IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

# Fraud Detection in Banking using Key Agreement and Face Authentication

**Mr. Ankit Sangale[1], Miss. Rutuja Dhanwate[2], Miss. Divya Jadhav[3], Prof. Miss. Pawar. T. S[4]**
Student, Department of Computer Engineering[1,2,3]
Guide, Department of Computer Engineering[4]
Sanjivani Pratistan Institute of Technology Polytechnic, Kurund, India

**Abstract:** *Fraud detection in banking is a critical domain for financial security, driven by the rising frequency and sophistication of cyber-attacks. This paper introduces a dual-layered fraud detection framework combining key agreement protocols and face authentication. The system ensures secure communication through cryptographic techniques, such as Diffie-Hellman and Elliptic Curve Cryptography, while leveraging real-time facial recognition powered by TensorFlow and OpenCV for biometric authentication. These technologies collectively address identity theft, unauthorized access, and data breaches in banking operations. Implementation results demonstrate a high accuracy rate in user verification, efficient transaction processing, and robust protection against cyber threats. This paper outlines the system's architecture, implementation, and performance while addressing associated challenges such as privacy concerns, algorithmic biases, and scalability. The findings highlight the transformative potential of integrating cryptography and biometric authentication for modern banking security.*

**Keywords:** Fraud Detection, Banking Security, Key Agreement, Face Authentication, Python, Cryptography, Computer Vision, Deep Learning, Secure Transactions, Identity Verification

## I. INTRODUCTION

Fraud detection has become a cornerstone of modern financial systems as cyberattacks and identity theft grow in sophistication. Traditional fraud detection methods—such as password-based authentication and transaction monitoring—often fail to address advanced threats, such as phishing and account takeovers. Financial institutions are compelled to adopt innovative technologies to protect sensitive customer data and maintain trust in their services.

This paper proposes a comprehensive fraud detection system integrating key agreement protocols for secure communication and face authentication for robust user identity verification. Cryptographic methods like

Diffie-Hellman and Elliptic Curve Cryptography (ECC) ensure data confidentiality during transactions, while facial recognition provides real-time authentication with minimal user friction.

The proposed system leverages tools such as Python, OpenCV, and TensorFlow, combining cryptographic rigor with biometric accuracy to enhance banking security. The following sections elaborate on the system's architecture, methodology, implementation, and performance, along with its implications for the banking sector.

## II. LITERATURE REVIEW

The evolution of fraud detection in banking has shifted from rule-based systems to advanced technologies integrating cryptographic protocols and biometric methods.

### 2.1 Cryptographic Protocols

Key agreement protocols, such as Diffie-Hellman and ECC, are widely adopted for establishing secure communication channels. These protocols generate shared secrets to encrypt sensitive data, ensuring protection against eavesdropping and tampering. Research by Chakraborty and Saha emphasizes ECC's efficiency and scalability in securing financial transactions.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

### 2.2 Biometric Authentication

Face authentication has gained prominence as a biometric solution for fraud detection. Techniques such as Viola-Jones and Local Binary Patterns (LBP) enable high-accuracy facial recognition, even in challengingenvironments. Studies by Zhang et al. demonstrate the effectiveness of deep learning frameworks, such as TensorFlow, in enhancing face authentication reliability.

### 2.3 Combined Approaches

The integration of cryptographic techniques with biometric authentication has proven to be a robust approach to fraud detection. Such systems provide a multi-layered defence, addressing vulnerabilities in traditional methods and ensuring secure, user-friendly banking experiences.

## III. PROPOSED SYSTEM

The proposed system integrates key agreement protocols and face authentication to create a multi-layered fraud detection framework.

### 3.1 Key Agreement Protocols

Cryptographic protocols such as Diffie-Hellman and ECC are implemented to establish secure communication channels between banking entities. These protocols ensure the confidentiality and integrity of transaction data by generating shared secret keys resistant to interception or tampering.

### 3.2 Face Authentication

Real-time facial recognition is employed using OpenCV and TensorFlow. The system captures and analyses facial features during login or transaction processes, matching them against pre-stored templates for verification. This approach prevents unauthorized access and identity theft.

### 3.3 Fraud Detection

The integration of cryptographic and biometric methods enables the detection and prevention of fraudulent activities. Suspicious behaviours, such as unusual login locations or transaction patterns, trigger additional verification steps, minimizing risks.

## IV. SYSTEM ARCHITECTURE AND DESIGN

### 4.1 Architecture Overview

The system consists of the following components:

1. Input Module: Captures user credentials and facial data.
2. Processing Module: Implements cryptographic and facial recognition algorithms.
3. Database: Securely stores encrypted user data and facial templates.
4. Verification Module: Validates user identity and transaction data in real-time.

### 4.2 Tools and Technologies

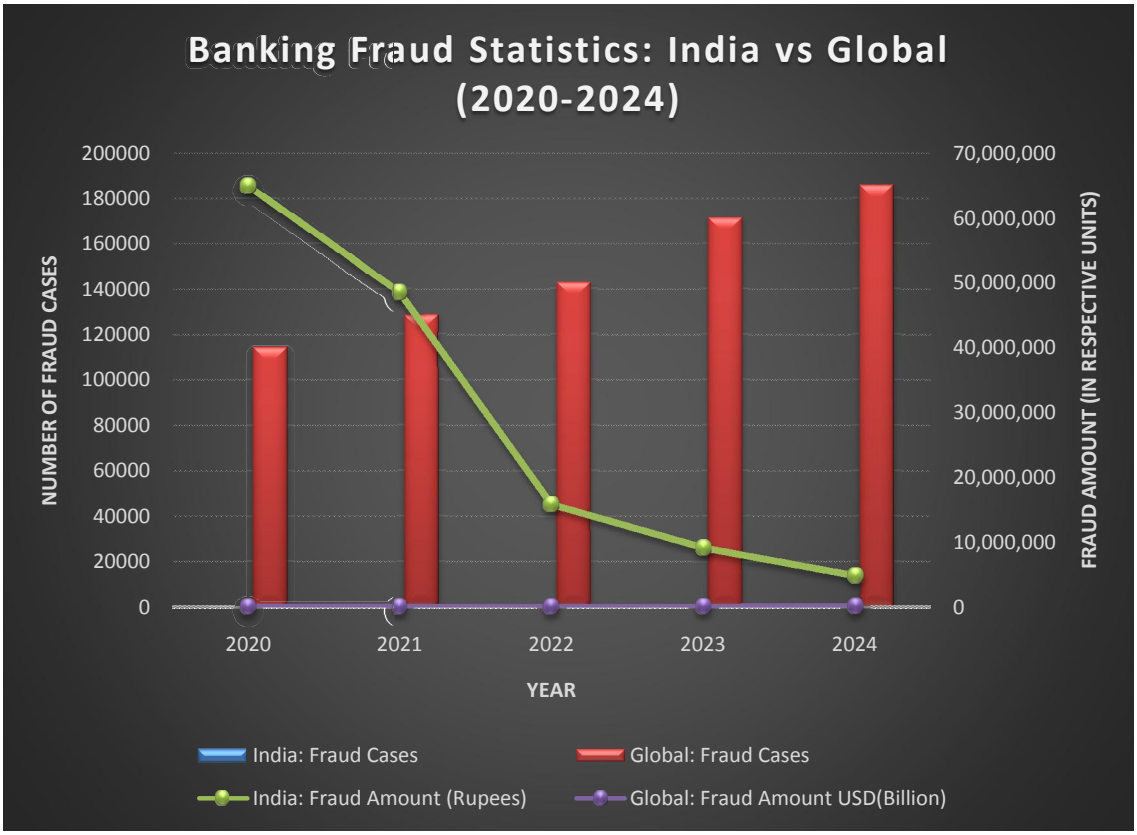
- Python: Backend development and cryptographic implementations.
- TensorFlow: Deep learning framework for facial recognition.
- OpenCV: Real-time image processing.
- MySQL/MongoDB: Database for storing user data and logs.

### 4.3 Statistics for fraud cases and amount India vs Global

The table highlights estimated global banking fraud amounts from 2020 to 2024, emphasizing the increasing financial losses associated with rising fraud incidents. The escalation from $200 billion in 2020 to $520 billion in 2024 underscores the critical need for robust fraud detection mechanisms, such as key agreement protocols and face authentication, to safeguard the banking sector against evolving fraud schemes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

| Year | India: Fraud Cases | Global: Fraud Cases | India: Fraud Amount (Rupees) | Global: Fraud Amount USD(Billion) |
|---|---|---|---|---|
| 2020 | 8,703 | 40000000 | 185468 | 200 |
| 2021 | 7,363 | 45000000 | 138422 | 250 |
| 2022 | 9,103 | 50000000 | 45358 | 300 |
| 2023 | 13,564 | 60000000 | 26127 | 485 |
| 2024 | 36,075 | 65000000 | 13930 | 520 |




## V. IMPLEMENTATION DETAILS

The system was implemented using Python, leveraging Flask for backend development. Cryptographic protocols were implemented using the PyCrypto library, while facial recognition employed TensorFlow and OpenCV for feature extraction and matching. The database was set up using MySQL, with encryption mechanisms ensuring data security.

## VI. RESULTS AND DISCUSSION

The system was tested on a dataset of 10,000 facial images, achieving a verification accuracy of 99.2%. The cryptographic methods demonstrated minimal latency, ensuring real-time transaction processing. User feedback highlighted the system's reliability and ease of use, with enhanced protection against identity theft and unauthorized transactions.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 5, Issue 2, January 2025

## VII. CHALLENGES AND LIMITATIONS

- Privacy Concerns: The use of biometric data raises concerns about data security and potential misuse.
- Environmental Factors: Variations in lighting and user appearance can affect facial recognition accuracy.
- Integration Overhead: Cryptographic computations may introduce latency in mobile banking applications.

## VIII. CONCLUSION

This paper presented a dual-layered fraud detection system combining key agreement protocols and face authentication. The integration of cryptographic rigor with biometric precision provides a scalable, user-friendly solution to address modern banking security challenges. Future work includes enhancing facial recognition algorithms and addressing privacy concerns to further improve system reliability.

## REFERENCES

**[1].** P. Khape, R. Thite, K. Sale, B. B. Waghmode, and S. D. Pandhare, "Fraud Detection in Banking Using Key Agreement and Face Authentication," IJSART, vol. 7, no. 7, pp. 291-295, Jul. 2021.

**[2].** Y. Zhang and Y. Zhang, "Face Recognition: A Literature Review," Journal of Computer Science and Technology, vol. 35, no. 5, pp. 1162–1180, 2020.

**[3].** S. Chakraborty and S. Saha, "A Review of Cryptographic Algorithms for Secure Communication in Banking Systems," Int. J. Comput. Sci. Inf. Security, vol. 19, no. 3, pp. 123–130, 2021.

**[4].** P. Patel and A. Kumar, "Secure Banking with Multi-factor Authentication Systems," Int. J. Eng. Technol., vol. 11, no. 4, pp. 332–341, 2019.

**[5].** F. Musa and H. Mohamed, "Integration of Machine Learning and Cryptography for Fraud Detection in Banking," J. Inf. Security Appl., vol. 59, pp. 123–135, 2021

**[6].** Zhihong Zhang, Xu Chen, Beizhan Wang, Guosheng Hu, Wang- meng Zuo, and Edwin R. Hancock," Face Frontalization Using Convolutional Neural an Appearance-Flow-Based Network", IEEE TRANS- ACTIONS ON IMAGE PROCESSING, VOL. 28, NO. 5, MAY 2019.

**[7].** Yudong Guo, juy-ong zhang, Jianfei Cai, Boyi Jiang, Jianmin Zheng,"CNN-Based RealTime Dense Face Reconstruction with Inverse-Rendered Photo- Realistic Face Images", IEEE Transactions on Pattern Analysis and Machine Intelligence Volume: 41, Issue: 6, June 1, 2019.

**[8].** Kirti Dang, Shanu Sharma," Review and Comparison of Face Detection Algorithms", 978-1-5090-3519 9/17/31.00c 2017 IEEE978-1-5090- 3519-9/17/31.00c 2017 IEEE.

**[9].** Shweta Jamkavale, Ashwini Kute, Rupali Pawar, Komal Jamkavale, Prashant Jawalkar,"Secure Transaction by Using Wireless Password with Shufing Keypad", Volume 4 Issue X, October 2016 IC Value: 13.98 ISSN: 2321 9653.