International Journal for Modern Trends in Science and Technology
Volume 12, Issue 06, pages 210-215.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue06.html
DOI: https://doi.org/10.5281/zenodo.20739531

Automated Fraud Detection System for Secure Online Transactions

Raja Kondaveti, Tirumani Prem Teja, Kethineedi Gnana Prasanna, Mangina Om Lakshmi Naga Harshitha

Department of Information Technology Swarnandhra College of Engineering & Technology, Seetharamapuram, Narsapur, Andhra Pradesh, INDIA.

To Cite this Article
Raja Kondaveti, Tirumani Prem Teja, Kethineedi Gnana Prasanna & Mangina Om Lakshmi Naga Harshitha (2026). Automated Fraud Detection System for Secure Online Transactions. International Journal for Modern Trends in Science and Technology, 12(06), 210-215. https://doi.org/10.5281/zenodo.20739531

Article Info
Received: 16 May 2026; Revised: 07 May 2026; Accepted: 12 June 2026.

KEYWORDS

Fraud Detection, Machine Learning, Online Transactions, Spring Boot, Data Analytics, Cybersecurity, Anomaly Detection, Financial Security

ABSTRACT

With the rapid growth of digital payment systems, online transactions have become an integral part of daily life. However, this growth has also led to a significant increase in fraudulent activities, resulting in financial losses and security challenges. Traditional rule-based fraud detection systems are no longer sufficient to detect complex and evolving fraud patterns. To address this issue, this project proposes an Automated Fraud Detection System for Secure Online Transactions that leverages data-driven and machine learning techniques to identify suspicious activities effectively.The system analyzes multiple transaction parameters, including transaction amount, time, location, and user behavior, to classify transactions as either genuine or fraudulent. It is developed using Java, Spring Boot, HTML, Thymeleaf, MySQL, and machine learning algorithms to ensure scalability and real-time processing. The architecture includes key modules such as user authentication, transaction processing, fraud detection engine, and an interactive dashboard for monitoring and analysis. The system provides real-time fraud detection results along with visual insights such as transaction statistics, risk levels, and alerts for suspicious activities.The proposed solution enhances transaction security by enabling early detection of fraudulent behavior, reducing financial losses, and minimizing manual intervention. It can be effectively deployed in banking systems, e-commerce platforms, and online payment applications to improve reliability, trust, and overall security in digital transactions.

1. INTRODUCTION

In today's digital era, online transactions have become a common part of everyday life. People use online platforms for banking, shopping, and money transfers due to their convenience and speed. However, with the rapid growth of digital payments, the risk of fraud has also increased significantly. Fraudulent activities such as unauthorized access, suspicious transactions, and

identity misuse can cause serious financial losses.Traditional systems that rely on fixed rules are not effective in detecting modern and complex fraud patterns. Therefore, there is a need for an intelligent system that can analyse user behaviour and detect fraud automatically. This project presents a Fraud Detection System for Online Transactions that monitors transaction data, identifies suspicious patterns, and provides real-time decisions.

The system includes features such as user authentication, transaction monitoring, fraud detection engine, and a dashboard for analysis. It classifies transactions as genuine or fraudulent and provides alerts to improve security. The system is developed using Spring Boot, Java, HTML, Thyme leaf, MySQL, and machine learning techniques, ensuring efficient processing and accurate detection. The dashboard provides insights such as transaction statistics, suspicious activity count, and risk indicators, helping users and administrators monitor fraud effectively.

a. Background of Online Transactions

Online transactions refer to the transfer of money or payment through digital platforms such as mobile banking, websites, and payment applications. These systems are widely used because they are fast, easy, and accessible from anywhere. With increasing digitalization, online transactions have become an essential part of modern financial systems.

Fig 1.1.Online Payment Illustration

b. Fraud in Online Transactions

Fraud in online transactions occurs when unauthorized or suspicious activities are performed to gain financial benefits. Examples include fake transactions, identity theft, and unusual behaviour such as large payments from unknown locations. Fraudsters continuously change their methods, making detection more difficult.

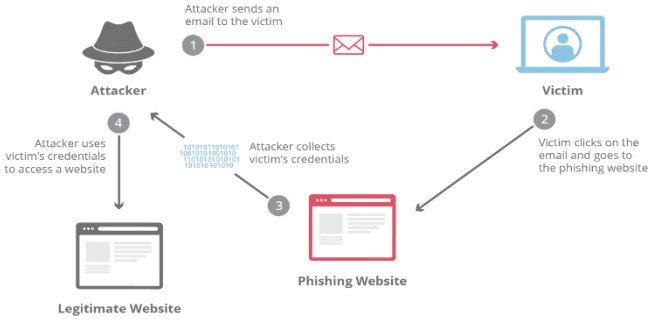

Fig 1.2.Phishing Attack Process Diagram

c. Need for Fraud Detection System

As online transactions increase, manual monitoring becomes difficult and inefficient. There is a need for an automated system that can detect fraud in real time. A fraud detection system helps in identifying suspicious activities quickly, reducing financial losses, and improving user trust. It also ensures better security for both users and financial institutions.

2 LITERATURE SURVEY

Financial fraud has become a critical issue with the rapid expansion of digital payment systems and online transactions. Traditional fraud detection methods, which rely on predefined rules, are no longer effective in identifying complex and evolving fraud patterns. According to , financial fraud is a dynamic problem that requires adaptive and intelligent detection techniques. Researchers have increasingly focused on data-driven and machine learning approaches to enhance fraud detection accuracy and efficiency. Early studies highlight the importance of anomaly detection techniques in identifying unusual transaction behaviors, which serve as indicators of potential fraud.

Several machine learning techniques have been proposed for fraud detection, including supervised and unsupervised learning models. Studies show that algorithms such as Decision Trees, Random Forest, Support Vector Machines, and Neural Networks are widely used for classifying fraudulent transactions. For instance, research demonstrates that machine learning-based credit card fraud detection systems significantly improve detection rates compared to traditional systems . Deep learning approaches, such as Variational Autoencoders and Artificial Neural

Networks, have also been applied to detect complex fraud patterns by learning hidden relationships within transaction data. Additionally, cost-sensitive learning and imbalanced data handling techniques have been introduced to address the challenge of skewed datasets, where fraudulent transactions are rare compared to genuine ones.

Recent advancements emphasize the use of real-time fraud detection systems that analyze transaction data such as amount, time, location, and user behavior. These systems incorporate anomaly detection, behavioral analysis, and risk scoring models to identify suspicious activities instantly. Research also highlights the role of hybrid approaches that combine multiple techniques, such as clustering and classification, to improve performance. Furthermore, studies indicate that integrating fraud detection systems with dashboards and visualization tools enhances monitoring and decision-making for administrators. Such systems provide insights into transaction trends, risk levels, and suspicious activities, enabling faster response and mitigation.

Despite significant progress, challenges remain in fraud detection systems, including handling large-scale data, adapting to evolving fraud strategies, and ensuring data privacy and security. Ethical considerations related to AI usage and decision-making transparency are also important factors in financial systems . Therefore, modern fraud detection systems must balance accuracy, efficiency, and security while maintaining user trust. The proposed system builds upon these existing studies by implementing a real-time, machine learning-based fraud detection model integrated with a secure and scalable web application, aiming to provide improved accuracy, reduced manual effort, and enhanced transaction security.

3 PROPOSED METHODOLOGY

The proposed system is an *Automated Fraud Detection System for Secure Online Transactions* that utilizes machine learning techniques and modern web technologies to identify fraudulent activities in real time. The system analyzes transaction data such as transaction amount, time, location, and user behavior to automatically classify transactions as either genuine or fraudulent. By moving beyond traditional rule-based approaches, the system is capable of detecting both known and unknown fraud patterns with improved accuracy and efficiency.

The system is composed of multiple modules, including a secure user authentication system, transaction monitoring module, and a machine learning-based fraud detection engine. The fraud detection engine, implemented using Weka, processes transaction data and predicts the likelihood of fraud. Additionally, an interactive dashboard is provided to display transaction statistics, risk levels, and alerts for suspicious activities, enabling effective monitoring and decision-making. The system is developed using Java and Spring Boot for backend processing, HTML and Thymeleaf for frontend design, and MySQL for database management, ensuring scalability and secure data handling.

The proposed system offers several advantages, including real-time fraud detection, reduced dependency on manual verification, and improved accuracy in identifying suspicious transactions. It helps in minimizing financial losses by detecting fraud at an early stage and provides a user-friendly dashboard for monitoring and analysis. Furthermore, the system is scalable and capable of handling large volumes of transaction data, making it suitable for applications in banking, e-commerce, and online payment platforms.

3.1 SYSTEM ARCHITECTURE

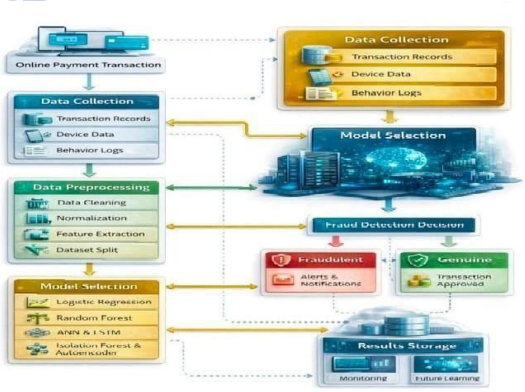

Fig 3.1 Proposed System Architecture

The system architecture illustrates how different components interact to perform real-time fraud detection efficiently. The frontend, developed using HTML and Thymeleaf, provides a user-friendly interface where users can input transaction data and view results. This data is then sent to the backend built with Spring Boot, which handles request processing and implements

the business logic of the application. The backend communicates with the machine learning model developed using Weka, which analyzes the transaction data and predicts whether the transaction is fraudulent or genuine. All transaction details and prediction results are stored in the MySQL database, ensuring proper data management and retrieval. The processed results are then displayed on a dashboard, enabling users and administrators to monitor transactions and detect suspicious activities effectively.

The system utilizes multiple machine learning models, including Logistic Regression, Random Forest, Decision Tree, and Naive Bayes, to improve the accuracy and reliability of fraud detection. These models are trained on historical transaction data to learn patterns and identify anomalies. Based on various factors such as transaction amount, location, and time, the models classify each transaction as either genuine or fraudulent. For example, a transaction with a high amount, originating from a new location, and occurring at an unusual time may be flagged as fraudulent. This combination of architectural design and machine learning techniques enables the system to provide intelligent, data-driven, and real-time fraud detection.

3.2 USE CASE DIAGRAM

The Use Case Diagram illustrates the functional requirements of the system, defining the interactions between external Actors and the internal System Boundary. It provides a high-level overview of the system's capabilities and the scope of user-driven operations.

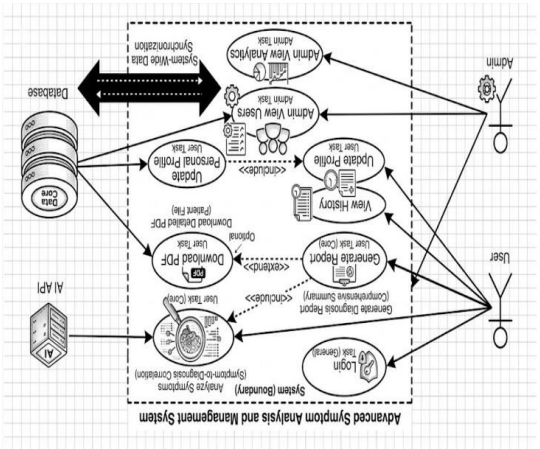

Fig 3.2 Use Case Diagram

4 RESULTS

The system execution begins with the user login module, where users enter their credentials through a secure interface. After successful authentication, the user is redirected to the main dashboard. The interface is designed to be user-friendly and displays important information such as transaction summaries, fraud alerts, and system status. The smooth navigation between pages such as login, investigation, and visualization confirms the proper functioning of the frontend and backend integration.

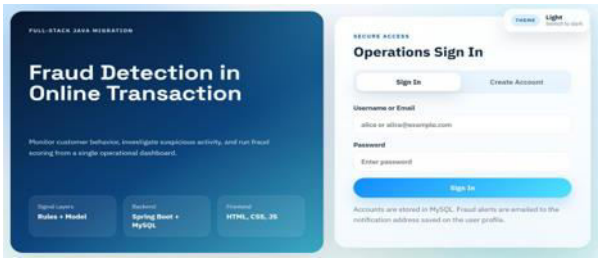

Fig 4.1: **Fraud_Detection_Login_Interface**

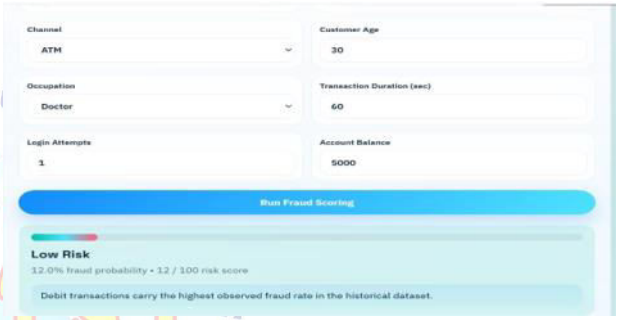

Fig 4.2: **Risk Scoring**

The fraud detection process is carried out using a machine learning model integrated into the system. When users input transaction-related details such as channel, customer age, occupation, transaction duration, login attempts, and account balance, the system processes the data and generates a prediction. The output is displayed as a risk level along with fraud probability. For example, transactions may be classified as “Low Risk” with a corresponding probability score. This demonstrates the system’s capability to provide real-time fraud predictions and risk assessment.

Fig 4.3: **Fraud_Detection_ Dashboard**

The dashboard provides a detailed summary of transaction data and fraud analysis. It displays key metrics such as total transactions, total debit and credit

amounts, average transaction value, maximum transaction amount, and suspicious transaction count. It also shows the percentage of suspicious transactions and identifies the primary transaction channel. These metrics help in understanding overall system performance and user behaviour patterns.

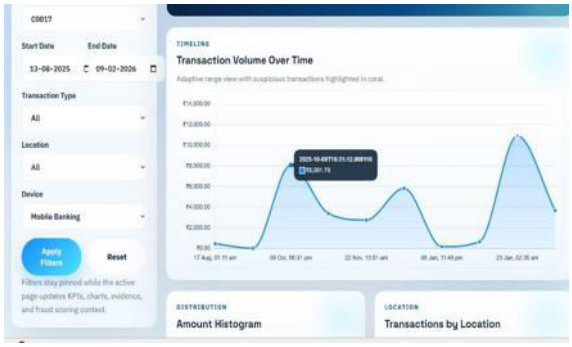

Fig 4.4: **Fraud_Detection_Visualization**

The dashboard interface presents a visual analysis of transaction data, highlighting patterns and potential fraud indicators over time. It includes filter options such as start date, end date, transaction type, location, and device type, allowing users to refine and customize the displayed data. The main section features a timeline graph titled "Transaction Volume Over Time," where transaction trends are plotted, and suspicious activities are emphasized for easy identification. Peaks and fluctuations in the graph help administrators quickly detect unusual transaction spikes that may indicate fraudulent behavior. Additionally, the dashboard provides sections for distribution analysis, such as amount histograms and location-based transaction insights, enabling comprehensive monitoring and data-driven decision-making.

5 CONCLUSION

The **Fraud Detection System for Online Transactions** developed in this project successfully demonstrates how machine learning and web technologies can be combined to improve financial security. The system is designed to monitor transaction data, identify suspicious activities, and provide real-time fraud predictions through an interactive web interface.

From the experimental results, it is evident that the system performs effectively in detecting fraudulent transactions. The integration of machine learning models with the backend allows the system to analyse multiple parameters such as transaction amount, time, location, device, and user behaviour. Based on these inputs, the system classifies transactions as either *fraudulent* or *genuine* and assigns a risk score.

The developed application includes several important modules such as user authentication, transaction investigation, fraud scoring, alert notification, and data visualization. The dashboard provides meaningful insights including total transactions, suspicious count, transaction distribution, and risk indicators. These features help users and administrators to easily monitor and analyse transaction patterns.

The fraud scoring module further enhances the system by providing probability-based risk assessment (e.g., low risk with 12% probability), making the output more interpretable and useful for decision-making. The visualization components, such as graphs and charts, improve understanding of transaction trends and suspicious activities across locations and time periods.

Although a minor server error was observed during initial testing, it highlights the importance of proper backend integration and error handling. After resolving it, the system functioned correctly, confirming its reliability.

6 FUTURE ENHANCEMENT

The future scope of the *automated fraud detection system for secure online transactions* includes several enhancements that can significantly improve its effectiveness and real-world usability. one important advancement is the implementation of a real-time alert system that can notify users instantly through sms, email, or mobile push notifications whenever a suspicious transaction is detected. this will enable users to take immediate action, such as blocking accounts or verifying transactions, thereby reducing potential financial losses. additionally, integrating more advanced machine learning models such as deep learning, xgboost, and ensemble techniques can further enhance the system's ability to detect complex and evolving fraud patterns with higher accuracy.

Another key area of improvement is handling imbalanced datasets, which is a common challenge in fraud detection systems where fraudulent transactions are rare compared to genuine ones. techniques such as

smote (synthetic minority oversampling) and other data balancing methods can be applied to improve model performance and reduce bias. furthermore, integrating the system with real banking apis, payment gateways, and financial institutions will allow real-time monitoring of live transactions, making the system more practical and applicable in real-world scenarios. strengthening security features such as multi-factor authentication, data encryption, and role-based access control will also ensure better protection of sensitive financial data.

In addition, the system can be enhanced by incorporating explainable ai (xai) techniques, which provide clear explanations for why a transaction is flagged as fraudulent. this improves transparency and builds user trust in the system. developing a mobile application version will further increase accessibility, allowing users to monitor transactions and receive alerts anytime and anywhere. moreover, implementing a continuous learning mechanism, where the model updates itself based on new transaction data and user feedback, will ensure that the system remains adaptive to emerging fraud trends. these future enhancements will transform the system into a more intelligent, secure, and scalable solution for modern digital transaction environments.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

[1] PricewaterhouseCoopers. Encuesta Global de Crimen y Fraude Económico de PwC Colombia 2022–2023; PricewaterhouseCoopers: London, UK, 2022.

[2] Reurink, A. Financial fraud: A literature review. J. Econ. Surv. 2018, 32, 1292–1325. [CrossRef]

[3] Ahmed, M.; Mahmood, A.N.; Islam, M.R. A survey of anomaly detection techniques in financial domain. Future Gener. Comput. Syst. 2016, 55, 278–288. [CrossRef]

[4] Femila, Roseline, J.F.; Naidu, G.; Samuthira Pandi, V.; Alamelu alias Rajasree, S.; Mageswari, D.N. Autonomous credit card fraud detection using machine learning approach. Comput. Electr. Eng. 2022, 102, 108132. [CrossRef]

[5] Tingfei, H.; Guangquan, C.; Kuihua, H. Using variational auto encoding in credit card fraud detection. IEEE Access 2020, 8, 149841–149853. [CrossRef]

[6] Dantas, R.M.; Firdaus, R.; Jaleel, F.; Neves Mata, P.; Mata, M.N.; Li, G. Systemic acquired critique of credit card deception exposure through machine learning. J. Open Innov. Technol. Mark. Complex. 2022, 8, 192. [CrossRef]

[7] Dal Pozzolo, A.; Caelen, O.; Le Borgne, Y.A.; Waterschoot, S.; Bontempi, G. Learned lessons in credit card fraud detection from a practitioner perspective. Expert Syst. Appl. 2022, 41, 4915–4928. [CrossRef]

[8] Makki, S.; Assaghir, Z.; Taher, Y.; Haque, R.; Hacid, M.S.; Zeineddine, H. An experimental study with imbalanced classification approaches for credit card fraud detection. IEEE Access 2019, 7, 93010–93022. [CrossRef].

[9] Rakowski, R.; Polak, P.; Kowalikova, P. Ethical aspects of the impact of AI: The status of humans in the era of artificial intelligence. Society 2021, 58, 196–203. [CrossRef]

[10] Alarfaj, F.K.; Malik, I.; Khan, H.U.; Almusallam, N.; Ramzan, M.; Ahmed, M. Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access 2022, 10, 39700–39715. [CrossRef]

[11] Madhurya, M.J.; Gururaj, H.L.; Soundarya, B.C.; Vidyashree, K.P.; Rajendra, A.B. Exploratory analysis of credit card fraud detection using machine learning techniques. Glob. Transitions Proc. 2022, 3, 31–37. [CrossRef]

[12] Sahin, Y.; Bulkan, S.; Duman, E. A cost-sensitive decision tree approach for fraud detection. Expert Syst. Appl. 2013, 40, 5916–5923. [CrossRef]

[13] Vanini, P.; Rossi, S.; Zvizdic, E.; Domenig, T. Online payment fraud: From anomaly detection to risk management. Financ. Innov. 2023, 9, 66.

[14] Srokosz, M.; Bobyk, A.; Ksiezopolski, B.; Wydra, M. Machine-learning-based scoring system for antifraud CISIRTs in banking environment. Electronics 2023, 12, 251. [CrossRef]

[15] Zhou,H.;Chai, H.; Qiu, M. Fraud detection within bankcard enrollment on mobile device based payment using machine learning. Front. Inf. Technol. Electron. Eng. 2018, 19, 1537– 1545. [CrossRef]