Enhanced Net Banking Security Using Illusion PIN, Facial Biometrics, And Collaborative Transaction Approval

Jayasurya A[1], Janaranjan M[2], Rishikanth R[3], Aathin Prince K[4] , Dhivya Dharshini G[5],
[1, 2, 3, 4] Dept of Computer Science & Engineering
[5]Assist prof, Dept of Computer Science & Engineering
[1, 2, 3, 4, 5] CARE College of Engineering
Approved by AICTE | Affiliated to Anna University

Abstract- *This paper presents an enhanced Net Banking security framework designed to overcome the limitations of traditional authentication mechanisms such as passwords and PINs, which are increasingly vulnerable to cyber threats including phishing, shoulder surfing, and brute-force attacks. This system introduces a multi-layered authentication approach combining Illusion PIN techniques with real-time facial biometric verification. Blockchain technology ensures secure, transparent, and tamper-proof storage of transaction records. A Joint Account Multi-Party Authorization (MPA) module enables collaborative transaction approvals, requiring consent from multiple authorized users before executing sensitive operations. By integrating these technologies, the proposed system delivers a comprehensive, secure, and user-friendly Net Banking environment that minimizes fraud and ensures robust protection of financial data.*

I. INTRODUCTION

1.1 Project Overview

The rapid growth of digital banking has significantly increased convenience, but it has also introduced serious security concerns. Traditional authentication methods such as passwords and PINs are no longer sufficient to protect users from modern threats like phishing, brute-force attacks, shoulder surfing, and identity theft. The proposed system provides a secure multi-layered framework to address these challenges. Its architecture includes:

- **Frontend:** Web interface for user interaction and banking operations.
- **Backend:** Python-based application logic for authentication and transaction handling.
- **Database:** Secure local server for storing user profiles, transaction records, and biometric templates.
- **Blockchain Layer:** Decentralized ledger for tamper-proof record storage.
-

1.2 Problem Description

- **Credential Theft:** Passwords and PINs are vulnerable to phishing and brute-force attacks.
- **Shoulder Surfing:** Attackers visually observe PIN entry in public environments.
- **Weak Identity Verification:** Existing systems lack reliable biometric verification after login.
- **Joint Account Risk:** Single-user control over shared accounts increases fraud exposure.
- **Data Tampering:** Centralized records are susceptible to unauthorized modification.

II. LITERATURE SURVEY

Existing research highlights OTP-based authentication for ATM security (Bansal, 2025), real-time ATM monitoring using IoT (Thopate et al., 2023), and multi-modal biometric systems for banking (Monisha et al., 2024). Studies on facial recognition in mobile banking (Machap, 2023) and blockchain-based self-sovereign identity (Ahmed et al., 2023) reinforce the need for multi-layered approaches. This project integrates these insights into a unified, scalable security framework combining biometrics, Illusion PIN, and blockchain.

III. PROPOSED SYSTEM

3.1 System Architecture

The platform comprises four integrated layers:

- **User Layer:** Account holders and joint users interact via a secure web portal.
- **Authentication Layer:** Illusion PIN and facial biometric verification validate identity.
- **Application Layer:** Handles transaction processing, MPA workflows, and OTP validation.

- **Blockchain Layer:** Stores all transaction records in an immutable, decentralized ledger.

3.2 Key Features

- **Users:** Illusion PIN login, face verification, transaction initiation, and account management.
- **Joint Account Holders:** Multi-party approval for high-value or sensitive transactions.
- **Admins:** User management, audit trails, and system monitoring.

IV. METHODOLOGY

The system follows an iterative development approach:

- **Requirements Analysis:** Identified security gaps in traditional net banking systems.
- **Design:** Wireframing and prototyping for secure UI/UX flows including Illusion PIN interface.
- **Implementation:** Python backend with MySQL database and facial recognition SDK integration.
- **Testing:** Unit, integration, system, and user acceptance testing to ensure robustness and security.

Screenshots

Home Page / Login Screen
(Insert screenshot here)
Illusion PIN Entry Interface
(Insert screenshot here)
Face Verification Screen
(Insert screenshot here)
Joint Account MPA Approval
(Insert screenshot here)
Transaction History (Blockchain Log)
(Insert screenshot here)

V. DISCUSSION

Strengths

- Multi-layered authentication combining Illusion PIN and facial biometrics prevents common attack vectors.
- Blockchain ensures tamper-proof, transparent, and auditable transaction records.
- MPA module enforces collaborative control for joint accounts, reducing fraud risk.
- Reverse OTP verification adds an additional safeguard for transaction validation.

Limitations

- Facial recognition accuracy may be affected by poor lighting or camera quality.
- Blockchain transaction logging introduces slight latency in real-time operations.
- Current implementation is limited to web-based access without mobile app support.

Future Work

- Integration of additional biometrics such as fingerprint and iris recognition.
- AI-based anomaly detection for real-time fraud prevention.
- Mobile application development with secure API integration.
- Smart contract automation for MPA rules within the blockchain framework.
- Multi-language support and cloud-based scalable deployment.

VI. PERFORMANCE COMPARISON

AUTHENTICATION METHOD	SHOULDER SURFING RESISTANCE	BIOMETRIC VERIFICATION	TAMPER-PROOF RECORDS	MULTI-PARTY APPROVAL
Traditional PIN / Password	Low	No	No	No
OTP-Based System	Medium	No	No	No
Biometric Only	High	Yes	No	No
Proposed System	**Very High**	**Yes**	**Yes (Blockchain)**	**Yes (MPA)**

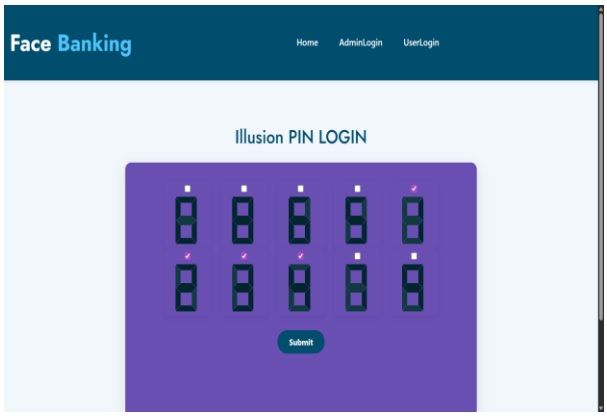
VII. CONCLUSION

The proposed Net Banking security system successfully addresses the limitations of traditional authentication mechanisms by introducing a multi-layered security framework. By combining Illusion PIN and real-time facial biometric verification, the system significantly enhances

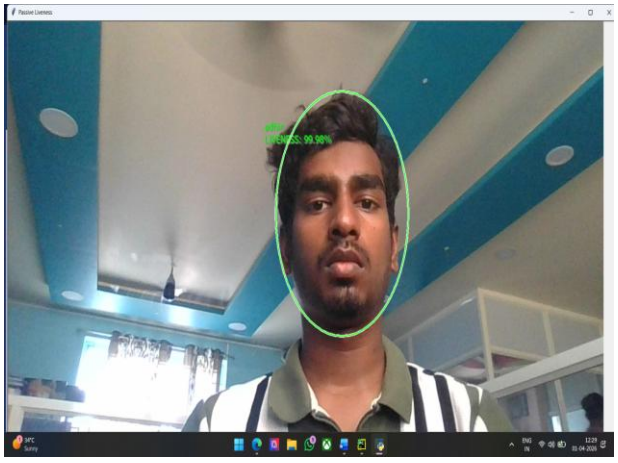
user authentication and protects against shoulder surfing, phishing, and brute-force attacks. The integration of blockchain technology ensures that all transaction records are stored in a decentralized and tamper-proof manner, guaranteeing data integrity and traceability. The inclusion of the Multi-Party Authorization (MPA) module further strengthens security for joint accounts by requiring multiple approvals for sensitive transactions. Overall, the system provides a comprehensive, secure, and user-friendly Net Banking environment that enhances trust and safety in digital financial transactions, demonstrating strong potential for real-world deployment in modern banking infrastructures.

VIII. SCREENSHOTS

Illusion PIN



Face verification



REFERENCES

[1] Bansal, Nitin. "The Impact of Financial Security Enhancement Through One Time Password in ATM Cash Transactions." *Organizational Sociology in the Digital Age.* IGI Global Scientific Publishing, 2025. 453–468.

[2] Thopate, Kaushalya, et al. "Smart ATM Security and Alert System with Real-Time Monitoring." *International Journal on Recent and Innovation Trends in Computing and Communication* 11.7 (2023): 32–38.

[3] Monisha, T., J. Reshma, and S. Shalini. "Enhancing Banking Security Through Multi-Modal Biometric Authentication System." *IRJET* 10.3 (2024): 68–78.

[4] Otuonye, Anthony I., et al. "Improving Security Features of Traditional ATM-Based Banking Services via Fingerprint Biometrics Scheme."

[5] Beju, Daniela-Georgeta, and Codruța-Maria Făt. "Frauds in Banking System: Frauds with Cards and Their Associated Services." *Springer International Publishing*, 2023. 31–52.

[6] Cavus, Nadire, et al. "Examining User Verification Schemes, Safety and Secrecy Issues Affecting M-Banking: Systematic Literature Review." *Sage Open* 13.1 (2023).

[7] Machap, Kamalakannan. "Facial Recognition Authentication Adds an Extra Layer of Security to Mobile Banking Systems." *Journal of Applied Technology and Innovation* 7.1 (2023).

[8] Ahmed, Khaled AM, et al. "A Blockchain Self-Sovereign Identity for Open Banking Secured by the Customer's Banking Cards." *Future Internet* 15.6 (2023): 208.

[9] Pavithra, Mrs Panthangi, et al. "Enhanced Security for ATMs with Facial Recognition Features and OTP." *Journal of Nonlinear Analysis and Optimization* 15.1 (2024).