IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Preventing Theft In ATM Banking With AI And Blockchain

*S.UMA,
Assistant Professor,
Department of Computer science and
Engineering Paavai Engineering College,
Pachal, Namakkal.
J.NAJLA FARVEEN, S.DHANALAKSHMI,
B.BOOMATHI.
Final Year, Department of Computer Science and Engineering, Paavai Engineering College, Pachal, Namakkal.

Abstract: ATM banking is increasingly vulnerable to financial fraud, posing serious risks to users and institutions. Traditional detection systems often lack real-time capabilities, necessitating more advanced solutions. This project presents a security framework that combines Artificial Intelligence (AI) and Blockchain technology to effectively prevent ATM fraud. AI is used to analyze transactions and detect anomalies using multi-factor authentication, including illusion PINs, facial recognition, and a reverse OTP system. Meanwhile, Blockchain ensures secure, transparent, and immutable transaction records, preventing unauthorized alterations. The integration of deep learning enables accurate behavioral analysis, reducing false positives and enabling real-time fraud identification. Blockchain's decentralized ledger further enhances security and data integrity. Experimental results show that the AI-driven system significantly improves fraud detection accuracy, while blockchain guarantees robust protection of transaction data. This approach demonstrates the powerful synergy between AI and Blockchain, offering a scalable, efficient, and secure method for safeguarding ATM banking against fraud.

Keywords: Deep Learning for Transaction Monitoring; Secure ATM Systems; Decentralized Ledger Technology; Multi-Factor Authentication.

1. INTRODUCTION

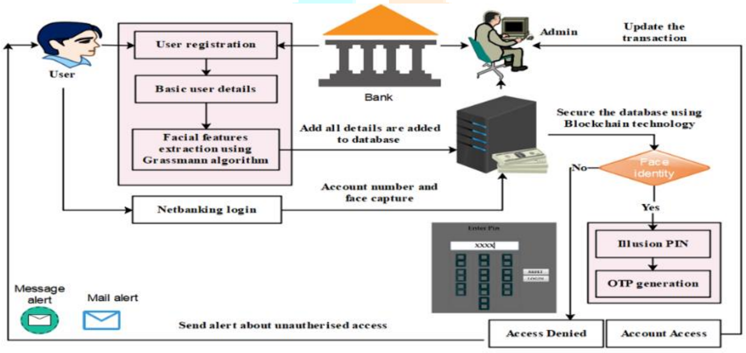
Authentication plays a vital role in safeguarding computer-based systems by ensuring that only authorized users gain access. In digital environments, especially in online banking, preventing unauthorized access is critical, as a successful login by a malicious user grants complete access to sensitive user data and services. Traditional methods such as passwords and PINs are increasingly vulnerable to attacks like phishing, keylogging, or brute-force methods. To enhance security and mitigate the risks associated with unauthorized access, this system introduces a face recognition-based authentication approach as a more secure and user-friendly alternative. Facial recognition leverages advanced computer vision and machine learning algorithms to identify and authenticate users based on their unique facial features. It is particularly effective in preventing impersonation and unauthorized logins, offering a high level of accuracy and convenience. With the rise of AI-powered biometric systems, face recognition can be seamlessly integrated into mobile and web platforms, making the authentication process more robust. To further strengthen the integrity and security of sensitive data, this system incorporates blockchain technology for storage and verification. Blockchain, being a decentralized and tamper-resistant ledger, ensures that transaction records and authentication logs remain immutable and transparent. This dual-layered security framework—combining facial recognition and blockchain—significantly reduces the chances of fraud and data breaches in online banking platforms. By integrating these advanced technologies, the system not only enhances user trust but also provides a scalable, secure, and future-ready solution for protecting digital financial services against evolving cyber threats.

2. OBJECTIVES

This work aims to develop an AI-powered system designed to detect and identify fraudulent activities in ATM operations in real time. By utilizing facial recognition and intelligent analysis, the system ensures that only authorized users can access services. To further enhance security, blockchain technology is integrated to store and verify transaction data. Blockchain's decentralized and tamper-proof nature guarantees data transparency and prevents unauthorized alterations. Together, these technologies create a robust framework that enhances the integrity and reliability of financial transactions, significantly reducing the risk of fraud and increasing user trust in modern ATM banking systems.

3. METHODOLOGY

The proposed system integrates advanced Artificial Intelligence (AI) techniques and Blockchain technology to provide a multi-layered, secure authentication framework for ATM banking. The methodology is designed to ensure both the accurate identification of users and the secure recording of transaction data, thus significantly reducing fraudulent activity.


User
User registration
Basic user details
Facial features extraction using Grassmann algorithm
Bank
Admin
Update the transaction
Add all details are added to database
Secure the database using Blockchain technology
Face identity
No
Yes
Account number and face capture
Netbanking login
Illusion PIN
OTP generation
Message alert
Mail alert
Send alert about unautherised access
Access Denied
Account Access

3.1 Facial Recognition and Authentication

The first layer of authentication leverages face biometric technology. During registration, the user's facial features are captured using a high-resolution camera. These images are preprocessed through normalization and geometric transformation techniques. Facial landmarks such as eyes, nose, and mouth are identified using algorithms like OpenCV or Dlib.

A feature vector is then generated using deep learning models that extract distinguishing characteristics from each facial region. These vectors are mapped into a subspace using the Grassmannian manifold approach to improve matching accuracy. For verification during ATM usage, the system compares the real-time input image against the stored facial features using distance metrics like geodesic distance and canonical correlation.

3.2 Illusion PIN-Based Verification

To further enhance authentication, the system employs an illusion-based PIN method. Unlike traditional numeric PINs, this technique randomizes visual inputs, making it resistant to shoulder-surfing and screen recording attacks. This method provides an additional security layer before granting ATM access.

3.3 Blockchain-Based Transaction Validation

The second phase of the system focuses on transaction-level security. Once a transaction is initiated, its details are hashed using SHA-256 encryption and broadcasted to a decentralized blockchain network. The consensus mechanism—either proof-of-work or proof-of-stake—is applied to validate the transaction. After verification, the transaction data is added as a new block containing the timestamp, previous hash, and digital signatures.

This decentralized ledger prevents data manipulation, ensuring transaction transparency and integrity.

3.4 Module Integration

The complete system consists of modules for user registration, PIN verification, facial image validation, transaction execution, and blockchain storage. This modular architecture allows scalability, flexibility, and robust performance in real-world ATM environments.

4. ALGORITHMS USED

The proposed system uses a combination of artificial intelligence techniques and blockchain cryptographic methods to ensure secure ATM banking transactions. The algorithms are divided into two major functional domains: facial recognition and blockchain transaction validation.

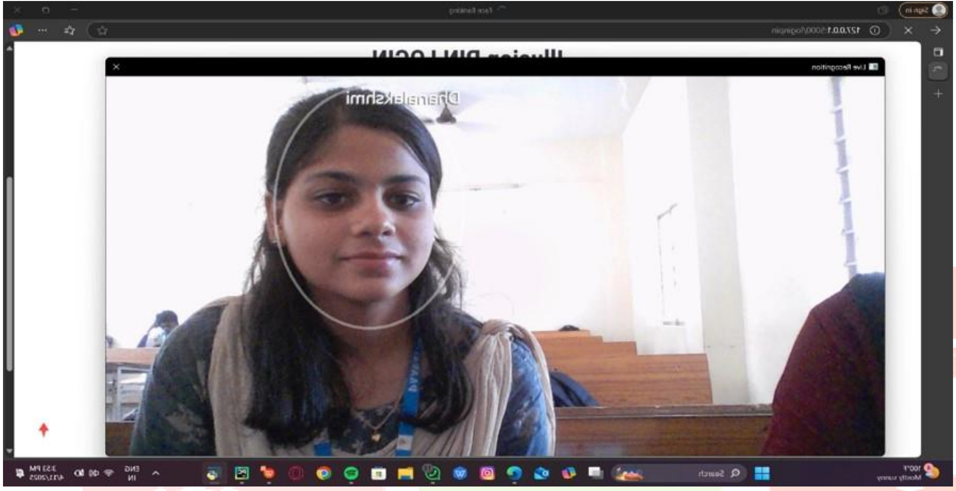
4.1 Facial Recognition Algorithm

The system initiates face recognition by capturing a live image of the user through the ATM's camera. A face detection algorithm isolates the facial region using affine transformations to normalize the coordinates. Once the face is detected, feature extraction is performed to obtain key attributes such as eye spacing, nose shape, and jawline structure. These features are mapped to a subspace using Grassmannian manifold learning, which allows for efficient classification in lower dimensions.

To determine identity, the extracted feature vector is compared with stored vectors using projection-based distance metrics such as Geodesic Distance and Canonical Correlation. This step ensures only the registered user can gain access, minimizing the risk of impersonation or spoofing.

4.2 PIN Verification Algorithm

To complement facial recognition, an Illusion PIN verification algorithm is used. This method introduces a dynamic and randomized keypad layout, which prevents shoulder-surfing and visual skimming. The user must input their PIN based on shifting visual clues, making it highly resistant to traditional observation attacks.



4.3 Blockchain Transaction Algorithm

After successful user authentication, transaction details are processed through a cryptographic hashing algorithm (SHA-256). The hashed data is then broadcasted across a blockchain network where nodes validate it using a consensus mechanism, such as Proof-of-Work (PoW) or Proof-of-Stake (PoS). Once verified, the transaction is recorded in a block that includes timestamps, digital signatures, and a hash of the previous block, ensuring the immutability and traceability of financial data.This integrated algorithmic approach fortifies ATM systems against both digital and physical security threats.

5.IMPLEMENTATION AND DEVELOPMENT

The implementation of the proposed ATM fraud prevention system involves the integration of facial biometric verification and blockchain-based transaction recording within a secure and modular framework. The development focuses on real-time authentication, accuracy, and data integrity.

5.1 System Design

The system is structured into distinct modules: user registration, PIN verification, face image verification, online transaction processing, and blockchain storage. During registration, users create a personal PIN and provide a facial image. The facial data is processed using feature extraction techniques to generate a unique identity vector, which is stored securely in a database.

5.2 Development Tools

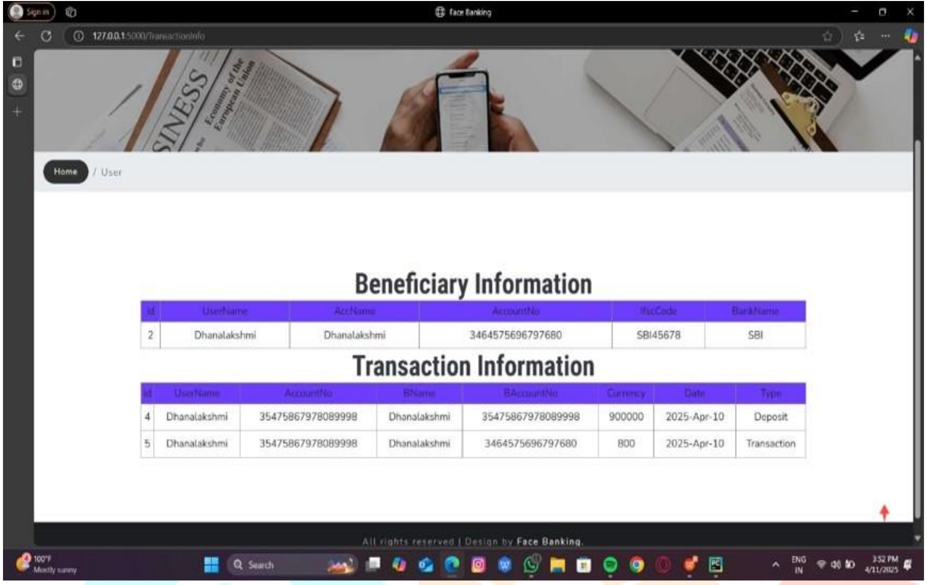
The application is developed using Python 3.7.4, with PyCharm as the integrated development environment. The user interface is built with Tkinter for client-side interaction. OpenCV is used for capturing and processing facial images, and facial recognition algorithms are trained using machine learning techniques. The system runs on Windows 10 (64-bit) and requires hardware specifications including an Intel processor (2.6 GHz), 4 GB RAM, a standard keyboard, a 15-inch monitor, and a webcam.

5.3 PIN and Face Verification

Upon system login, the user first verifies identity through an Illusion PIN technique, where digits are randomized to prevent visual tracking. This is followed by facial recognition. The live face image is compared against stored records using subspace mapping and Grassmannian learning models. Only if both layers pass validation is the user granted transaction access.

5.4 Blockchain Integration

Transaction details are hashed and broadcasted across a blockchain network. Consensus mechanisms like Proof-of-Work or Proof-of-Stake validate these entries. The verified transactions are then immutably stored in blocks containing timestamps, hash references, and digital signatures. This dual-layer system ensures both authentication robustness and the immutability of sensitive transaction data, offering a scalable solution for secure ATM banking.



Beneficiary Information

id	UserName	AccName	AccountNo	IfscCode	BankName
2	Dhanalakshmi	Dhanalakshmi	3464575696797680	SBI45678	SBI

Transaction Information

id	UserName	AccountNo	BName	BAccountNo	Currency	Date	Type
4	Dhanalakshmi	35475867978089998	Dhanalakshmi	35475867978089998	900000	2025-Apr-10	Deposit
5	Dhanalakshmi	35475867978089998	Dhanalakshmi	3464575696797680	800	2025-Apr-10	Transaction

6. CONCLUSION

This study introduces a hybrid security model for ATM banking that combines artificial intelligence-driven facial recognition with blockchain technology to combat fraud and unauthorized access. Traditional PIN-based systems are increasingly susceptible to threats such as shoulder-surfing and data breaches. The integration of an illusion-based PIN method with face biometric authentication creates a dual-layer security mechanism, enhancing both usability and resistance to common attack vectors.

The system’s face recognition module captures and verifies user identity using advanced feature extraction and subspace mapping techniques, ensuring accurate and real-time authentication. This prevents unauthorized users from accessing ATM services even if they obtain a user's PIN.

On the other hand, blockchain technology ensures the security and immutability of transaction records. Each transaction is encrypted, validated via a consensus mechanism, and stored as a tamper-proof entry in a decentralized ledger.

By combining these technologies, the proposed system offers a scalable and secure solution for modern banking environments. It provides not only strong user authentication but also ensures transaction integrity, ultimately promoting trust and resilience in digital financial systems. Future enhancements may include support for mobile-based transactions, lighter AI models, and extended biometric modalities for broader applicability.

7.REFERENCE

- Khan, Habib Ullah, et al. "Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis." Ieee Access 11 (2023): 80181-80198.
- Karim, Nader Abdel, et al. "Online banking user authentication methods: a systematic literature review." Ieee Access 12 (2023): 741-757.
- Darem, Abdulbasit A., et al. "Cyber threats classifications and countermeasures in banking and financial sector." IEEe Access 11 (2023): 125138-125158.
- Sedik, Ahmed, et al. "Deep learning modalities for biometric alteration detection in 5G networks-based secure smart cities." IEEE Access 9 (2021): 94780-94788.
- Hajiabbasi, Milad, Ehsan Akhtarkavan, and Babak Majidi. "Cyber-physical customer management for internet of robotic things-enabled banking." Ieee Access 11 (2023): 34062-34079.
- Ahmed, Waqas, et al. "Security in next generation mobile payment systems: A comprehensive survey." IEEE Access 9 (2021): 115932-115950.

- Hashemi, Seyedeh Khadijeh, Seyedeh Leili Mirtaheri, and Sergio Greco. "Fraud detection in banking data by machine learning techniques." Ieee Access 11 (2022): 3034-3043.
- Yang, Wensi, et al. "Ffd: A federated learning based method for credit card fraud detection." Big data–bigData 2019: 8th international congress, held as part of the services conference federation, SCF 2019, san diego, CA, USA, June 25–30, 2019, proceedings 8. Springer International Publishing, 2019.
- Sadgali, Imane, Nawal Sael, and Faouzia Benabbou. "Fraud detection in credit card transaction using neural networks." Proceedings of the 4th international conference on smart city applications. 2019.
- Asha, R. B., and Suresh Kumar KR. "Credit card fraud detection using artificial neural network." Global Transitions Proceedings 2.1 (2021): 35-41.