IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 12, Issue 03, March 2026 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2025.v1203.10

Financial Fraud Detection

Ashish G
Assistant Professor,Department of Information Technology
Sengunthar Engineering College (Autononomous), Tiruchengode, India
gashish.it@scteng.co.in
https://orcid.org/0009-0008-1007-5010
Janani S,Priya B,Priyadharshini N,Swathi S
Department of Information Technology
Sengunthar Engineering College (Autononomous), Tiruchengode, India
jananisit2026@scteng.co.in,priyabit2026@scteng.co.in,
priyadharshininit2026@scteng.co.in,swathisit2026@scteng.co.in

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.12/Issue03/ISMR26.MRIS10089
Research Article Open Access| Double-Blind Peer-Reviewed| Article ID: IJIRIS/RS/Vol.12/Issue03/ISMR26.MRIS10089
Received: 31, January 2026, Revised: 14, February 2026, Accepted: 17, March 2026, Published Online: 25,March 2026.
https://www.ijiris.com/volumes/Vol12/iss-03/10.ISMR26.MRIS10089.pdf
Article Citation: Ashish,Janani,Priya,Priyadharshini,Swathi(2026),Financial Fraud Detection,IJIRIS: International Journal of Innovative Research in Information Security, Volume 12, Issue 03 of 2026 pages 132-136
Doi:> https://doi.org/10.26562/ijiris.2026.v1203.10
BibTeX Key: Ashish@2026Financial
IJIRIS papers should be cited as IJIRIS (International Journal of Innovative Research in Information Security, AM Publications, India 2026, ISSN 2349-7017, https://doi.org/10.26562/ijiris.2026.v1203.10 The journal's official abbreviation is IJIRIS. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: Financial institutions face significant losses due to New Bank Account (NBA) fraud, which has become increasingly prevalent with the rise in online banking usage. Detecting such fraud is challenging because the datasets are highly imbalanced non-fraudulent instances vastly outnumber fraudulent ones. This imbalance often causes traditional machine learning models to over look minority class instances (i.e.,the actual fraud cases). To address these challenges, this project proposes a robust fraud detection system using Random Forest and Extreme Gradient Boosting (XGBoost) algorithms. These ensemble learning techniques are well-suited for handling imbalanced classification problems and can effectively distinguish between legitimate and fraudulent transactions. The Bank Account Fraud (BAF) dataset is utilized to train and validate the model. The model leverages risk-return features, transaction behavior and account characteristics to detect anomalies. Data preprocessing includes normalization, handling class imbalance using techniques like SMOTE (Synthetic Minority Over-sampling Technique), and feature engineering. Random Forest, a bagging method, is used for it ability to reduce variance and avoid over fitting. XG Boost ,a boosting method, enhances detection performance by focusing on misclassified instances in successive iterations. The proposed system achieves a True Positive Rate (TPR) of 0.95 and a detection accuracy of 94.06%, significantly improving fraud identification without compromising on false positive control. This approach provides a reliable and scalable fraud detection framework, built using Django for the web application and Python for model development, enabling effective fraud risk management in real time.
Keywords: Financial Fraud Detection, Machine Learning, Transaction Monitoring, Data Analysis, Fraud Prevention, Banking Security, Predictive Modeling, Pattern Recognition, Risk Analysis, Real-Time Monitoring.

1. INTRODUCTION

Fraud is defined as the intentional deception or concealment of a substantial truth with the purpose of influencing someone to action it to their harm (as defined by the American Institute of Certified Public Accountants). Fraud is something you've either witnessed firsthandorheardaboutfromafriend.You'veprobablyheardstoriesaboutpeoplehaving their identities stolen. That's use of some type. People who steal other people's identities use their fictitious identities to make transactions using the personal information of victim, such as their bank account and credit card. Many victims of identity theft have lost tens of thousands of dollars in addition to their excellent credit ratings. Fraud is a severe offence that must not be taken lightly. Fraud is a punishable offence in most regions, with varying degrees of punishment. The most prevalent methods of card theft include stealing the card before it is received by the owner, obtaining card details from the owner via phone calls, sending in appropriate links to the owner's mobile phone in order to obtain card details, and appropriating missing cards The most prevalent methods of card theft include stealing the card before it is received by the owner, obtaining card details from the owner via phone calls, sending inappropriate links to the owner's mobile phone in order to obtain card details, and appropriating missing cards.

TRANSACTION MONITORING

Transaction monitoring is a critical component of fraud detection systems. It involves continuously analyzing financial transactions to detect unusual patterns or suspicious activities. The system monitors transaction details such as transaction amount, transaction time, and location. If any abnormal behavior is detected, the system generates alerts to prevent fraudulent transactions.

For example, If a user normally makes small transactions in one city but suddenly a very large transaction occurs from another location, the system may consider this activity suspicious. In such cases, the system can send an alert, temporarily block the transaction, or request additional verification from the user. Transaction monitoring helps financial institutions detect fraud early, prevent financial losses, and protect customer accounts.

DATA ANALYSIS

Data analysis is the process of examining, organizing, and interpreting data to discover useful information and patterns. In a Financial Fraud Detection System, data analysis helps identify unusual transaction patterns that may indicate fraudulent activity. Financial institutions generate a large amount of transaction data every day, including information such as transaction amount, transaction time, user details, location, and payment method. Data analysis techniques are used to study this data and detect patterns in user behaviour. By analysing historical transaction data, the system can understand what is considered normal transaction behaviour for a user. If a transaction significantly differs from the usual pattern, it may be marked as suspicious. For example, if a user typically performs small transactions but suddenly makes a very large Transaction or performs multiple transactions in a short time, the system may flag it as potential fraud.

MACHINE LEARNING IN FRAUD DETECTION

Machine learning is a technology that enables computers to learn from data and make decisions without being explicitly programmed. In financial fraud detection systems, machine learning is used to analyse large volumes of transaction data and identify patterns that may indicate fraudulent activities. Traditional fraud detection systems often rely on fixed rules to detect suspicious transactions. However, these rule-based systems may fail to identify new or complex fraud patterns. Machine learning improves this process by learning from historical transaction data and automatically detecting unusual behaviour. In a fraud detection system, machine learning algorithms analyse various transaction features such as transaction amount, transaction frequency, location, time of transaction, and user behaviour. Based on these factors, the system can classify transactions as legitimate or fraudulent.

SECURITY AND RISK MANAGEMENT

Security and risk management are important aspects of a financial fraud detection system. They focus on protecting financial transactions and minimizing the risks associated with fraudulent activities. With the rapid growth of digital banking and online payments, ensuringsecurefinancialsystemshasbecomeessentialforfinancialinstitutions.Security measures are implemented to protect sensitive financial data and prevent unauthorized access to banking systems. These measures may include user authentication, encryption, secure databases, and access control mechanisms. By implementing strong security practices, financial institutions can safeguard customer information and maintain the integrity of transaction data.

2. LITERATURE REVIEW

Intelligent fraud detection in financial statements uses machine learning and data mining techniques to identify fraudulent activities. Traditional methods like manual audits and rule-based systems are often slow and less effective. Modern approaches analyze large financial datasets to detect unusual patterns and improve fraud detection. However, challenges remain, such as adapting to changing fraud methods and integrating different data sources for accurate analysis. These intelligent systems help protect businesses, investors, and financial markets from financial fraud.

ADVANCEMENTS IN FINANCIAL FRAUD DETECTION TECHNOLOGIES

With the rapid growth of digital banking and online payment systems, financial fraud has become a major challenge for financial institutions worldwide. Traditional fraud detection methods relied mainly on manual monitoring and rule-based systems, which were limited in their ability to detect complex and evolving fraud patterns. Recent technological advancements have significantly improved the effectiveness of fraud detection systems. Machine learning and data mining techniques are widely used in modern financial fraud detection systems. These technologies analyze large volumes of transaction data to identify hidden patterns and anomalies that may indicate fraudulent activities. Algorithms such as Logistic Regression, Decision Trees, and Random Forest are commonly used to classify transactions as legitimate or fraudulent.

TRANSACTION MONITORING AND ANOMALY DETECTION

Transaction monitoring plays a crucial role in financial fraud detection by continuously observing financial activities and identifying suspicious patterns. With the increasing number of digital transactions, financial institutions require advanced systems that can analyze large volumes of data quickly and accurately. Modern fraud detection systems use automated monitoring tools to track transaction details such as transaction amount, location, frequency, and time. Anomaly detection techniques are widely used to identify unusual or abnormal transaction behavior. These techniques analyze historical transaction data to understand normal user behavior and detect deviations from typical patterns. For example, if a user suddenly performs multiple high-value transactions within a short period or initiates a transaction from an unfamiliar location, the system may flag it as suspicious.

MACHINE LEARNING TECHNIQUES FOR FRAUD DETECTION

Machine learning techniques have become an essential part of modern financial fraud detection systems. These techniques enable systems to analyse large volumes of transaction data and identify hidden patterns that may indicate fraudulent activities. Unlike traditional rule-based systems, machine learning models can learn from historical data and continuously improve their detection accuracy. Several machine learning algorithms are commonly used in fraud detection, including Logistic Regression, Decision Tree, Random Forest, and Support Vector Machines. These algorithms analyze various transaction features such as transaction amount, transaction time, location, frequency, and user behavior patterns. Based on these factors, the models classify transactions as legitimate or fraudulent.

IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 12, Issue 03, March 2026 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2025.v1203.10

SECURITY MECHANISMS IN FINANCIAL FRAUD DETECTION

Security mechanisms play a vital role in financial fraud detection systems by protecting sensitive financial data and preventing unauthorized access to financial platforms. As digital banking and online transactions increase, financial institutions must implement strong security measures to ensure safe and reliable financial operations. Modern financial systems use various security techniques such as encryption, multi-factor authentication, and secure access control to protect user accounts and transaction data. Encryption ensures that sensitive information such as account numbers and transaction details are securely transmitted and stored, preventing unauthorized users from accessing the data.

CONSOLIDATING RESEARCH INSIGHTS FOR FINANCIAL FRAUD DETECTION SYSTEM

The research studies and technological advancements discussed in the previous sections highlight the importance of integrating data analysis, transaction monitoring, machine learning techniques, and security mechanisms in a unified financial fraud detection system. While many existing solutions focus on individual aspects of fraud detection, a comprehensive system that combines these technologies can significantly improve fraud prevention and financial security. Modern fraud detection systems aim to analyze large volumes of transaction data in real time, identify suspicious patterns, and prevent fraudulent activities before financial losses occur. By integrating machine learning algorithms with real-time transaction monitoring, financial institutions can detect anomalies more accurately and respond quickly to potential threats

3. EXISTING SYSTEM

In the existing credit card fraud detection systems, traditional rule-based and statistical methods are primarily used to identify suspicious transactions. These systems rely on predefined rules such as purchase amount limits, unusual spending locations, or sudden transaction spikes. While these methods work for basic fraud detection, they lack the flexibilitytoadapttonewandevolvingfraudpatterns.Manualinvestigationplaysamajor role in verifying alerts, which makes the process slow and less efficient. Additionally, many legacy systems suffer from poor utilization of large amounts of transactional data. Due to limited analytical capabilities, they often fail to detect hidden patterns or sophisticated fraudulent behaviours. As fraudsters become more advanced, existing methods struggle to identify real-time fraud occurrences, resulting in delayed responses and increased financial damage.

4. PROPOSED SYSTEM

The proposed credit card fraud detection system utilizes advanced machine learning techniques to automatically identify fraudulent transactions with high accuracy. By using real-world transaction data that includes both legitimate and fraudulent records, the system captures hidden patterns through feature engineering and PCA based components. Data preprocessing techniques like normalization, duplicate removal, and SMOTE are applied to enhance data quality and improve model performance, especially in cases of class imbalance. This system employs ensemble-based classifiers such as Random Forest and XG Boost to efficiently learn from historical transaction behaviour. These models help reduce false alarms while accurately detecting subtle fraud activities. Performance evaluation metrics like Precision, Recall, F1-Score, and ROC-AUC ensure that the most reliable and optimized model is selected for deployment in real time fraud prevention scenarios.

DATA COLLECTION AND PREPROCESSING

Data collection and preprocessing are important steps in the development of a financial fraud detection system. The system requires a large amount of transaction data to analyze user behavior and detect fraudulent activities. This data is typically collected from banking systems, payment platforms, or financial transaction databases. The collected dataset usually contains various transaction details such as transaction ID, userID, transaction amount, transaction time, location, payment method, and transaction status. These features help the system understand transaction patterns and identify unusual activities that may indicate fraud.

MACHINE LEARNING MODEL FOR FRAUD DETECTION

Machine learning models play a crucial role in detecting fraudulent financial transactions. These models analyze historical transaction data and learn patterns that distinguish normal transactions from fraudulent ones. By using machine learning algorithms, the system can automatically identify suspicious activities and classify transactions as legitimate or fraudulent. In the proposed system, algorithms such as Logistic Regression, Decision Tree, and Random Forest are used to build the fraud detection model.

REAL-TIME FRAUD DETECTION AND ALERT SYSTEM

Real-time fraud detection is an essential component of the Financial Fraud Detection System. It enables the system to analyze financial transactions immediately as they occur and identify suspicious activities without delay. By monitoring transactions in real time, financial institutions can prevent fraudulent transactions before they are completed. When a user performs a financial transaction, the system automatically collects important details such as transaction amount, time, location, and user behavior patterns. These details are analyzed using the trained machine learning model. If the system detects unusual patterns or anomalies that indicate possible fraud, the transaction is flagged as suspicious.

DATA VISUALIZATION AND REPORTING

Data visualization and reporting are important components of the Financial Fraud Detection System. These features help financial institutions understand transaction patterns, monitor suspicious activities, and analyze fraud trends more effectively. By presenting complex transaction data in a clear and visual format, the system makes it easier for administrators and analysts to identify potential fraud. The system generates various reports based on transaction data, including the number of transactions, suspicious transaction alerts, and fraud detection results.

IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 12, Issue 03, March 2026 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2025.v1203.10

These reports provide valuable insights into user behavior and help organizations monitor financial activities efficiently.

SYSTEM PERFORMANCE AND BENEFITS

The Financial Fraud Detection System is designed to improve the efficiency, accuracy, and security of financial transaction monitoring. By integrating data analysis, machine learning algorithms, and real-time monitoring, the system can detect suspicious activities quickly and reduce the risk of financial fraud.

ADVANCED ANALYTICS AND DECISION SUPPORT

Advanced analytics and decision support systems play an important role in improving the effectiveness of financial fraud detection. By analyzing large volumes of financial transaction data, the system can identify patterns, trends, and unusual activities that may indicate fraudulent behavior. The Financial Fraud Detection System uses analytical techniques to evaluate transaction history, customer behavior, and risk levels associated with different transactions. These insights help financial institutions understand fraud patterns and take preventive actions before significant financial losses occur.

EXPECTED OUTCOMES AND BENEFITS

The implementation of the Financial Fraud Detection System is expected to provide several significant benefits to financial institutions and digital payment platforms. By integrating data analysis, machine learning algorithms, and real-time monitoring, the system improves the ability to detect and prevent fraudulent transactions effectively. One of the primary outcomes of the system is the early detection of suspicious financial activities. By analyzing transaction patterns and identifying unusual behavior, the system can quickly detect potential fraud and generate alerts for further investigation.

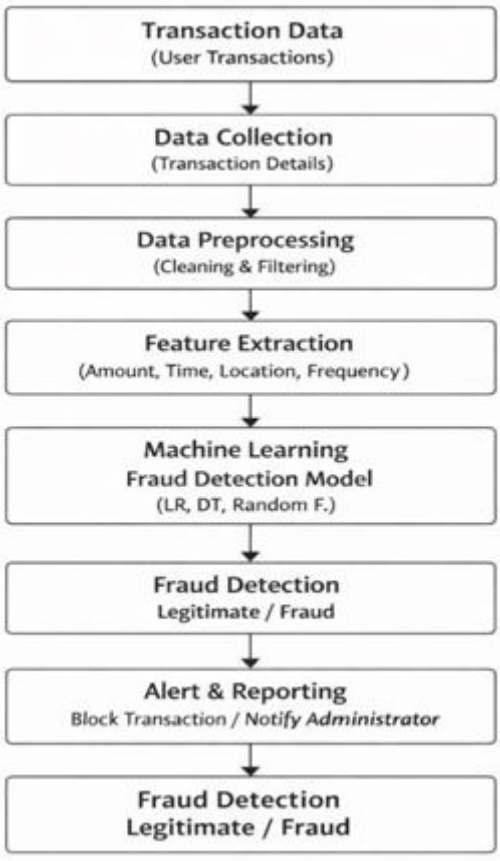

Figure1. Block Diagram

5. CONCLUSION

In this project, an efficient machine learning-based credit card fraud detection system has been successfully developed to overcome the challenges faced by traditional fraud monitoring techniques. By utilizing a reliable dataset from the Kaggle platform, the system learns complex and hidden patterns in transactional behaviour that are not easily identified through manual or rule-based methods. Data preprocessing techniques such as normalization, duplicate removal, and class balancing significantly improve the quality and usability of the transaction data, ensuring a strong foundation for model training. The application of advanced classifiers like Random Forest and XG Boost enables the system to classify and detect fraudulent transactions with high accuracy and robustness. These models are capable of adapting to dynamic fraud patterns and significantly reducing false positives. Performance evaluation using metrics such as Precision, Recall,F1-Score,and ROC-AUC demonstrates the effectiveness of the proposed method in distinguishing legitimate transactions from fraudulent ones, even in highly imbalanced datasets

6. FUTUREWORK

Although the proposed system demonstrates strong performance in fraud detection, there are several future enhancements that can further improve its efficiency and adaptability.

One potential improvement is integrating real-time data streaming from banking systems, which would allow the model to flag suspicious transactions instantly before financial damage occurs. Additionally, more advanced machine learning algorithms, including deep learning models such as LSTMs and Auto encoders, can be incorporated to detect complex fraud patterns and behaviour changes over time. Another enhancement is the implementation of adaptive learning capability, where the model continuously updates itself with new fraud data. Fraud techniques evolve rapidly, and a self-learning mechanism will ensure the system remains effective against emerging fraud activities. Furthermore, securing sensitive financial data with privacy-preserving techniques like federated learning and differential privacy can make the system suitable for large-scale deployment across multiple banks without data sharing concerns. Finally, adding explainable AI (XAI) methods will help financial analysts better understand why a transaction was flagged as fraudulent, enabling more trust and transparency in decision- making.Integratinggraphicaldashboardsforinteractivevisualization,alertnotifications, and automated reporting can enhance user experience for banking security teams. With these improvements, the system can become a fully intelligent, scalable, and industry- ready solution for global financial fraud prevention.

REFERENCES

1. Andrea,D.,DalPozzolo,A.,Sleeman,L.,&Bontempi,G.CreditCardFraud Detection using Adversarial Oversampling.