IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429 Volume 5, Issue 3, May 2025 Impact Factor: 7.67

# Preventing Financial Fraud in Net Banking with AI and Face Recognition Technology

**B. Venkatesh M.E., R. Santhosh, P. Shiyam**

Assistant Professor, Department of Information Technology Students,
B.Tech., Final Year, Department of Information Technology
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India.
venkateshaamec@gmail.com, santhoshravi7503@gmail.com, shiyam9904@gmail.com

**Abstract**: *Online banking has revolutionized financial transactions by offering unmatched convenience, yet it continues to face persistent security challenges. Existing security mechanisms such as One-Time Passwords (OTPs), smart cards, and USB tokens, though widely adopted, have notable limitations. OTPs can be intercepted, while smart cards and tokens are susceptible to loss, theft, and misuse, making them less reliable for robust security. This project proposes a next-generation Net Banking security framework that integrates* ***real-time facial biometrics*** *to address these vulnerabilities. By combining* ***facial recognition with the Grassmann algorithm****, the system delivers a* ***scalable, cost-effective, and efficient user authentication solution*** *superior to traditional biometric methods like fingerprint and iris recognition. Furthermore, the system enhances PIN security through an innovative* ***Illusion View-based PIN identification and verification mechanism****, significantly reducing the risk of* ***PIN theft, shoulder surfing, and brute force attacks****. To counter spoofing attempts and ensure the authenticity of users,* ***liveness detection*** *is embedded into the facial recognition module. This prevents unauthorized access by effectively distinguishing live users from fraudulent attempts using printed images or static photos. Through the convergence of facial biometrics, PIN obfuscation, and liveness verification, this system aims to establish a* ***multi-layered security model*** *that addresses current weaknesses in Net Banking authentication. It offers a* ***more secure, user-friendly, and fraud-resistant*** *alternative to conventional card- and PIN-based methods, thereby fortifying online banking against evolving cyber threats.*

**Keywords**: Multi-factor authentication (MFA), Phishing attacks, Photo/video spoofing, Artificial Intelligence (AI), Machine learning (ML), Image-based authentication, PIN obfuscation, Illusion PIN, Liveness detection, Real-time user authentication, Spoofing resistance, Secure PIN entry, Continuous authentication

## I. INTRODUCTION

With the increasing dependence on digital banking platforms, the threat of online financial fraud has become more prevalent, demanding more secure and user- friendly authentication methods. Traditional security approaches such as usernames, passwords, and One-Time Passwords (OTPs) are often vulnerable to attacks like phishing, shoulder surfing, and brute force attempts. These systems are also prone to human error and are often inconvenient for users, resulting in poor password hygiene and compromised accounts. Recognizing these limitations, this project proposes a next-generation net banking authentication model that combines behavioral and biometric security for robust fraud prevention. The proposed system introduces a dual-layer authentication mechanism.

The first layer employs an Illusion PIN-based verification system that enhances security by making the user's PIN entry unintelligible to external observers, thus mitigating the risk of shoulder-surfing and pattern recognition attacks. This innovative approach ensures that even if someone is physically watching the login process, they cannot easily deduce the actual PIN. Unlike conventional PIN entry systems, this method blends deception with authentication, offering a stronger defense against common intrusion techniques while maintaining ease of use.

DOI: 10.48175/IJARSCT-26334

The second layer integrates real-time facial recognition with liveness detection, using the Grassmann algorithm for accurate facial feature extraction and matching. This biometric layer ensures that access is granted only to the legitimate user, even if someone manages to obtain their PIN. Liveness detection further prevents spoofing using printed photos or video replays, making the system resilient against common face recognition vulnerabilities. During sensitive operations like fund transfers, the system re-verifies the user's identity through face recognition, adding a real-time security checkpoint. Together, these layers form a cost- effective, scalable, and user-friendly security model that strengthens trust in net banking and significantly reduces the risk of unauthorized financial activities.

## II. PROBLEM STATEMENT

Traditional net banking authentication systems, primarily based on PIN and password mechanisms, have become increasingly vulnerable to various types of cyberattacks, such as phishing, credential theft, and shoulder-surfing. These systems often rely on static credentials like usernames, PINs, or OTPs that can easily be compromised through a variety of techniques. PIN-based systems are highly susceptible to brute force attacks, guessing attempts, and social engineering tactics. Additionally, the increasing use of mobile banking apps has made it easier for attackers to exploit weak authentication practices and gain unauthorized access to users' accounts, putting sensitive financial data at significant risk.

Conventional authentication methods also offer little protection against attacks where users are unaware of fraudulent activities, such as SIM swapping or stolen OTPs. Another critical issue with existing systems is the inability to accurately verify the identity of users during sensitive transactions. Face recognition technologies, while offering an advanced form of biometric authentication, are often vulnerable to spoofing using printed images or videos of the user. Moreover, traditional biometric systems lack the ability to verify whether the individual is physically present, making it easy for attackers to bypass authentication using a photo or video replay. To further compound these issues, traditional banking systems do not provide real-time alerts for unauthorized transactions beyond initial account access, making it difficult for users to monitor and respond to fraudulent activities promptly. As online banking evolves, the need for a more sophisticated and secure multi-layered authentication system that addresses these challenges has become paramount.

## III. EXISTING SYSTEM

Online banking security has always been a critical concern, and various technologies have been implemented to safeguard financial transactions. One of the most used security measures is the One-Time Password (OTP) system. OTPs are temporary passwords that are typically sent to a user's mobile device or email and are used to authenticate a transaction. While OTPs provide an additional layer of security, they are not foolproof. Attackers can exploit vulnerabilities such as SIM swapping or intercepting OTPs via phishing or man- in-the-middle attacks. Additionally, OTPs are limited to one-time use and do not provide continuous security verification, which leaves the system susceptible to ongoing fraud once the initial authentication is bypassed. Another widely adopted security measure is the use of smart cards and USB tokens, which serve as physical devices that verify the user's identity. These tokens generate a secure code or store authentication data to allow users to access their online banking accounts. While this method adds a physical security layer, it is not immune to theft or loss. If a user's smart card or USB token is stolen or lost, it can be used by an attacker to gain unauthorized access. Furthermore, these systems require users to carry an additional physical device, which may cause inconvenience and disrupt the smoothness of the user experience. Despite these efforts, existing authentication methods like username-password combinations and PIN-based systems still present significant vulnerabilities.

Conventional methods are vulnerable to brute-force attacks, where attackers systematically guess login credentials, or online dictionary attacks, where common words or simple patterns are used to break into an account. The inherent weakness of passwords, especially weak or reused ones opens the door for unauthorized access. Moreover, users often fail to adopt strong passwords or change them regularly, leaving their accounts open to fraud. SMS alerts, which are sometimes used to notify users about transactions, only provide a snapshot of current activities. They are not sufficient for ongoing security monitoring, leaving it difficult for users to track unauthorized access or fraud in real time.

## IV. PROPOSED SYSTEM

The proposed system introduces a multi-layered authentication approach to enhance the security and usability of net banking platforms. The first layer utilizes an Illusion PIN-based authentication method, which obscures the actual PIN input to prevent shoulder-surfing attacks. This method presents users with a deceptive visual pattern where the true PIN is hidden among a grid of random numbers, ensuring that even if an attacker observes the user entering their PIN, they cannot accurately determine the correct sequence. This additional layer of security minimizes the risk of PIN theft through direct observation or brute force. The second layer of authentication involves real-time facial recognition using advanced AI algorithms, specifically the Grassmann algorithm, to ensure that the user's face matches the stored biometric data. This system works by capturing the user's facial features and comparing them to pre-registered data in the database. The Grassmann algorithm enhances the accuracy of facial recognition by evaluating essential facial features such as energy, mean, and standard deviation, forming a unique feature vector. To prevent spoofing attempts, liveness detection is also incorporated, distinguishing between a real user and fraudulent attempts using photographs or videos, thus strengthening the biometric verification process. The proposed system aims to provide seamless, real-time authentication while maintaining a high level of security. It integrates SMS alerts to notify users of each transaction, ensuring that they are immediately aware of any unauthorized activities on their accounts. By combining Illusion PIN-based verification with facial recognition and liveness detection, the system ensures a robust, secure, and user-friendly authentication experience. This multi-layered security model not only reduces the risk of fraud but also enhances the privacy and trust of users when conducting sensitive online banking transactions

### ADVANTAGES OF THE PROPOSED SYSTEM

- Enhanced security with multi-layered authentication (Illusion PIN + facial recognition).
- Prevents shoulder surfing and brute-force attacks through the Illusion PIN method.
- Real-time face authentication with liveness detection to block spoofing attempts.
- SMS alerts keep users informed about transactions and suspicious activities.
- No need for additional hardware; the system works with standard cameras and smartphones

## V. GRASSMANN ALGORITHM FOR FACE RECOGNITION

To improve recognition performance, face detection is initially applied to each frame, ensuring that only the facial region is analyzed. This step eliminates background noise and irrelevant content. Once the face is localized, geometric normalization is performed using affine transformation based on facial landmarks, aligning each face to a common coordinate frame for consistent analysis.

The core of the approach involves operating on subspaces that represent face images, which lie on a Grassmann manifold. The goal is to compute a central subspace, known as the Karcher mean, that best represents a set of face subspaces. This process follows an iterative algorithm with the following steps:

### 1. Initialization

Start by randomly selecting one subspace from the dataset as the initial estimate of the Karcher mean.

### 2. Tangent Vector Computation

Calculate the average direction (tangent vector) from the current estimate to all other subspaces in the dataset. This represents the overall direction in which the estimate should move to become more representative of the dataset.

### 3. Convergence Check

If the average direction is sufficiently small—indicating that the estimate is close to the true mean—the algorithm stops and returns the current estimate as the final Karcher mean.

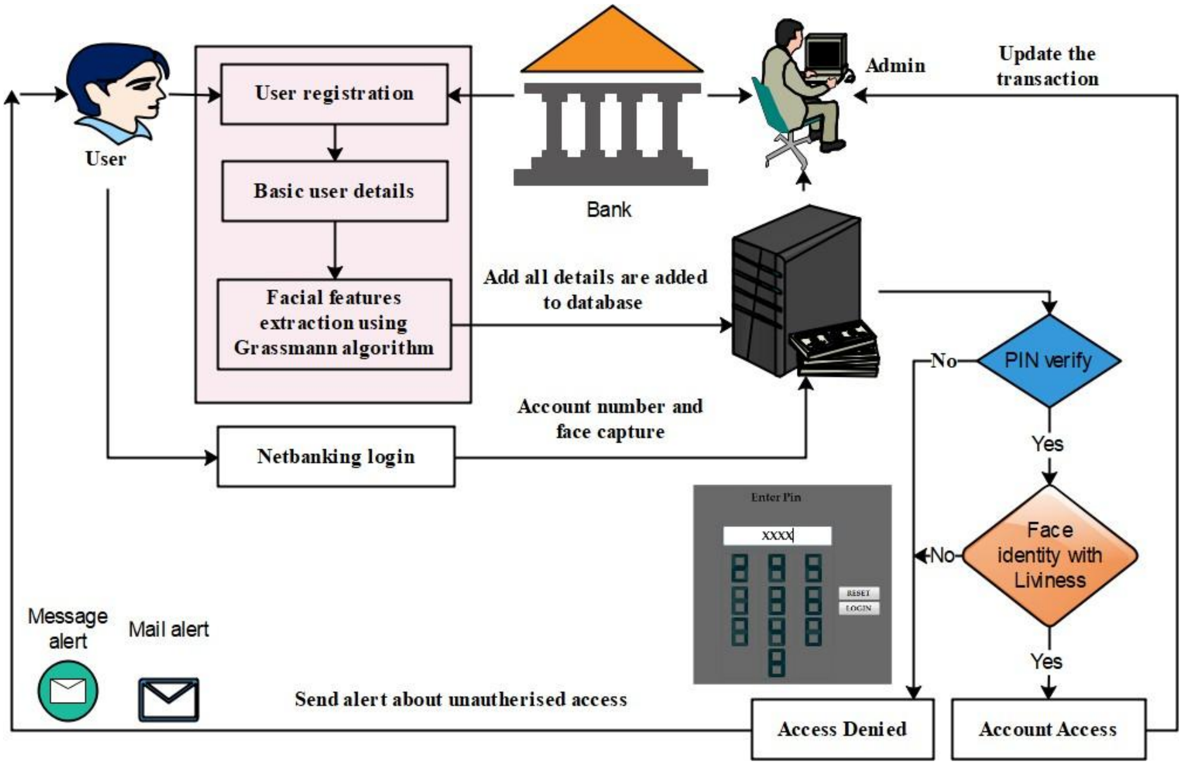
### 4. Update Step

If convergence has not yet been achieved, the current estimate is adjusted slightly in the direction of the average tangent vector. This step is repeated iteratively to refine the estimate.

DOI: 10.48175/IJARSCT-26334

The process continues until the estimate stabilizes or a maximum number of iterations is reached. This algorithm ensures that the final Karcher mean effectively captures the intrinsic structure of facial subspace representations, making it suitable for tasks such as face recognition and clustering.

## VI. SYSTEM ARCHITECTURE DIAGRAM


User
User registration
Basic user details
Facial features extraction using Grassmann algorithm
Bank
Admin
Update the transaction
Add all details are added to database
Account number and face capture
Netbanking login
PIN verify
No
Yes
Face identity with Liviness
No
Yes
Enter Pin
xxxx
RESET
LOGIN
Message alert
Mail alert
Send alert about unautherised access
Access Denied
Account Access

## VII. MODULES

**List of Modules:**

1. Bank Interface Creation
2. User Registration Process
3. User PIN Verification
4. Face Image Verification
5. Online Transaction

### 1. Bank Interface Creation

- Online banking is thus changing the way people shop and how retailers operate.
- In this module, admin and user interface are created.
- Admin can be viewing the details of users, accounts details and so on.
- The user can be performing various operations such as net banking, credit card transactions, and debit card transactions.

### 2. User Register Process

- Before a user can be authenticated to the system, they must be registered with the system for the first time.

- This step is called registration. So, for a new user, must get register with a system and then authenticated before he can request services.
- The face image register module consists of two main components: the camera and the database.
- Here, users should create their own PIN number for further verification process.
- Once the camera has captured the individual's facial features, the data is stored in a database.

### 3. User PIN Verification

- Authentication is the process of determining whether a user should be allowed to access to a particular system or resource.
- User can't remember strong password easily and the passwords that can be remembered are easy to guess.
- After registration, user enters the system using login setting.
- A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security.
- PIN authentication process allows influencing Illusion PIN method for stronger PIN verification.

### 4. Face Image Verification

- After registration, the user can set password using face capture process.
- First, the camera is enabling in system for capturing the face.
- The identification of the test image is done by locating the image in the database that has the highest similarity with the test image.
- Here feature vector is made from important values of the image from each filter Energy, mean and standard deviation forming a 40-value feature vector for every image.
- The input facial features match with database using Grassmann learning algorithm.

### 5. Online Transaction

- Users initiate online transactions by logging into their accounts and selecting the transaction type (e.g., purchase, money transfer).
- During the transaction process, prompt the user for face verification.
- Capture the user's face image using a webcam or smartphone camera.
- Extract facial features from the captured image using the same face recognition algorithm and Grassmann learning model trained in the previous module.
- Compare the extracted features to the authenticated user's stored features. If the match is successful, carry through the transaction; if not, reject it.

## VIII. CONCLUSION

The proposed system for preventing financial fraud in net banking through multi-layer authentication, combining Illusion PIN-based authentication and real-time face biometrics, provides a robust and efficient solution to enhance online banking security. By integrating face verification with advanced Grassmann learning algorithms and liveness detection, the system effectively mitigates the risks associated with traditional authentication methods like PIN theft, shoulder surfing, and phishing attacks. The use of real-time face biometrics for transaction verification ensures that only authorized users can complete sensitive banking activities, making unauthorized access significantly harder. Overall, this approach offers a scalable and cost- effective solution to the ongoing challenge of securing online banking systems. The incorporation of SMS alerts for transaction updates, combined with multi-layer security checks, provides users with real-time information on their account activities, further reducing the potential for fraud. With its combination of convenience, security, and user-friendly design, the system presents a substantial advancement over existing banking security measures, ultimately providing safer, more reliable online financial transactions.

DOI: 10.48175/IJARSCT-26334

## REFERENCES

[1]. 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.

[2]. Karim, Nader Abdel, et al. "Online banking user authentication methods: a systematic literature review." IEEE Access 12 (2023): 741- 757.

[3]. Darem, Abdulbasit A., et al. "Cyber threats classifications and countermeasures in banking and financial sector." IEEE Access 11 (2023): 125138-125158.

[4]. Sedik, Ahmed, et al. "Deep learning modalities for biometric alteration detection in 5G networks-based secure smart cities." IEEE Access 9 (2021): 94780-94788.

[5]. Hajiabbasi, Milad, Ehsan Akhtarkavan, and Babak Majidi. "Cyber-physical customer management for internet of robotic things-enabled banking." IEEE Access 11 (2023): 34062-34079.

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

[7]. Hashemi, Seyedeh Khadijeh, Seyedeh Leili Mirtaheri, and Sergio Greco. "Fraud detection in banking data by machine learning techniques." IEEE Access 11 (2022): 3034- 3043.

[8]. 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.

[9]. 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.

[10]. Asha, R. B., and Suresh Kumar KR. "Credit card fraud detection using artificial neural network." Global Transitions Proceedings 2.1 (2021): 35-41

DOI: 10.48175/IJARSCT-26334