Volume 11, Issue 2, February – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb1354

SafeGuard: Implies Protection and Security for Bank Transaction Using Artificial Intelligence

P. G. Nemade[1]; Shraddha Ingole[2]; Khushi Sharma[3]; Radha Ghom[4]; Asmita Nandane[5]; Sejal Shinde[6]

[1]Professor
[1;2;3;4;5;6]Computer Science and Engineering Department, PRPCEM

Publication Date: 2026/03/09

Abstract: In today's digitally driven banking environment, secure and reliable financial transactions are essential for economic stability and user trust. However, the rapid growth of online banking services has also led to an increase in fraudulent activities, unauthorized access, and cyber threats. SafeGuard is an intelligent bank transaction security system designed to enhance protection and ensure secure financial operations using artificial intelligence techniques. The system employs machine learning algorithms to analyze transaction patterns, identify abnormal behavior, and detect potential fraud in real time. By examining factors such as transaction amount, frequency, time, location, and user behavior, SafeGuard provides adaptive and accurate risk assessment. The integration of data analytics, anomaly detection, and predictive modeling enables the system to continuously learn from historical transaction data and respond effectively to emerging threats. With a scalable architecture and automated decision-making mechanism, SafeGuard offers a reliable solution for strengthening banking security. This project aims to improve transaction safety, reduce financial fraud, and promote user confidence in digital banking systems through intelligent, technology-driven security measures.

Keywords: *Banking Security, Artificial Intelligence, Machine Learning, Fraud Detection, Anomaly Detection, Secure Transactions, Financial Cybersecurity.*

How to Cite: P. G. Nemade; Shraddha Ingole; Khushi Sharma; Radha Ghom; Asmita Nandane; Sejal Shinde (2026) SafeGuard: Implies Protection and Security for Bank Transaction Using Artificial Intelligence. *International Journal of Innovative Science and Research Technology,* 11(2), 2985-2989. https://doi.org/10.38124/ijisrt/26feb1354

I. INTRODUCTION

Banking transactions form the backbone of modern financial systems, enabling individuals and organizations to transfer money quickly and efficiently. With the rapid growth of digital banking services such as online payments, mobile banking, and electronic fund transfers, financial institutions now process millions of transactions every day. While this digital transformation has improved convenience and accessibility, it has also introduced serious security challenges. Cyber fraud, unauthorized transactions, identity theft, and financial scams have become increasingly common, posing significant risks to both banks and customers. Ensuring secure and trustworthy banking transactions has therefore become a critical requirement in today's technology-driven world.

In many banking systems, transaction security is still largely dependent on traditional methods such as passwords, PINs, onetime passwords, and rule-based fraud detection mechanisms. Although these approaches provide basic protection, they often fail to detect sophisticated and evolving fraud techniques. Modern attackers frequently exploit system vulnerabilities, stolen credentials, and behavioral loopholes to bypass static security rules. As a result, there is a growing need for intelligent and adaptive security solutions that can analyze transaction behavior in real time and respond effectively to potential threats.

Recent advancements in Artificial Intelligence (AI) and Machine Learning (ML) have created new opportunities for enhancing banking security. AI-based systems can analyze large volumes of transaction data and identify hidden patterns that are difficult for traditional systems to detect. Machine learning algorithms are capable of learning from historical transaction records and recognizing abnormal behavior based on factors such as transaction amount, frequency, time, location, and user activity patterns. These capabilities allow intelligent systems to detect fraud more accurately and reduce false alerts.

SafeGuard is developed with this objective in mind. It is an AI-driven bank transaction security system designed to provide enhanced protection and reliability for digital financial operations. The system continuously monitors transaction activities, extracts relevant behavioral features, and evaluates them using trained machine learning models. Based on this analysis, SafeGuard determines the risk level of each transaction and takes appropriate actions, such as approving

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb1354

genuine transactions or blocking suspicious ones. The system also adapts over time by learning from new transaction data, making it more effective against emerging fraud patterns.

The motivation behind SafeGuard arises from the increasing demand for secure, efficient, and scalable banking security solutions in an era of digital finance. Unlike conventional systems that rely on fixed rules, SafeGuard offers a dynamic and intelligent approach to fraud detection. By integrating realtime monitoring, data analytics, and automated decision making, the system aims to strengthen transaction security while maintaining a smooth user experience.

This research paper presents the design, architecture, implementation, and evaluation of the SafeGuard system. It explains the machine learning techniques used for transaction analysis, the system workflow for fraud detection, and the performance evaluation based on accuracy and reliability. The results demonstrate the effectiveness of AI-based security mechanisms and highlight the potential of SafeGuard as a practical solution for protecting bank transactions in modern financial environments.

➢ *Objectives*

- To enhance the security of bank transactions by using artificial intelligence based techniques.
- To analyze transaction behavior and identify suspicious or fraudulent activities in real time.
- To detect unauthorized transactions by examining parameters such as transaction amount, frequency, time, and user behavior.
- To reduce financial fraud and minimize losses for banks and customers.
- To improve the accuracy of fraud detection while reducing false alerts and unnecessary transaction blocks.
- To provide an adaptive security system that continuously learns from historical and new transaction data.
- To ensure safe, reliable, and seamless digital banking experiences for users.
- To integrate machine learning algorithms that make the system smarter and more effective over time.
- To monitor transaction patterns regularly and provide timely alerts for potential security threats.

II. LITERATURE REVIEW

Bank transaction security and fraud detection have been widely studied due to the rapid growth of digital banking and online payment systems. Traditional fraud detection techniques were primarily rule-based, relying on predefined thresholds and manually crafted rules. Although these systems were effective in detecting known fraud patterns, they lacked adaptability and often failed to identify new and complex fraud behaviors. Early studies emphasized statistical analysis and expert-defined rules, which resulted in high false positive rates and limited scalability.

With the advancement of Machine Learning (ML), researchers began applying supervised learning algorithms to detect fraudulent banking transactions. Support Vector Machines (SVMs) and Logistic Regression were among the earliest models used for transaction classification. Dal Pozzolo et al. demonstrated that SVM-based models could effectively classify genuine and fraudulent transactions by learning decision boundaries from historical transaction data. However, these methods required careful feature selection and struggled with highly imbalanced datasets, which are common in financial fraud scenarios.

Ensemble learning techniques such as Decision Trees and Random Forests have also been explored for fraud detection in banking systems. Decision Trees provide interpretable models by creating rule-based structures from transaction features such as transaction amount, transaction time, and transaction frequency. Random Forests, as ensemble models, improve robustness and reduce overfitting by combining multiple decision trees. Studies show that Random Forest-based systems achieve higher accuracy and better generalization compared to single-model approaches, making them suitable for real-time banking applications.

Recent research has focused on deep learning techniques to capture complex and non-linear transaction patterns. Neural Networks, Long Short-Term Memory (LSTM) networks, and hybrid deep learning models have been applied to sequential transaction data to detect temporal fraud patterns. These models analyze user transaction history over time and identify abnormal behavior that deviates from normal spending patterns. Although deep learning approaches provide high detection accuracy, they require large datasets and significant computational resources.

Anomaly detection techniques have also gained attention in banking security research. Unsupervised and semi-supervised learning methods such as Isolation Forests and Autoencoders are used to identify rare and unusual transaction behavior without requiring extensive labeled data. These approaches are particularly useful in detecting new and previously unseen fraud patterns. However, balancing detection sensitivity and false alert rates remains a challenge.

More recently, researchers have explored hybrid security frameworks that integrate machine learning with real-time monitoring and risk scoring mechanisms. These systems continuously evaluate transaction risk and dynamically adapt to changing fraud strategies. Studies highlight that AI-driven security systems significantly improve fraud detection accuracy, reduce financial losses, and enhance customer trust in digital banking platforms.

Based on the reviewed literature, it is evident that artificial intelligence and machine learning techniques provide effective solutions for securing bank transactions. However, challenges such as data imbalance, false positives, and system adaptability still exist. The proposed SafeGuard system aims to address these challenges by implementing adaptive machine learning models with real-time transaction analysis to enhance banking transaction security.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb1354

III. METHODOLOGY

➢ *Overview of the Methodology*

This section describes the systematic approach used to design and implement an AI-based real-time fraud detection and prevention system for banking transactions. The proposed methodology integrates data analytics, machine learning, and real-time monitoring to identify suspicious activities and prevent financial fraud before monetary loss occurs.

- *The Primary Objectives of the System are:*

✓ To learn transaction behavior from historical banking data.
✓ To analyze live transactions and identify abnormal patterns.
✓ To prevent fraud instantly through automated actions and alert mechanisms.

The overall workflow begins with data collection and ends with continuous model improvement to adapt to evolving fraud techniques.

➢ *Data Collection*

Data collection is a crucial step in fraud detection, as the effectiveness of AI models largely depends on the quality and diversity of data. The system gathers large volumes of transaction-related data from multiple banking sources, including:

- *Customer Transaction History*

✓ Login information such as IP address, device ID, and geographic location
✓ Merchant and payment gateway details
✓ Records of previously identified fraud cases

All collected data is securely stored in a protected database to ensure privacy and regulatory compliance.

For example, if a customer normally performs transactions within India but suddenly attempts a high-value transaction from another country, such behavior is flagged as potentially suspicious.

➢ *Data Preprocessing*

Raw banking data often contains noise, inconsistencies, and missing values. Therefore, preprocessing is performed before feeding the data into AI models. This step includes:

- Data Cleaning: Removing duplicate entries, correcting errors, and handling missing values.
- Data Transformation: Converting categorical attributes such as device type or location into numerical representations.
- Data Normalization: Scaling transaction values to maintain uniformity and prevent bias toward higher amounts.
- Dataset Balancing: Since fraudulent transactions are rare compared to genuine ones, techniques such as SMOTE (Synthetic Minority Oversampling Technique) are applied to balance the dataset.

Preprocessing ensures that the data is accurate, consistent, and suitable for effective model training.

➢ *Feature Extraction*

Feature extraction focuses on identifying the most relevant parameters that contribute to fraud detection. These features capture user behavior and transaction characteristics, including:

- Transaction amount
- Time and frequency of transactions
- Location of transaction
- Device and network information
- Sudden changes in spending patterns

For instance, a large number of transactions occurring within a very short time interval may indicate fraudulent activity. Selecting meaningful features improves the accuracy and reliability of the detection model.

➢ *AI Model Training*

After feature extraction, machine learning and deep learning models are trained using historical transaction data. The system employs various algorithms to classify transactions as genuine or fraudulent, such as:

- Machine Learning Models: Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines (SVM).
- Deep Learning Models: Artificial Neural Networks (ANN), Recurrent Neural Networks (RNN), and Autoencoders.

During training, the models learn patterns and relationships within the data that distinguish normal transactions from fraudulent ones. For example, a Random Forest model can learn decision rules based on transaction amount, location, and frequency to assess risk levels.

➢ *Real-Time Fraud Detection*

Once trained, the AI model is deployed within the bank's live transaction processing system. Each incoming transaction is evaluated in real time and assigned a fraud risk score based on learned patterns.

- Low risk score: Transaction is approved automatically.
- High risk score: Transaction is marked as suspicious and forwarded for preventive action.

This stage requires high speed and accuracy, as banking systems process millions of transactions continuously.

➢ *Fraud Prevention and Alert Mechanism*

Fraud detection is effective only when combined with immediate preventive actions. Based on the fraud risk score, the system performs automated responses:

- Low Risk: Transaction proceeds without interruption.
- Medium Risk: Additional authentication such as OTP, biometric verification, or facial recognition is requested.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb1354

- High Risk: Transaction is blocked instantly to prevent financial loss.

- *Simultaneously, Alert Notifications are Sent:*

✓ To customers via SMS, email, or mobile application notifications.
✓ To the bank's security team for further investigation and response.

This dual alert mechanism ensures transparency, quick action, and enhanced customer trust.

➢ *Continuous Learning and Model Improvement*

Fraud patterns evolve rapidly, making continuous learning an essential component of the system. The proposed methodology incorporates a feedback loop where:

- Newly identified fraud cases are added to the dataset.
- The AI models are retrained periodically using updated data.
- Performance metrics such as false positives and detection accuracy are analyzed.
- Improved models are redeployed into the live system.

This adaptive learning process enables the system to handle emerging fraud techniques, changes in customer behavior, and increasing transaction volumes effectively.

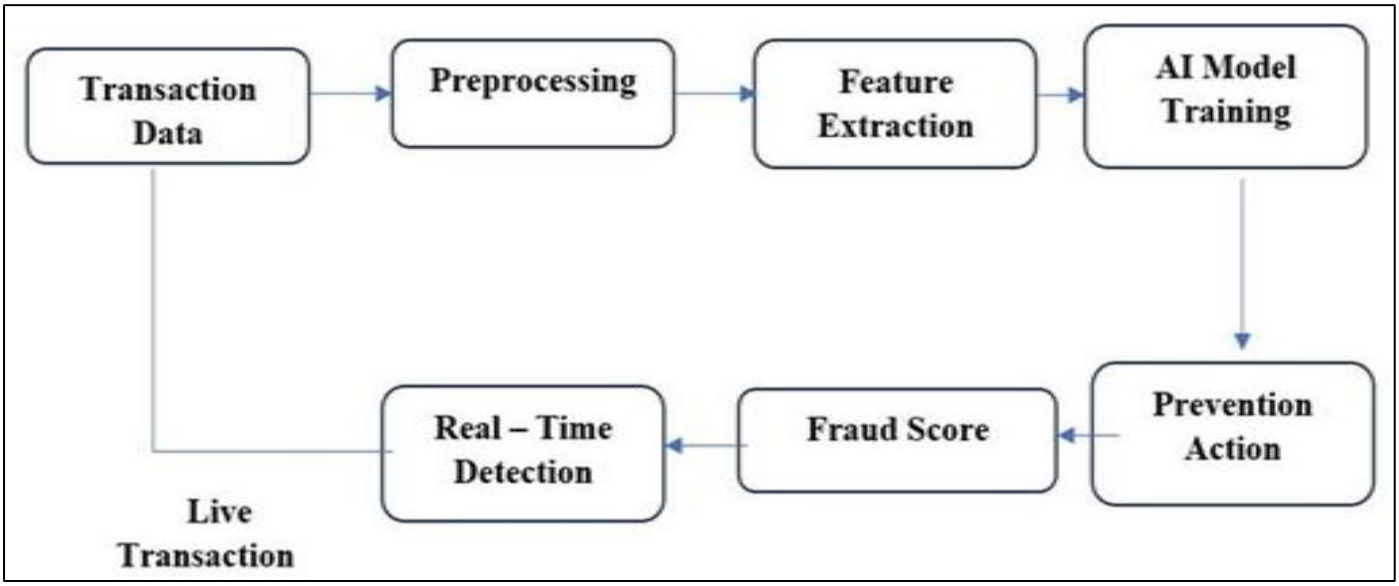

Fig 1 Methodology Block Diagram

IV. CONCLUSION

The SafeGuard project demonstrates how artificial intelligence can significantly enhance the security of modern banking transactions. With the rapid growth of digital banking, users face increasing risks such as fraud, unauthorized access, and cyber-attacks. SafeGuard addresses these challenges by intelligently monitoring transaction behavior and identifying suspicious activities in real time. By analyzing transaction patterns, user behavior, and historical data, the system is able to distinguish between genuine and fraudulent transactions with improved accuracy.

The proposed system reduces dependency on traditional rulebased security mechanisms by incorporating machine learning models that continuously learn and adapt to new fraud patterns. This adaptive nature makes SafeGuard more effective against evolving cyber threats. In addition, features such as instant alerts, transaction blocking, and administrative monitoring ensure timely response and improved trust in digital banking systems.

SafeGuard not only improves transaction security but also enhances user confidence by providing a secure and reliable banking environment. The system is scalable, cost-effective, and suitable for real-world banking applications. With future enhancements such as biometric authentication, blockchain integration, and advanced deep learning models, SafeGuard can evolve into a more robust and intelligent banking security framework. Overall, the project highlights how AI-driven solutions can play a vital role in safeguarding financial transactions and strengthening the digital banking ecosystem.

REFERENCES

[1]. N. Dalal and A. Kumar, "Artificial Intelligence Techniques for Fraud Detection in Banking Systems," IEEE Access, vol. 11, pp. 45621–45632, 2024.
[2]. S. Bhattacharya, K. Maddikunta, and S. R. Kaluri, "A Review of Machine Learning-Based Financial Fraud Detection," IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 5, pp. 1987–2002, May 2023.
[3]. A. K. Jain and P. Singh, "Secure Online Banking Using AI and Behavioral Analysis," Proc. IEEE Int. Conf. on Advanced Computing, pp. 112–117, Dec. 2023.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26feb1354

[4]. M. Omar, R. Mahmoud, and T. Hassan, "Credit Card Fraud Detection Using Machine Learning Algorithms," IEEE Access, vol. 10, pp. 78543–78555, 2022.
[5]. V. Patil and S. Kulkarni, "AI-Based Transaction Monitoring System for Banking Security," International Journal of Computer Applications, vol. 185, no. 12, pp. 21–26, 2024.
[6]. R. Agrawal and S. Sharma, "An Intelligent Framework for Real-Time Fraud Detection in Digital Payments," IEEE Conference on Data Science and Analytics, pp. 65–70, 2023.
[7]. K. Gupta, A. Verma, and N. Mehta, "Machine Learning Approaches for Secure Financial Transactions," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 3421–3432, 2023.
[8]. P. K. Mishra and R. Tiwari, "Cybersecurity Challenges in Online Banking and AI-Based Solutions," IEEE Access, vol. 12, pp. 10211–10222, 2024.