2026 Volume: 02 Issue: 04 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-13

ONLINE BANKING FRAUD DETECTION USING CYBER SECURITY

***S. Keerthana, S. Ravi Kumar, M. Bharath Kumar**

GMR Institute of Technology.

Article Received: 13 March 2026
Article Revised: 02 April 2026
Published on: 22 April 2026

***Corresponding Author: S. Keerthana**
GMR Institute of Technology.

DOI: https://doi-doi.org/101555/ijarp.5400

1. ABSTRACT

The rapid proliferation of digital banking services has significantly increased the volume and velocity of financial transactions, while simultaneously expanding the attack surface for sophisticated fraud schemes. Conventional security mechanisms, predominantly reliant on static authentication techniques, are increasingly inadequate in mitigating evolving and context-aware cyber threats. This study proposes an intelligent, multi-layered fraud prevention framework that integrates Multi-Factor Authentication (MFA), behavioural analytics, and machine learning–driven risk assessment to enhance transaction security in dynamic environments. The proposed system employs behavioural profiling techniques to continuously monitor user interaction patterns, including device usage, transaction behaviour, and temporal activity, enabling the detection of deviations indicative of fraudulent intent. A Random Forest–based classification model is utilized to analyse transactional and contextual features, generating a dynamic risk score for each activity. This risk-adaptive approach facilitates real-time decision-making, including step-up authentication or transaction blocking based on the assessed threat level. Additionally, the framework incorporates continuous learning mechanisms to address concept drift and evolving fraud patterns, thereby maintaining model robustness over time. Real-time monitoring and adaptive thresholding contribute to improved detection accuracy while minimizing false positives. The architecture is designed to ensure scalability, operational efficiency, and minimal impact on legitimate user experience. The proposed system demonstrates the effectiveness of combining authentication, behavioural intelligence, and ensemble machine learning techniques in delivering a resilient and practical solution for modern digital banking fraud prevention.

KEYWORDS: Fraud Detection, Online Banking Security, Machine Learning, MFA, Risk Analysis, Cyber Threats

2. INTRODUCTION

Online banking has become a key part of modern digital life, enabling fast and convenient financial transactions. At the core of this system lies trust, ensuring that every transaction is secure and authentic. However, with the growth of digital platforms, fraud techniques have also become more advanced and difficult to detect. Traditional security methods like passwords are no longer sufficient, as attackers use techniques such as phishing and account takeover to exploit system weaknesses. To address this, modern systems use Multi-Factor Authentication (MFA), adding extra layers of verification. While this improves security, it still cannot fully prevent sophisticated fraud attacks. This has led to the adoption of machine learning and risk-based analysis, where systems continuously monitor transactions, learn user behavior, and detect anomalies in real time. By assigning risk levels to each transaction, the system can make intelligent decisions such as allowing, verifying, or blocking activities. Together, these approaches create a smart and adaptive fraud detection system that enhances security while maintaining a smooth user experience.

In addition to these measures, behavioral biometrics further strengthen security by analyzing patterns such as typing speed, mouse movements, and login habits to uniquely identify users. Device fingerprinting is also employed to recognize trusted devices and flag unknown or suspicious access attempts. Real-time alert systems notify users and administrators instantly when unusual activities are detected, enabling quick response and mitigation. Integration of adaptive authentication ensures that the level of security dynamically adjusts based on the risk score of each transaction. Furthermore, continuous model training allows the system to evolve with emerging fraud patterns, improving detection accuracy over time. These combined technologies create a proactive defense mechanism, reducing false positives while ensuring genuine users experience minimal disruption. Overall, this layered and intelligent approach significantly enhances the resilience of online banking systems against modern cyber threats.

3. LITERATURE REVIEW

Several researchers have analyzed the growing challenges of online banking fraud and the need for advanced security mechanisms in digital financial systems.

“Multi-Factor Authentication in Digital Banking Systems” discusses the role of multiple authentication layers in enhancing user verification and preventing unauthorized access. It explains how combining knowledge, possession, and biometric factors improves security compared to traditional password-based systems. The study also highlights adaptive MFA

techniques that dynamically adjust authentication requirements based on risk levels. However, it points out limitations such as increased user friction and inability to detect fraudulent activities after login, suggesting the need for continuous authentication mechanisms. [1]

“Behavioral Biometrics for Continuous Authentication in Online Banking” explores the use of user interaction patterns such as keystroke dynamics, touch behavior, and mouse movements for identity verification. It emphasizes that behavioral biometrics enables passive and continuous authentication without interrupting user experience. The study demonstrates improved fraud detection capability by identifying deviations in user behavior. However, it also highlights challenges such as variability in user patterns and higher false positive rates, recommending integration with other security approaches. [2]

“Credit Card Fraud Detection using Machine Learning Techniques” examines the application of supervised learning algorithms such as Random Forest and Support Vector Machines for detecting fraudulent transactions. It highlights the effectiveness of these models in handling large-scale and high-dimensional datasets. The study also addresses the issue of class imbalance using techniques like oversampling and cost-sensitive learning. However, it notes that model performance may degrade over time due to evolving fraud patterns, suggesting the need for adaptive learning models. [3]

“Deep Learning Approaches for Financial Fraud Detection using LSTM and GRU Networks” focuses on the use of sequential models to capture temporal patterns in transaction data. It explains how LSTM and GRU networks improve detection accuracy by analyzing time-dependent behaviors. The study highlights their effectiveness in identifying complex fraud scenarios that traditional models may miss. However, it also discusses limitations such as high computational cost and lack of interpretability, which can affect their practical deployment in real-time systems. [4]

“Concept Drift Adaptation Techniques in Fraud Detection Systems” addresses the challenge of continuously changing fraud patterns in financial systems. It discusses various adaptive learning methods such as sliding window techniques, incremental learning, and ensemble approaches to handle concept drift. The study shows that these methods improve long-term model performance and maintain detection accuracy. However, it also points out challenges related to computational complexity and maintaining model stability during frequent updates. [5]

“BANKSEALER: A Decision Support System for Online Banking Fraud Detection” presents an integrated framework combining rule-based methods and machine learning techniques for

real-time fraud detection. It highlights features such as alert generation, transaction monitoring, and visualization tools to assist analysts in identifying suspicious activities. The study demonstrates improved operational efficiency and detection capability. However, it also notes that reliance on predefined rules limits adaptability, suggesting the integration of more dynamic and intelligent models. [6]

4. METHODOLOGY

The proposed system prevents online banking fraud by combining Multi-Factor Authentication (MFA) with Risk-Based Analysis to verify user identity and analyze transaction behavior in real time. This approach not only checks whether the user is legitimate but also evaluates the risk associated with each login or transaction before granting access.

4.1. Approach

The proposed system combines Multi-Factor Authentication (MFA) with Risk-Based Analysis to detect and prevent online banking fraud. It verifies users through multiple authentication factors and analyzes transaction behavior to calculate a risk score.

4.1.1. Data Collection and User Profiling

The system collects user-related information such as login time, IP address, device ID, browser type, location, transaction amount, and transaction frequency. Using this data, the system builds a user behavior profile that represents the customer's normal banking activities. These profiles help distinguish between legitimate behavior and suspicious actions.

4.1.2. Multi-Factor Authentication (MFA)

To ensure secure access, the system verifies users through multiple authentication layers:

- Knowledge Factor: Password or PIN entered by the user.
- Possession Factor: Registered device verification using device fingerprinting.
- Biometric Factor: Fingerprint or facial recognition for additional security.
- Even if attackers obtain login credentials, they cannot easily bypass these multiple verification layers.

4.1.3. Risk Score Calculation

After authentication, the system performs risk-based analysis by comparing the current login or transaction details

with the stored user behavior profile. Several risk indicators are evaluated, including:

- Login from a new or unknown device
- Unusual login time or transaction frequency

Each factor contributes to a risk score, which determines whether the activity is normal or potentially fraudulent.

4.1.4. Fraud Detection and Decision Making

If the calculated risk score is low, the system allows the transaction normally. If the risk score is moderate, additional verification such as OTP or biometric confirmation is requested. If the risk score is high, the system blocks the transaction and flags it as suspicious for further investigation.

4.1.5. Alert Generation and Security Response

When suspicious activity is detected, the system immediately sends alerts to the user and the bank's fraud monitoring system. This allows quick action such as temporarily freezing the account, verifying the user's identity, or reversing unauthorized transactions.

4.1.6. Continuous Monitoring and System Improvement

The system continuously updates user profiles based on new transaction data. Over time, this improves the accuracy of fraud detection and helps adapt to evolving fraud techniques used by cybercriminals.

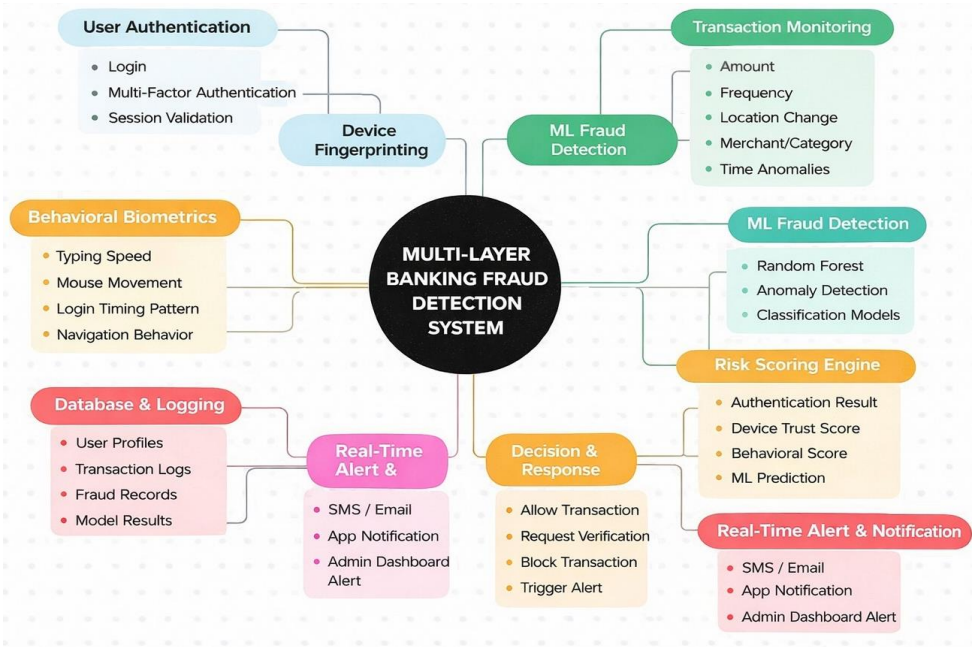


Fig 4.2: Multi – Layer Banking Fraud Detection System.

4.3. Multi-Layer Banking Fraud Detection System (Explanation)

1. User Authentication: The user first logs in using multi-factor authentication (password, OTP, or biometric). This ensures that only authorized users access the account.

2. Device Fingerprinting: The system identifies the user's device using details like browser, operating system, and network information to detect unknown or suspicious devices

3. Behavioral Biometrics: It analyzes user behavior such as typing speed, mouse movement, login time, and navigation patterns to verify if the activity matches the genuine user.

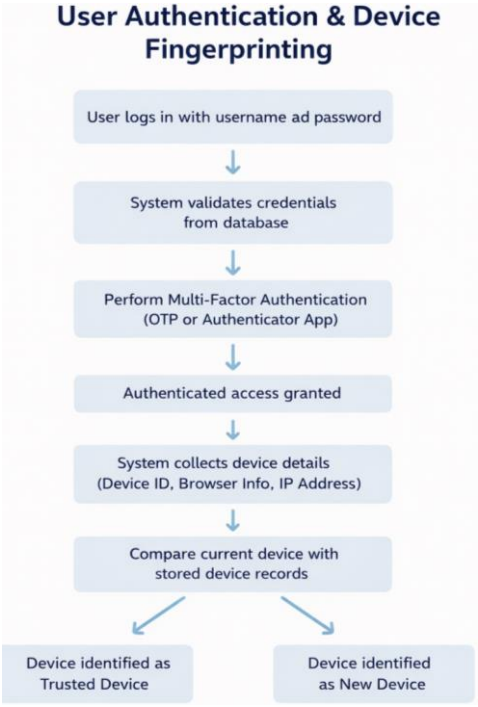
4. Transaction Monitoring: The system checks transaction details like amount, frequency, location change, merchant category, and unusual timing to detect abnormal activities.

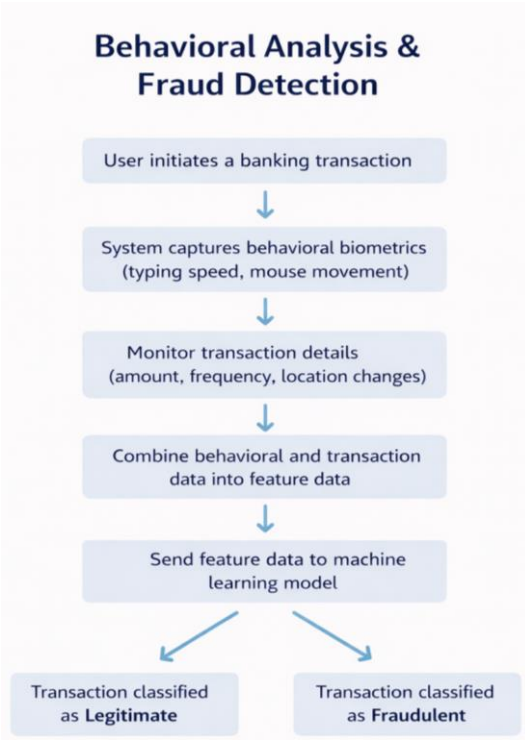
5. Machine Learning Fraud Detection; ML models such as Random Forest and anomaly detection algorithms analyze the data and predict whether a transaction is normal or fraudulent.

6. Risk Scoring Engine: A risk score is calculated based on authentication results, device trust level, user behavior, and ML predictions.

7. Decision & Response: Based on the risk score, the system may allow the transaction, request additional verification, or block the transaction.

8. Alerts & Logging: If fraud is suspected, real-time alerts are sent via SMS, email, or app notification, and all activities are stored in the database for monitoring.





Main Modules

1. Smart User Authentication

Instead of relying only on passwords, the system uses:

1. Login credentials 2. OTP-based verification 3. Session validation

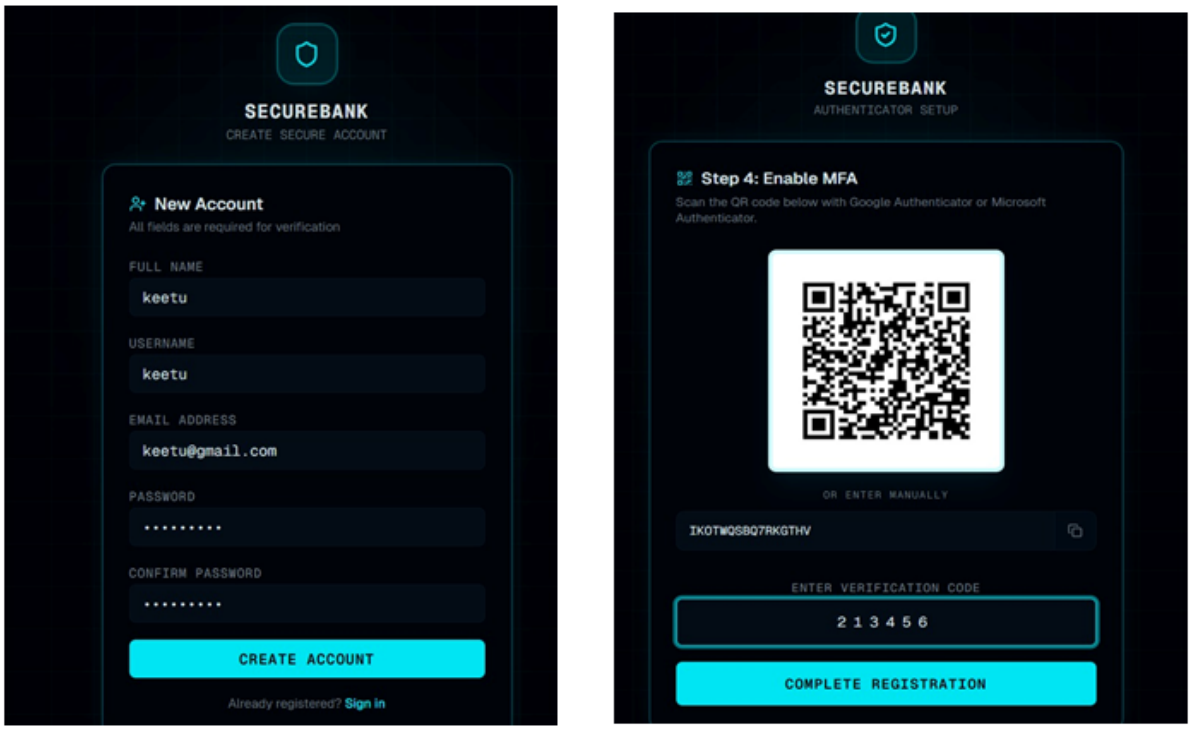


Fig 4.3.1: Sign up page Multi factor Authentication.

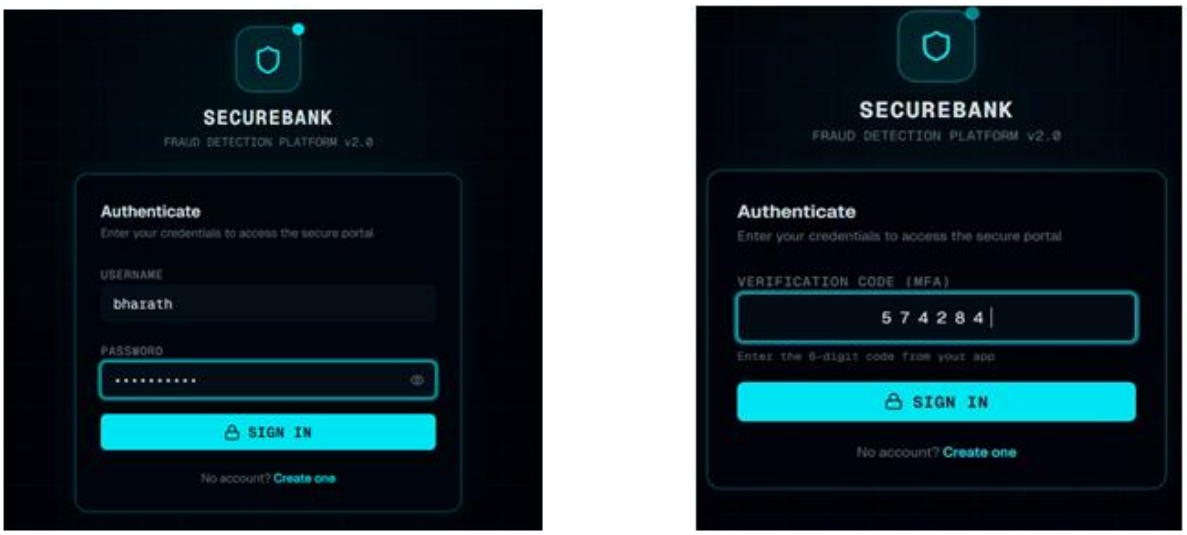


Fig 4.3.2: Login page Multi factor Authentication

2. Real-Time Transaction Monitoring

Every transaction is captured and analysed instantly based on:

i. Transaction amount ii. Time and frequency iii. Location and device

This module acts as the first checkpoint for anomaly detection.

3. Machine Learning–Driven Fraud Detection

At the core of the system:

- A Random Forest model is trained on transaction patterns
- It detects hidden relationships and unusual behaviors
- Outputs: Normal, Suspicious, Fraudulent

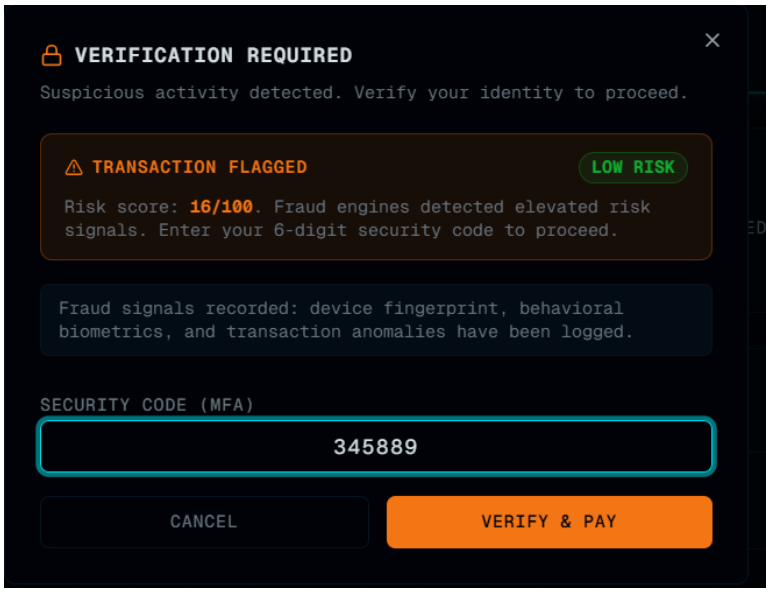


Fig 4.3.3: Transaction Monitoring.

4. Risk-Based Decision Engine

Each transaction is assigned a dynamic risk score:

- Low risk → Allowed
- Medium risk → Additional verification
- High risk → Blocked

This approach makes the system adaptive rather than rigid.

5. Alert and Response System

When fraud is detected:

- Instant alerts are sent to users
- Admin dashboard logs suspicious activity
- System can block or delay transactions

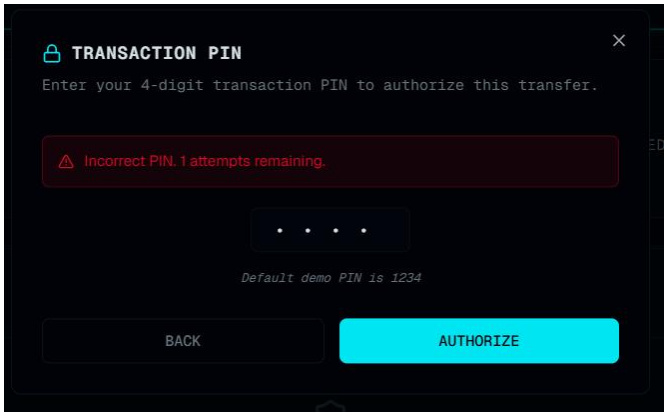


Fig 4.3.4: Risk-Based Detection.

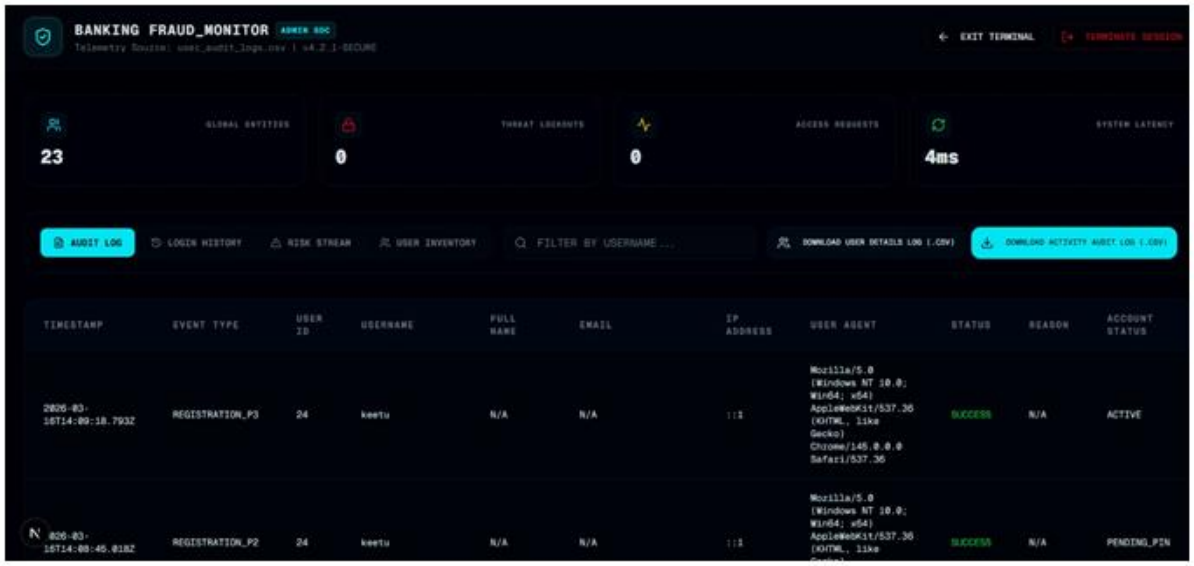


Fig 4.3.5. Audit Log

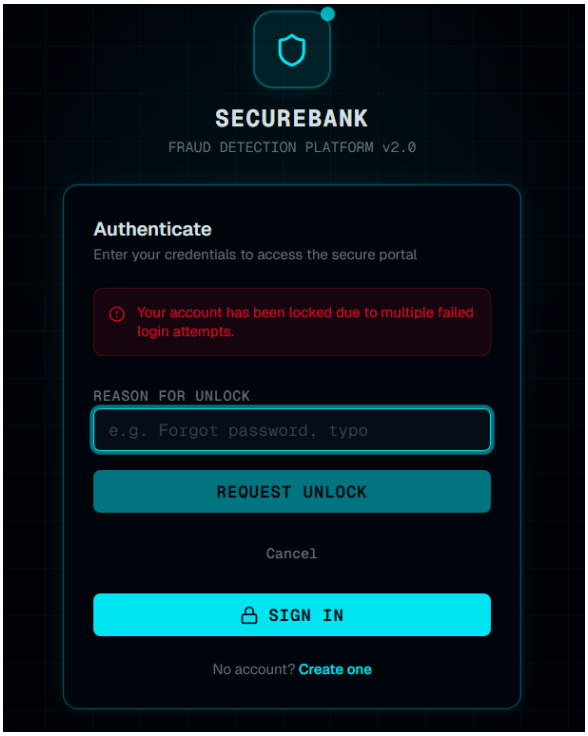


Fig 4.3.6. Account unlock request.

Fig 4.3.7. Admin Unlocking the Account.

RESULTS AND DISCUSSION

The proposed multi-layer fraud prevention system was evaluated using transaction datasets containing both legitimate and fraudulent records to assess its effectiveness in real-world scenarios. The Random Forest–based classification model achieved high detection performance, demonstrating improved accuracy, precision, recall, and F1-score compared to traditional rule-based and single-layer approaches. The incorporation of behavioural biometrics enabled continuous authentication, allowing the system to detect anomalies in user behaviour even after successful login. Additionally, device fingerprinting contributed to

identifying suspicious access attempts from unrecognized or inconsistent devices. The implementation of real-time risk scoring allowed dynamic decision-making, where transactions were either approved, flagged for additional authentication, or blocked based on the computed risk level. This significantly reduced the response time to potential fraud incidents. The system also showed a noticeable reduction in false positive rates, thereby minimizing disruption to legitimate users and improving overall user experience. Furthermore, adaptive learning mechanisms effectively addressed concept drift by updating the model with new transaction patterns, ensuring sustained detection performance over time. Comparative analysis indicates that the integration of multiple security layers enhances robustness against various types of fraud, including account takeover and transaction manipulation. However, the system introduces moderate computational overhead due to continuous monitoring and frequent model updates. Despite this limitation, the overall performance demonstrates a favorable balance between security, accuracy, and usability. The results validate that the proposed framework is scalable, reliable, and suitable for deployment in modern digital banking environments.

CONCLUSION

The proposed multi-layer fraud prevention system enhances digital banking security by integrating Multi-Factor Authentication, device fingerprinting, behavioral biometrics, and machine learning–based transaction analysis. Using a Random Forest model, it effectively detects fraudulent activities by analyzing both transactional and contextual data. Real-time risk scoring and adaptive authentication enable dynamic, context-aware responses to suspicious behavior. Continuous learning mechanisms ensure the system remains robust against evolving fraud patterns. Despite moderate computational overhead, it maintains a strong balance between security, accuracy, and user experience. Overall, the framework is scalable, reliable, and easily integrable, making it well-suited for modern banking environments.

FUTURE SCOPE

The system can be enhanced by integrating advanced machine learning and deep learning models to improve fraud detection accuracy. It can be extended to support real-time cross-bank fraud detection and data sharing for better security. Future improvements may include the use of blockchain technology for secure and transparent transactions. The system can also

incorporate adaptive learning to handle evolving fraud patterns. Additionally, integration with mobile banking apps and IoT-based authentication can further strengthen security.

REFERENCES

1. S. Das, A. Banerjee, and R. Gupta, "Multi-factor authentication techniques for secure online banking systems," *International Journal of Information Security*, vol. 21, no. 2, pp. 145–158, 2022.
2. M. Conti, L. V. Mancini, and R. Spolaor, "Behavioral biometrics for continuous authentication in financial services," *IEEE Security & Privacy*, vol. 20, no. 1, pp. 30–39, 2022.
3. Dal Pozzolo, O. Caelen, and G. Bontempi, "Credit card fraud detection using machine learning: A survey," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 8, pp. 3784–3797, 2018.
4. S. Jurgovsky et al., "Sequence classification for credit-card fraud detection using recurrent neural networks," *Expert Systems with Applications*, vol. 100, pp. 234–245, 2018.
5. J. Gama, I. Žliobaitė, A. Bifet, M. Pechenizkiy, and A. Bouchachia, "A survey on concept drift adaptation," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–37, 2014.
6. M. Carcillo, Y.-A. Le Borgne, O. Caelen, and G. Bontempi, "Streaming active learning strategies for real-life credit card fraud detection: Assessment and visualization," *International Journal of Data Science and Analytics*, vol. 5, no. 4, pp. 285–300, 2018.
7. F. Carcillo, Y.-A. Le Borgne, O. Caelen, and G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection," *Information Sciences*, vol. 557, pp. 317–331, 2021.
8. Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit card fraud detection using hidden Markov model," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1, pp. 37–48, 2008.
9. V. J. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artificial Intelligence Review*, vol. 22, no. 2, pp. 85–126, 2004.
10. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90–113, 2016.
11. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.

12. N. Carneiro, G. Figueira, and M. Costa, “A data mining based system for credit-card fraud detection in e-tail,” *Decision Support Systems*, vol. 95, pp. 91–101, 2017.
13. E. Kirda and C. Kruegel, “Protecting users against phishing attacks using machine learning,” *Computer Networks*, vol. 51, no. 16, pp. 4579–4594, 2007.
14. R. Perols, “Financial statement fraud detection: An analysis of statistical and machine learning algorithms,” *Auditing: A Journal of Practice & Theory*, vol. 30, no. 2, pp. 19–50, 2011.
15. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review, 34(1), 1–14.