Next-Generation Net Banking Security Using Illusion-Oriented Pin Concealment And Real-Time Facial Authentication

Mrs.BanuppriyaP[1], Moulieswaran J[2], Mythiswaran M[3], Kavinkumar R[4], Somnath C[5]
[1]Assist prof, Dept of Computer Science and Engineering
[2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Mahendra Institute of Engineering and Technology, Namakkal, Tamil Nadu, India.

Abstract- *The rapid expansion of digital banking has improved the accessibility and efficiency of financial transactions but has also introduced significant security challenges. Traditional authentication methods such as passwords and PINs are vulnerable to attacks like phishing, brute-force, and shoulder surfing. This research proposes a multi-layered authentication framework to enhance net banking security. The first layer uses an illusion-oriented PIN mechanism that conceals user input through a dynamic and deceptive keypad. The second layer integrates real-time facial biometric authentication for accurate user verification. Advanced techniques are applied to extract and analyze unique facial features. This combination ensures that only authorized users can access the system, even if credentials are compromised. The proposed approach effectively reduces unauthorized access and financial fraud. It also maintains a balance between security and usability without requiring additional hardware.*

I. INTRODUCTION

The rapid growth of digital banking has made financial transactions faster and more convenient for users worldwide. However, this advancement has also introduced serious security challenges in protecting user data and identities. Traditional authentication methods such as PINs and passwords are vulnerable to attacks like phishing, shoulder surfing, and brute-force attempts. These weaknesses oftenlead to unauthorized access and financiallosses. To overcome these issues, stronger authentication mechanisms are required. Multi-factor authentication, combining knowledge-based and biometric methods, provides improved security. Facial authentication is gaining popularity due to its uniqueness and reliability. Additionally, illusion-oriented PIN concealment helps prevent observation-based attacks by dynamically altering input patterns. Integrating these techniques enhances both security and usability in net banking systems. This paper proposes a secure framework that combines illusion-based PIN entry with real-time facial authentication.

II. LITERATURE REVIEW

Recent studies in net banking security have focused on improving authentication mechanisms to address increasing cyber threats. Traditional password-based systems have been widely criticized for their vulnerability to phishing and brute-force attacks. Researchers have proposed multi-factor authentication methods that combine passwords with biometrics such as fingerprints and facial recognition to enhance security. Facial authentication systems have shown promising results due to their accuracy and difficulty to replicate, although they may face challenges under varying lighting conditions. Additionally, graphical and dynamic PIN-based techniques have been introduced to reduce risks like shoulder surfing and keylogging. Illusion-based PIN systems further improve security by masking the actual input through dynamic visual patterns. These advancements highlight the need for integrating multiple secure techniques, which forms the foundation of the proposed system.

III. METHODOLOGY

The proposed methodology adopts a multi-layered authentication approach to enhance net banking security. It integrates illusion-oriented PIN concealment, where the keypad dynamically changes to prevent observation-based attacks. In addition, real-time facial authentication is used to verify the user's identity through continuous monitoring. Both authentication factors are validated together before granting access to the system. This combined approach ensures improved protection against unauthorized access while maintaining a smooth user experience.

IV. TARGET

The target of the proposed system is to enhance the security of net banking platforms against modern cyber threats. It aims to protect users from attacks such as phishing, shoulder surfing, and unauthorized access. The system focuses on providing a reliable and user-friendly multi-factor authentication mechanism. It is designed to ensure that only

authorized users can access sensitive financial information. Additionally, the target includes improving trust and confidence in digital banking services.

V. RELATED WORK

METHODOLOGY

Existing systems mainly use single or two-factor authentication methods such as passwords combined with OTPs or biometrics. Many studies propose combining graphical passwords and facial recognition to improve security. However, most approaches lack protection against observation-based attacks. The proposed method improves upon these by integrating illusion-based PIN concealment with real-time facial verification.

DATA COLLECTION

Data used in related works typically include user credentials and facial image datasets for training recognition systems. Facial data is collected using cameras under different lighting and environmental conditions. Public datasets and real-time captured images are commonly used. Secure storage and privacy of collected data remain important considerations.

DATA PREPROCESSING

Preprocessing involves cleaning and preparing facial images for accurate recognition. Techniques such as resizing, normalization, and noise removal are applied. Face detection and alignment are performed to extract key features. These steps help improve the accuracy and efficiency of biometric authentication systems.

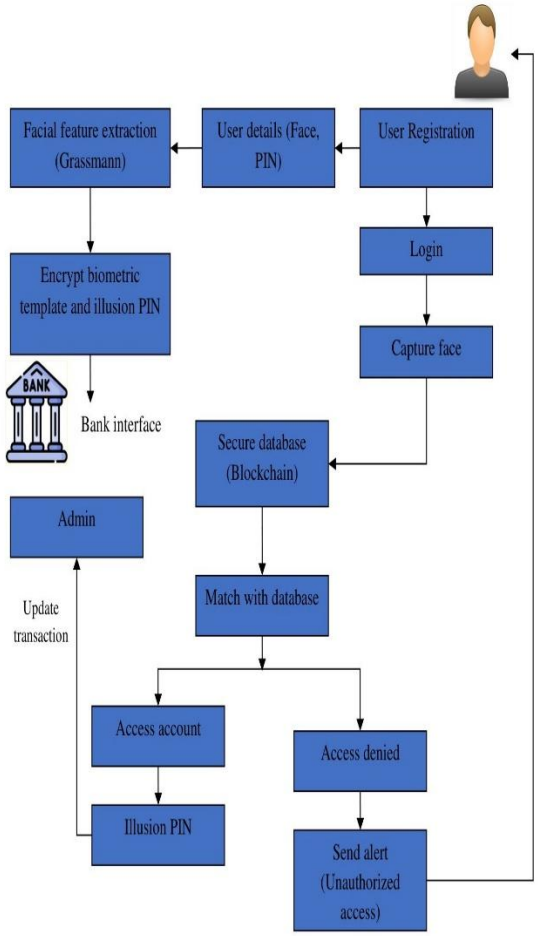
MODEL SELECTION

Various machine learning and deep learning models are used for facial recognition, including CNN-based architectures. Models are selected based on accuracy, speed, and real-time performance. Lightweight models are preferred for banking applications to reduce latency. The chosen model must balance security and computational efficiency.

EVALUATION

Evaluation of authentication systems is based on metrics such as accuracy, false acceptance rate, and false rejection rate. Security strength against attacks like phishing and shoulder surfing is also analyzed. Performance is tested under different conditions to ensure reliability. Results from related work show improvements, but still highlight the need for stronger multi-layered security systems.

VI. WORKFLOW DIAGRAM



VII. PROPOSED ALGORITHM

A. Illusion-Based Dynamic PIN Algorithm

This algorithm is used to secure PIN entry by dynamically changing the visual representation of the keypad. Each time the user enters a PIN, the positions or appearance of digits are altered, making it difficult for attackers to capture or predict the input. It protects against shoulder surfing and screen recording attacks by hiding the actual input pattern.

B. Face Detection Algorithm

This algorithm is used to detect the presence of a human face in real-time. It works by identifying facial features such as eyes, nose, and mouth using trained classifiers. Haar Cascade is efficient and widely used for fast face detection in live camera feeds.

C. Face Recognition Algorithm

LBPH is used to recognize and verify the user's identity by analyzing facial features. It converts facial images into numerical patterns and compares them with stored data. This algorithm is robust under different lighting conditions and suitable for real-time applications.

D. Authentication Algorithm

This is a security approach that combines two or more authentication methods, such as knowledge-based (PIN) and biometric (face). Access is granted only when all factors are successfully verified, ensuring higher security compared to single-factor systems.

VIII. RESULT

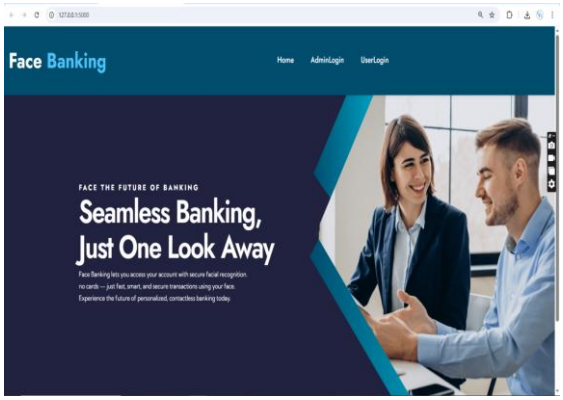


Fig 7.1

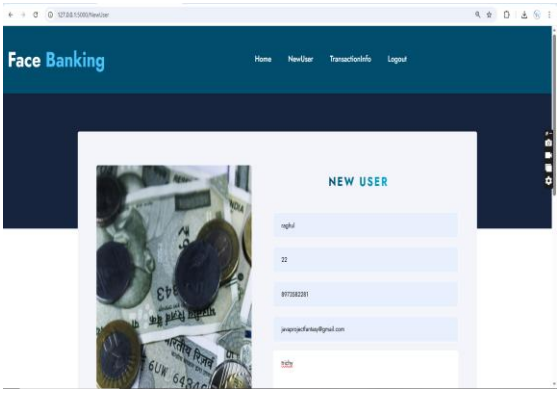


Fig 7.2

Fig 7.3

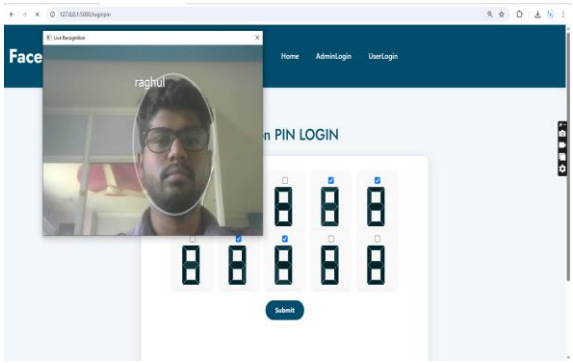


Fig 7.4

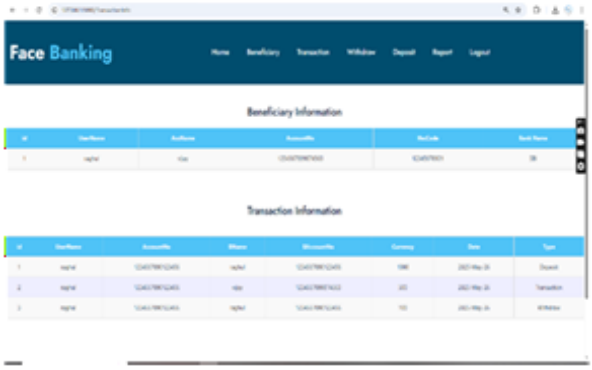


Fig 7.5

The proposed system shows improved security compared to traditional authentication methods. The illusion-based PIN mechanism successfully prevents shoulder surfing and observation attacks. Real-time facial authentication ensures accurate identification of users. The integration of both methods reduces the chances of unauthorized access. The system performs efficiently with minimal delay during authentication. Experimental analysis indicates high accuracy and reliability. Overall, the approach enhances both security and user experience in net banking systems.

IX. CONCLUSION

The proposed system offers a robust solution for enhancing net banking security. It overcomes the weaknesses

of traditional password and PIN-based authentication methods. The illusion-oriented PIN mechanism effectively protects against shoulder surfing and observation attacks. Real-time facial authentication ensures accurate and reliable user verification. The integration of these techniques provides a strong multi-factor authentication framework. The system significantly reduces the chances of unauthorized access and cyber threats. It maintains a balance between security, performance, and user convenience. The approach is practical and does not require additional hardware. Experimental results demonstrate improved accuracy and system efficiency. Overall, the proposed model strengthens trust and reliability in digital banking systems.

REFERENCES

[1] Ahmed, Waqas, et al. "Security in next generation mobile payment systems: A comprehensive survey." IEEE Access 9 (2021): 115932-115950.

[2] Hashemi, SeyedehKhadijeh, SeyedehLeiliMirtaheri, and Sergio Greco. "Fraud detection in banking data by machine learning techniques." IEEE Access 11 (2022): 3034-3043.

[3] Vergallo, Roberto, and Luca Mainetti. "The role of technology in improving the Customer Experience in the banking sector: A systematic mapping study." IEEE Access 10 (2022): 118024-118042.

[4] Almadan, Ali, and AjitaRattani. "Benchmarking neural network compression techniques for ocular-based user authentication on smartphones." IEEE Access 11 (2023): 36550-36565.

[5] Cavus, Nadire, et al. "Examining user verification schemes, safety and secrecy issues affecting m-banking: Systematic literature review." Sage Open 13.1 (2023): 21582440231152379.