) sent to a registered mobile device, thereby improving access control. Furthermore, Near Field Communication (NFC) technology enables contactless authentication through NFC-enabled cards or mobile wallets, minimizing the physical handling of ATM cards. Mobile-based authentication methods have emerged as well, allowing users to scan QR codes displayed on ATM screens and authorize transactions through secure banking applications. Additionally, tokenbased authentication systems, which rely on physical or virtual devices to generate OTPs, are used to supplement PIN-based access. While these systems have introduced convenience and multiple verification methods, they remain constrained by several technical and usability limitations.

III. PROPOSED SYSTEM

The proposed ATM User Face Identification system introduces an enhanced biometric authentication layer by integrating facial recognition technology into the existing ATM infrastructure. At the core of the system is a Convolutional Neural Network (CNN) that captures and analyzes facial features during each transaction. The captured facial data is compared against a securely stored facial database to verify user identity. In instances where a user's face is not recognized, an "Unknown Face Verification System" is triggered, which generates and sends a secure Face Verification Link to the user's registered mobile number. This secondary verification process ensures that only authorized individuals can proceed with the transaction.

IV. SYSTEM ARCHITECTURE

The proposed system architecture integrates facial recognition technology into the ATM transaction workflow to ensure secure and user-specific authentication. The architecture is composed of multiple interconnected modules designed to function seamlessly in real time, enhancing both usability and security. The core components of the system include the Face Capture Module, Feature Extraction Engine, Facial Recognition Model, Authentication Unit, and Notification Module.

During the account creation phase, the Face Capture Module utilizes a Convolutional Neural Network (CNN) to capture highresolution facial images of the user. These images are processed by the Feature Extraction Engine, which employs the FaceNet algorithm to generate unique facial embeddings that are securely stored in the bank's database. At the time of a transaction, the ATM camera captures the user's current facial image, and the system compares the extracted features against the pre-stored embeddings using a Temporal Convolutional Network (TCN). This dualmodel approach ensures robust verification under varying lighting conditions, facial angles, and user movement. If the face is recognized with high confidence, the user is granted access to banking services. In the event of a mismatch or an unrecognized face the system triggers the Unknown Face Forwarder, which sends a secure facial verification link to the registered mobile number of the account holder. This additional verification layer prevents unauthorized access and enhances system trustworthiness.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807050

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

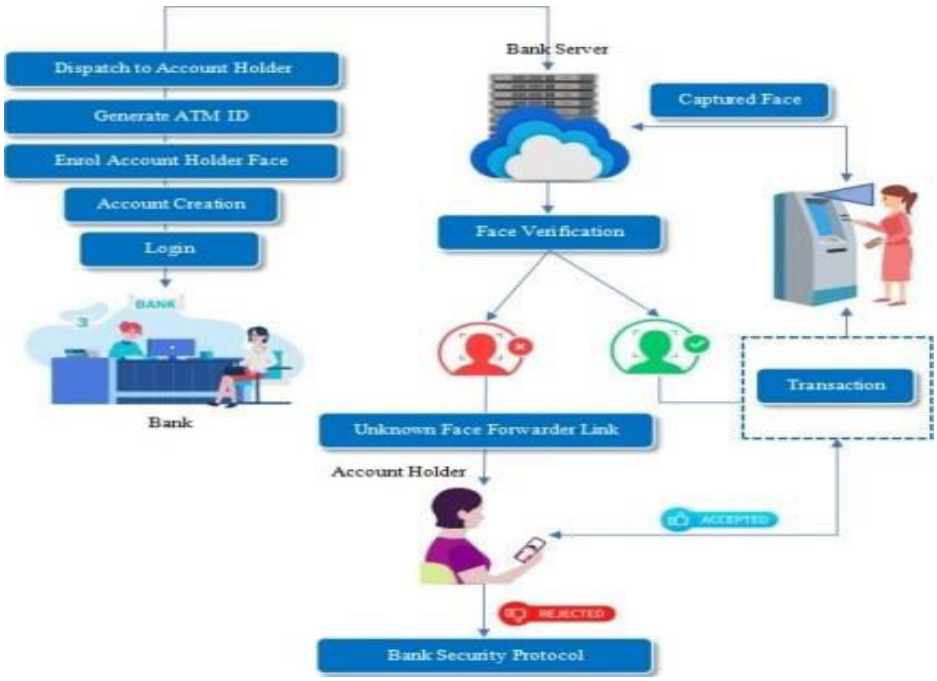


Fig 4.1 Architectural Diagram

Simultaneously, the Notification Module dispatches real-time alerts via SMS, email, or mobile application, keeping the user informed of all access attempts. The architecture supports modular integration with existing ATM systems, ensuring minimal disruption during deployment. Overall, the architecture leverages machine learning, biometric authentication, and realtime communication to establish a secure, intelligent, and user-centric ATM environment.

V. RESULTS

The proposed system, titled "Securing ATM Transactions with Facial Recognition-Based Verification Systems, " was thoroughly tested to evaluate its accuracy, robustness, performance, and security under real-time conditions. The system demonstrated its ability to accurately identify legitimate users through CNN-based facial recognition while effectively denying access to unregistered or fraudulent individuals.

Fig 5.1 login screen

The system architecture supports a multi-step process, beginning with a user interface for initiating a transaction, followed by live face capture using an integrated camera. Captured Images are processed in real time, and features are compared with stored FaceNet embeddings. If a mismatch occurs, the "Unknown Face Forwarder" module is triggered, which sends a secure facial verification link to the account holder's registered mobile number. This secondary

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

verification step proved effective in preventing unauthorized access, even when attempts were made using similar facial features or under altered appearances.

Fig 5.2 face capture screen

Testing was conducted under varying lighting conditions, facial orientations, and expressions. The CNN model maintained high accuracy in detecting and matching faces, validating the robustness of the system. In addition to recognition accuracy, the system's responsiveness was evaluated by simulating multiple concurrent requests. Results showed consistently low latency and reliable performance, indicating the system's readiness for real-world deployment.

Fig 5.3 Information screen

The integration of the Temporal Convolutional Network (TCN) further enhanced verification speed during transaction time. Real-time alert features, including SMS and app notifications, ensured users were Immediately informed of access attempts. Furthermore, secure data handling and log management via a MySQL backend contributed to system integrity and traceability.

Fig 5.4 verification screen

The system maintained a smooth user experience for authorized users while actively flagging and containing unauthorized interactions. Overall, the test outcomes confirmed that the proposed solution successfully enhances ATM transaction security through intelligent facial authentication, real-time communication, and secondary verification measures, all while maintaining operational efficiency and user convenience.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

VI. CONCLUSION

In the modern age of digital banking and rural development, ensuring security in agricultural farm transactions is becoming increasingly important. One of the most vulnerable areas remains Automated Teller Machines (ATMs), where fraudulent activities and unauthorized access continue to pose significant risks. To address this, the integration of biometric authentication systems offers a highly effective solution. This project proposes a secure ATM model that leverages biometric facial recognition along with an "Unknown Face Forwarder" mechanism to prevent fraudulent transactions, even when the account holder is either physically present or remotely located. By enforcing the use of a biometric feature— specifically facial recognition—for user identification, the system ensures that only the legitimate account owner can access banking services. The security is further strengthened through a layered authentication process that complements conventional tools such as ATM cards and PINs. This hybrid model integrates physical and biometric verification techniques, reducing the possibility of proxy access or card theft. The system also introduces a realtime communication framework that involves the account holder directly in every transaction attempt, through immediate notifications and facial verification links. This approach not only enhances security but also empowers users with full control over their accounts, especially in sensitive environments such as rural or agricultural financial operations.

VII. FUTURE ENHANCEMENTS

Several potential enhancements can be incorporated into the Real-Time Secure Clickbait and Face Biometric ATM User Authentication and Multiple Bank Transaction System to further improve its security, accessibility, and functionality. One significant advancement would be the integration of multi-factor authentication, combining facial recognition with additional authentication layers such as fingerprint scanning or password input to reinforce system security. Furthermore, the implementation of real-time alert notifications to bank administrators or security personnel during suspicious activity or attempted breaches could improve system responsiveness and threat mitigation. Another notable improvement would be the integration of the authentication system with mobile banking platforms, enabling users to manage transactions and account-related tasks through their mobile devices, enhancing both convenience and control. To increase accessibility for a diverse user base, the system could also be extended to support multiple languages, ensuring ease of use for individuals not fluent in the default system language. Additionally, expanding the system's capabilities to handle a broader range of banking operations—such as fund transfers, utility bill payments, and mini statements—would provide a more comprehensive and user-friendly banking experience. These future developments would collectively contribute to a highly secure, adaptable, and user-centric ATM ecosystem, aligning with evolving financial technologies and user expectations.

REFERENCES

1. J. Liang, H. Zhao, X. Li, and H. Zhao, "Face recognition system based on deep residual network," in Proc. 3rd Workshop Adv. Res. Technol. Ind. (WARTIA), Nov. 2017, p. 5.
2. I. Taleb, M. E. Amine Oeis, and M. O. Mamar, "Access control using automated face recognition: Based on the PCA & LDA algorithms," in Proc. 4th Int. Symp. ISKOMaghreb, Concepts Tools Knowl. Manage. (1SKO-Maghreb), Nov. 2014, pp. 1-5.
3. X. Pan, "Research and implementation of access control system based on RFID and FNN-face recognition," in Proc. 2nd Int.
4. Conf! Intell. Syst. Design Eng. Appl., Jan. 2012, 716-719, doi: 10.1109/1Sdea.2012.400.
5. A. A. Wazwaz, A. O. Herawi, M. J. Teti, and S. Y. Hemed, "Raspberry Pi and computers-based face detection and recognition system," in Proc. 4th Int. Conf. Compute. Technol. Appl. (ICCTA), May 2018, pp. 171-174.
6. A. Had, S. Bentura, M. Kedir-Talha, F. Abtahi, M. Attari, and F. Seoane, "Full impedance cardiography measurement device using Raspberry P13 and system-onchip biomedical instrumentation solutions," IEEE J. Biomed. Health Informant., vol. 22, no. 6, pp. 1883-1894, Nov. 2018.
7. A. Li, S. Shan, and W. Gao, "Coupled bias-variance tradeoff for cross-pose face recognition," IEEE Trans. Image Process. , vol. 21, no. l, pp. 305—315, Jan. 2012.
8. C. Ding, C. Xu, and D. Tao, "Multi-task pose-invariant face recognition," IEEE Trans. Image Process. , vol. 24, no. 3, pp. 980—993, Mar. 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com