International Journal for Modern Trends in Science and Technology
Volume 12, Issue 04, pages 862-867
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue04.html
DOI: https://doi.org/10.5281/zenodo.19644316

Real-Time Fraud Detection Dashboard for Financial Transactions

K. T. V. Subba Rao, B. Sai Santhi Priya, D. Jeeviteswararao, Ch. Kiran Babu, G. Nikhil

Department of Computer Science and Engineering, D.N.R. College of Engineering & Technology, Balusumudi, Bhimavaram, Andhra Pradesh, India

To Cite this Article
K. T. V. Subba Rao, B. Sai Santhi Priya, D. Jeeviteswararao, Ch. Kiran Babu & G. Nikhil (2026). Real-Time Fraud Detection Dashboard for Financial Transactions. International Journal for Modern Trends in Science and Technology, 12(04), 862-867. https://doi.org/10.5281/zenodo.19644316

Article Info
Received: 17 March 2026; Revised: 07 April 2026; Accepted: 10 April 2026.

KEYWORDS

Fraud Detection, Financial Transactions, Real-Time Monitoring, Anomaly Detection, Machine Learning, Data Analytics, Transaction Security

ABSTRACT

Financial transactions have increased rapidly with the growth of digital payment systems, making them more vulnerable to fraudulent activities. Without proper detection systems, it becomes difficult for financial institutions to ensure secure transactions and prevent financial losses, which plays a very important role in maintaining trust and reliability in digital platforms. Till date, many traditional fraud detection methods are slow, manual, and inefficient when handling large volumes of transaction data, leading to delays in identifying suspicious activities. The other drawback is that manual monitoring and verification processes consume more time and effort, making it difficult for organizations to respond quickly to fraud attempts. This project aims to provide a solution to these problems through the development of a Real-Time Fraud Detection Dashboard for Financial Transactions. The system continuously monitors transaction data and analyzes it to identify unusual patterns and suspicious activities. It classifies transactions as safe or potentially fraudulent based on predefined conditions and logical patterns. Users can input transaction details, and the system quickly processes the data to provide results, reducing the time required for verification. The dashboard provides a centralized platform for administrators to view transaction details, track fraud alerts, and analyze patterns effectively. By automating the detection process, the system reduces manual effort, improves accuracy, and enables faster decision-making. Overall, the project enhances security, increases efficiency, and provides a reliable solution for detecting and managing financial fraud.

1. INTRODUCTION

The rapid growth of digital payment systems and online financial transactions has significantly transformed the modern economy, but it has also led to a substantial increase in fraudulent activities [1,5,7]. With the advancement of technologies, fraudsters are using more sophisticated techniques, making traditional fraud detection systems ineffective and slow, as they mainly rely on manual verification and post-transaction analysis [7,17]. This results in delayed detection, financial losses, and reduced trust in financial systems [3,18]. Studies show that financial fraud leads to billions of dollars in losses globally each year, affecting banks, businesses, and individual users [3,5].

In many cases, fraudulent transactions go unnoticed until after completion, making recovery difficult and time-consuming [2,19]. To address these challenges, real-time fraud detection systems have gained importance by enabling continuous monitoring and instant identification of suspicious activities [6,7]. The proposed system, "Real-Time Fraud Detection Dashboard for Transactions using Spring Boot and SQL," focuses on detecting anomalies based on transaction patterns such as unusual transaction amounts, high frequency of transactions, and behavioral inconsistencies [4,8,16].

By integrating secure admin authentication, real-time dashboard analytics, and automated fraud detection techniques, the system reduces manual effort and enhances decision-making efficiency [5,6]. This approach improves security, minimizes financial risks, and provides a reliable platform for monitoring and managing financial transactions effectively [1,7,20].

1.1 PURPOSE

This paper proposes a real-time fraud detection dashboard for financial transactions using technologies like Spring Boot and SQL [5,6]. The system monitors transactions continuously and detects suspicious activities based on patterns such as unusual amounts and transaction frequency [4,8,16]. By providing a centralized dashboard with real-time alerts and analytics, it simplifies fraud detection and improves decision-making [6,7]. This approach reduces manual effort, minimizes financial risks, and enhances security and reliability in financial systems [1,5,7].

1.2 MOTIVATION

In today's fast-paced digital world, the rapid growth of online financial transactions brings significant challenges, including delayed fraud detection, manual verification processes, and increasing fraudulent activities [1,3,18]. Traditional systems often fail to detect suspicious transactions in real time, leading to financial losses and reduced trust [7,17]. Real-time fraud detection systems provide an effective solution by continuously monitoring transactions and identifying anomalies using pattern analysis [6,7].

By implementing a real-time fraud detection dashboard using technologies like Spring Boot and SQL, the system enables instant alerts, improved monitoring, and efficient decision-making [5,6]. This approach helps reduce fraud, enhance security, and allow organizations to manage financial transactions with greater confidence and reliability [5,7,20].

1.3 PROBLEM STATEMENT

Traditional fraud detection systems face challenges such as delayed detection, manual verification, and inability to handle large volumes of transactions efficiently [2,7,18]. These limitations increase the risk of financial loss and make the process slow and unreliable [3,19]. This paper aims to address these issues by proposing a real-time fraud detection dashboard for financial transactions [5,6].

By leveraging technologies like Spring Boot and SQL, the system continuously monitors transaction data and detects suspicious activities based on predefined patterns [4,8,16]. The dashboard provides instant alerts and visual insights, ensuring faster verification and better decision-making [6,7]. This solution streamlines fraud detection and reduces the risks associated with traditional methods [1,5,7].

2. LITERATURE REVIEW

Various studies focus on detecting financial fraud using machine learning and real-time systems, showing the need for fast and accurate solutions. Traditional rule-based methods use fixed limits but cannot handle changing fraud patterns effectively. To improve this, models like Random Forest and Gradient Boosting help in detecting fraud more accurately. Some approaches also study user behavior, such as transaction frequency and amount changes, to find unusual activities. Techniques like the Voted Perceptron model further improve detection by reducing errors. However, many existing systems do not provide real-time monitoring or clear visualization. To solve this, real-time fraud detection dashboards combine detection methods with simple analytics, helping in continuous monitoring and quick decision-making.

2.1 Machine Learning-Based Fraud Detection Systems AUTHORS: Sahithi et al.

This study focuses on detecting financial fraud using machine learning techniques, especially ensemble models like Random Forest, Gradient Boosting, and

XGBoost. These models combine multiple algorithms to improve accuracy and reduce false alarms. The system is capable of analyzing large amounts of transaction data and identifying fraudulent activities effectively. The results show that ensemble methods perform better than single models in detecting fraud and handling complex transaction patterns.

2.2 Hybrid and Behavior-Based Fraud Detection Approaches

AUTHORS: Karthik et al.

This research proposes a hybrid fraud detection system that uses both supervised and unsupervised learning methods. It focuses on analyzing user behavior such as transaction frequency, spending patterns, and location changes to detect unusual activities. This approach helps in identifying new types of fraud that were not seen before. The study highlights that behavior-based analysis improves the system's ability to detect fraud more efficiently and accurately.

2.3 Data Balancing Techniques in Fraud Detection

AUTHORS: : Gupta et al.

Gupta et al. studied the importance of handling imbalanced datasets in fraud detection systems. They proposed techniques such as SMOTE, oversampling, and undersampling to balance the data. These methods help in improving the performance of machine learning models. The study shows that combining multiple balancing techniques leads to better results. It reduces bias toward normal transactions and improves fraud detection accuracy. Proper data preprocessing plays a key role in building effective fraud detection systems.

2.4 Real-Time Stream Processing for Fraud Detection

AUTHORS: Ekundayo et al.

Ekundayo et al. introduced a real-time stream processing approach for fraud detection using big data tools. Their system processes continuous transaction data streams using technologies like Hadoop and Spark. It enables instant detection of suspicious activities without delay. The framework improves scalability and speed in high-volume environments. It also supports continuous monitoring of financial transactions. This approach is essential for building real-time fraud detection systems.

2.5 Anomaly Detection Techniques in Fraud Detection

AUTHORS: Dhalaria and Gandotra

Dhalaria and Gandotra proposed an anomaly detection approach to identify unusual patterns in transaction data. Their system focuses on detecting deviations from normal user behavior rather than relying only on predefined fraud cases. This helps in identifying new and unknown types of fraud effectively. The model continuously monitors transactions and flags suspicious activities. It improves detection capability by focusing on abnormal patterns. This approach is useful for enhancing fraud detection accuracy in dynamic enviro.

3. PROPOSED SYSTEM

The proposed system is a real-time fraud detection dashboard that integrates machine learning with a web-based application to identify fraudulent transactions efficiently. Developed using Spring Boot, MySQL, and web technologies, it uses a Random Forest model to analyze transactions, provide real-time alerts, and support quick decision-making through visual analytics.

Advantages of Proposed System

- Real-time fraud detection enables instant identification of suspicious transactions.
- Machine learning improves accuracy by analyzing complex patterns.
- Automation reduces manual effort in monitoring transactions.
- Provides fraud probability for better decision-making.
- Ensures security and scalability of the system.

3.1 SYSTEM ARCHITECTURE

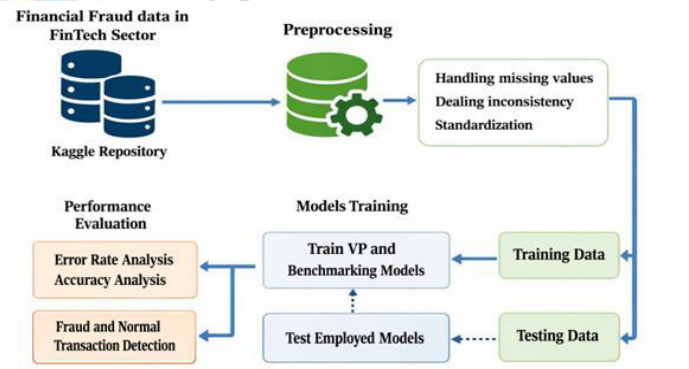


Fig 1 : Architecture Diagram

3.2 USE CASE DIAGRAM

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

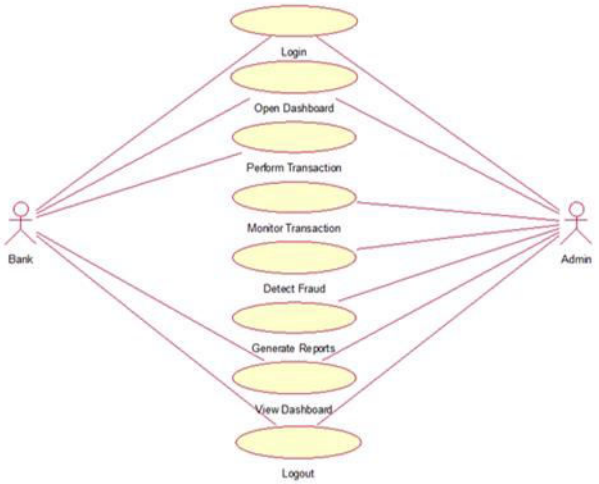


Fig 2 : Use case Diagram

3.3 CLASS DIAGRAM

The class diagram is used to refine the use case diagram and define a detailed design of the system. The class diagram classifies the actors defined in the use case diagram into a set of interrelated classes. The relationship or association between the classes can be either an "is-a" or "has-a" relationship. Each class in the class diagram may be capable of providing certain functionalities. These functionalities provided by the class are termed "methods" of the class. Apart from this, each class may have certain "attributes" that uniquely identify the class.

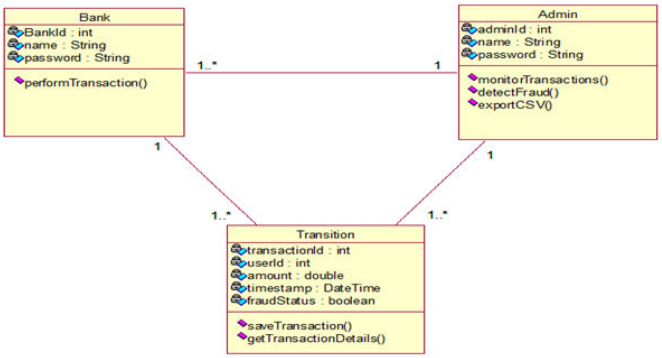


Fig 3 : Class Diagram

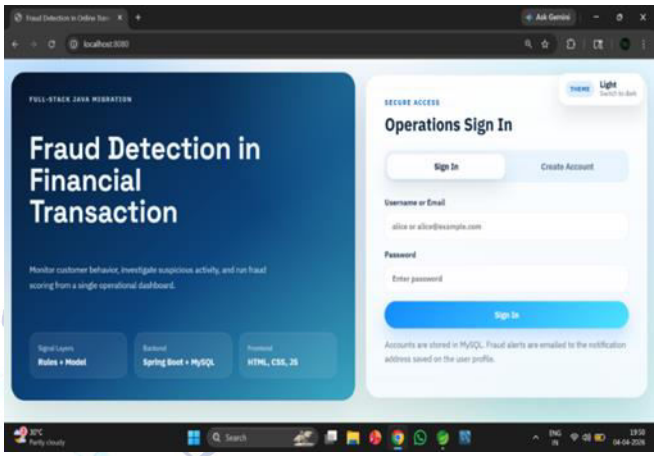
3.4 DATASET

The dataset used in this project consists of financial transaction records designed to support fraud detection. It includes both normal and fraudulent transactions, helping the system learn patterns and identify suspicious activities. The dataset contains important features such as transaction amount, transaction type (debit/credit), transaction channel (ATM/online/branch), customer age, occupation, transaction duration, login attempts, and account balance. These features provide valuable insights into user behaviour and transaction characteristics.

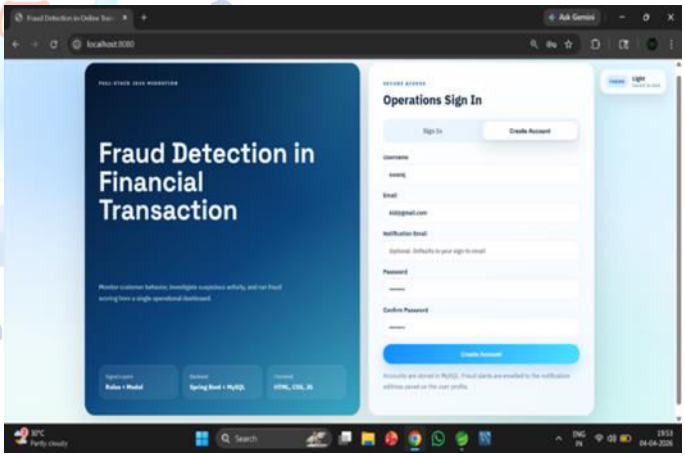
The dataset is collected from publicly available sources like Kaggle or generated synthetically to simulate real-world scenarios. Before using it, the data is preprocessed by cleaning, encoding categorical values, and normalizing numerical data. It is then used to train the Random Forest model, which helps in predicting fraud probability and improving the accuracy of real-time fraud detection in the system.

4. RESULTS

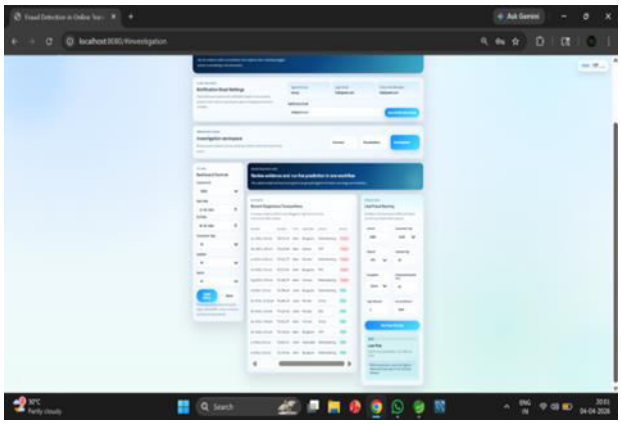
SIGN IN PAGE



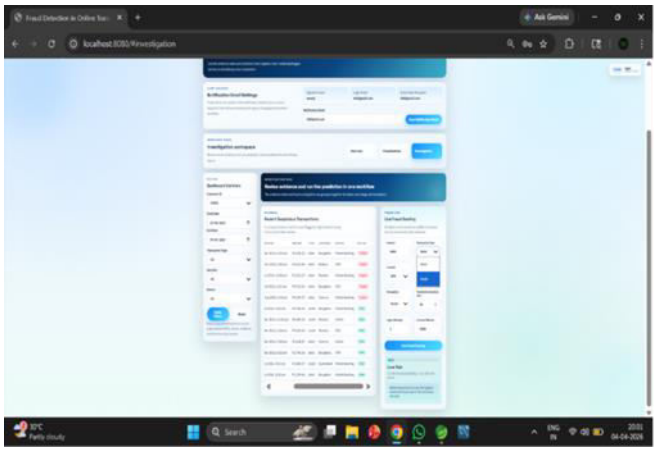
CREATE ACCOUNT



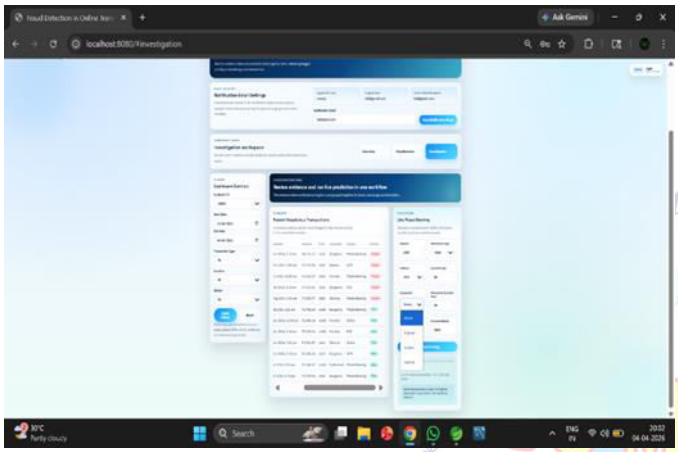
INVESTIGATION – RUN FRAUD SCORING



INVESTIGATION – TRANSACTION TYPE



INVESTIGATION - OCCUPATION



CONCLUSION

The Real-Time Fraud Detection Dashboard improves financial security by enabling real-time monitoring and analysis of transactions using Spring Boot, SQL, and web technologies. It provides secure authentication, dynamic dashboards, fraud analytics, and reporting features to quickly detect suspicious activities and support decision-making. With scalable architecture, strong security measures, and user-friendly design, the system enhances fraud prevention and ensures efficient, reliable transaction management. Additionally, it supports data-driven insights through visualization and historical analysis of fraud patterns. The modular design also allows future integration of advanced technologies like machine learning and real-time alert systems.

FUTURE SCOPE

- **Model Optimization and Retraining:** The existing Random Forest model can be improved using advanced tuning techniques and continuous retraining. This will enhance accuracy and adapt to new fraud patterns. It ensures better real-time fraud detection performance.
- **Advanced User Behavior Analysis:** Future systems can analyze detailed user behavior such as transaction frequency and patterns. This helps in detecting personalized fraud activities. It increases the precision of anomaly detection.
- **Real-Time Alert and Notification System:** A notification system can be added to send instant alerts via email or SMS. This enables quick response to suspicious transactions. It helps in minimizing financial risks effectively.
- **Integration with Payment Platforms:** The system can be integrated with platforms like Stripe and PayPal. This allows real-time monitoring across multiple payment channels. It improves practical implementation in financial systems.
- **Cloud Deployment and Scalability:** Deploying the system on cloud platforms like Amazon Web Services or Microsoft Azure enhances scalability and performance. It supports handling large volumes of transaction data. This makes the system enterprise-ready.

Conflict of interest statement

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

REFERENCES

[1] Sahithi, G.L.; Roshmi, V.; Sameera, Y.V.; Pradeepini, G. Credit card fraud detection using ensemble methods in machine learning. In Proceedings of the 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 28–30 April 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1237–1241.

[2] Gupta, P.; Varshney, A.; Khan, M.R.; Ahmed, R.; Shuaib, M.; Alam, S. Unbalanced credit card fraud detection data: A machine learning-oriented comparative study of balancing techniques. Procedia Comput. Sci. 2023, 218, 2575–2584. [CrossRef]

[3] Ekundayo, F.; Atoyebi, I.; Soyele, A.; Ogunwobi, E. Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning. Int. J. Res. Publ. Rev. 2024, 5, 5934–5948. [CrossRef]

[4] Karthik, V.S.S.; Mishra, A.; Reddy, U.S. Credit card fraud detection by modelling behaviour pattern using hybrid ensemble model. Arab. J. Sci. Eng. 2022, 47, 1987–1997. [CrossRef]

[5] Banka, S.; Kanchanapalli, B.; Shaik, N.K.; Dasari, K.; Poojitha, D.; Nalla, A. Securing Fintech: A Machine Learning Approach for Credit Card Fraud Detection. In Proceedings of the 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS), Coimbatore, India, 17–19 April 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 814–821.

[6] Chintale, P.; Ranjan, P.; Desani, N.R.; Desaboyina, G.; Malviya, R.K. Leveraging Aiml Ops for Fraud Detection and Prevention in Fintech. J. Harbin Eng. Univ. 2024, 45, 70–75.

[7] Dichev, A.; Zarkova, S.; Angelov, P. Machine Learning as a Tool for Assessment and Management of Fraud Risk in Banking Transactions. J. Risk Financ. Manag. 2025, 18, 130. [CrossRef]

[8] Niveditha, G.; Abarna, K.; Akshaya, G.V. Credit card fraud detection using random forest algorithm. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. 2019, 5, 301–306. [CrossRef]
[9] Naik, H.; Kanikar, P. Credit card fraud detection based on machine learning algorithms. Int. J. Comput. Appl. 2019, 182, 8–12. [CrossRef]
[10] Dhalaria, M.; Gandotra, E. MalDetect: A classifier fusion approach for detection of android malware. Expert Syst. Appl. 2024, 235, 121155. [CrossRef]
[11] Beltozar-Clemente, S.; Iparraguirre-Villanueva, O.; Pucuhuayla-Revatta, F.; Zapata-Paulini, J.; Cabanillas-Carbonell, M. Predicting customer abandonment in recurrent neural networks using short-term memory. J. Open Innov. Technol. Mark. Complex. 2024, 10, 100237. [CrossRef]
[12] Somvanshi, M.; Chavan, P.; Tambade, S.; Shinde, S.V. A review of machine learning techniques using decision tree and support vector machine. In Proceedings of the 2016 International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 12–13 August 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–7.
[13] Jadhav, S.D.; Channe,H.P. Comparative study of K-NN, naive Bayes and decision tree classification techniques.
[14] Int. J. Sci. Res. (IJSR) 2016, 5, 1842–1845.
[15] Randhawa, K.; Loo, C.K.; Seera, M.; Lim, C.P.; Nandi, A.K. Credit card fraud detection using AdaBoost and majority voting. IEEE Access 2018, 6, 14277–14284. [CrossRef]
[16] Yee, O.S.; Sagadevan, S.; Malim, N.H.A.H. Credit card fraud detection using machine learning as data mining technique. J. Telecommun. Electron. Comput. Eng. (JTEC) 2018, 10, 23–27.
[17] Jain, Y.; Tiwari, N.; Dubey, S.; Jain, S. A comparative analysis of various credit card fraud detection techniques. Int. J. Recent Technol. Eng. 2019, 7, 402–407.
[18] Qaddoura, R.; Biltawi, M.M. Improving fraud detection in an imbalanced class distribution using different oversampling techniques. In Proceedings of the 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI), Zarqa, Jordan, 6–8 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–5.
[19] Prasad, P.Y.; Chowdary, A.S.; Bavitha, C.; Mounisha, E.; Reethika, C. A comparison study of fraud detection in usage of credit cards using machine learning. In Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–13 April 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1204–1209.