International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(1) (2026)

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com

Peer Reviewed,Referred & Indexed Journal

Research Paper

FRAUDULENT ORDER DETECTION IN SUPPLY CHAIN TRANSACTIONS USING BEHAVIORAL SIGNALS

[1]M Bharath Kumar, [2] Ch Madhumathi ,[3]Ch Devaji, [4] G Gowtham Raj
[1]AssistantProfessor, [234]Students
Department of Computer Science and Technology
Siddhartha Institute of Technology & Sciences, Narapally
bharath@siddhartha.org.in, 23TQ1A05D1@siddhartha.co.in, 23TQ1A05G2@siddhartha.co.in, 23TQ1A0510@siddhartha.co.in,

Abstract

Supply chain systems process a vast number of transactions daily, making them highly susceptible to fraudulent activities such as fake orders, unauthorized purchases, and manipulation of transaction records. Detecting such fraud manually is both time-consuming and inefficient due to the large volume and complexity of transactional data. Therefore, there is a need for an intelligent and automated system to identify and prevent fraudulent activities effectively.

This project focuses on detecting fraudulent orders in supply chain transactions by analyzing behavioral signals generated during order processing. These behavioral signals include user activity patterns, order frequency, transaction timing, location variations, and purchasing behavior. By analyzing these patterns, the system can identify deviations from normal behavior, which may indicate potential fraud.

The proposed system utilizes data analysis and machine learning techniques to monitor and evaluate transaction data in real time. It learns the normal behavioral patterns of users and compares them with incoming transactions to detect anomalies. When suspicious activities are identified, the system generates alerts for administrators, enabling timely intervention to prevent financial losses.

The implementation of this system enhances transparency, improves fraud detection accuracy, and strengthens the overall security of supply chain operations. This project demonstrates how behavioral analytics combined with intelligent algorithms can effectively detect fraudulent activities and support secure and reliable transaction management in modern supply chains.

I. Introduction

In recent years, supply chain systems have become highly digitized with the adoption of e-commerce platforms, ERP systems, and online transaction processing technologies. These advancements have significantly improved operational efficiency, speed, and scalability of supply chain activities. However, the increased reliance on digital platforms has also introduced new security challenges, making supply chains more vulnerable to fraudulent activities such as fake orders, payment manipulation, identity theft, and unauthorized transactions. Such fraudulent activities can lead to

serious financial losses, disrupt operations, and damage the reputation of organizations.

Traditional fraud detection systems primarily rely on rule-based approaches, where predefined conditions are used to identify suspicious transactions. While these methods are simple to implement, they are often ineffective against modern and sophisticated fraud techniques that continuously evolve over time. As a result, there is a growing need for intelligent and adaptive systems that can detect fraud more accurately and efficiently.

To address this challenge, modern fraud detection systems leverage behavioral signals and machine learning techniques. Behavioral signals include user activity patterns, transaction frequency, login locations, device information, and purchasing behavior. By analyzing these signals, the system can understand normal user behavior and detect deviations that may indicate fraudulent activity. This approach enables early detection and prevention of fraud, improving the overall security and reliability of supply chain transactions.

II. Literature Survey

Fraud detection has become a critical component of modern supply chain management due to the rapid growth of digital transactions and online marketplaces. As supply chains evolve into complex, data-driven systems, the risk of fraudulent activities such as fake orders, invoice fraud, duplicate payments, and identity theft has increased significantly. Early research primarily relied on rule-based detection methods, where predefined rules were used to identify suspicious transactions. However, these approaches are limited in handling dynamic and sophisticated fraud patterns, as they cannot adapt to new or unseen fraudulent behaviors.

Recent studies emphasize the use of machine learning and artificial intelligence techniques to enhance fraud detection capabilities in supply chain transactions. These methods analyze large volumes of transactional and behavioral data to identify anomalies and unusual patterns that may indicate fraud. Algorithms such as Logistic Regression, Decision Trees, Random Forest, and Neural Networks have been widely applied to classify transactions as legitimate or fraudulent. These models continuously learn from historical data, improving their accuracy and ability to detect complex fraud patterns over time.

Furthermore, research highlights the importance of behavioral analytics in fraud detection. By analyzing user behavior such as transaction frequency, purchasing patterns, login activity, and location changes, systems can identify deviations from normal behavior that may signal fraudulent activity. This approach provides a more dynamic and proactive method of detection compared to traditional systems.

In modern supply chain environments, fraud detection systems are increasingly integrated with enterprise platforms such as Enterprise Resource Planning (ERP) and Supply Chain Management (SCM) systems. These integrated solutions enable real-time monitoring of financial and logistics transactions, allowing organizations to detect and respond to suspicious activities promptly.

III. System Analysis

The fraudulent order detection system in supply chain transactions focuses on identifying suspicious activities using behavioral signals and machine learning techniques. The system collects transaction data such as order details, user activity, login patterns, device information, and location data. This data is analyzed to understand normal user behavior and detect anomalies. Preprocessing techniques are applied to clean and normalize the data for better analysis. Feature selection is performed to identify the most relevant behavioral indicators of fraud. Machine learning models are trained using historical transaction data to classify orders as genuine or fraudulent. The system continuously monitors new transactions in real time. Evaluation metrics such as accuracy, precision, and recall are used to measure performance. Alerts are generated when suspicious behavior is detected. Overall, the system aims to improve security and reduce fraud in supply chain operations.

Existing System

The existing system for fraud detection in supply chain transactions mainly relies on rule-based and manual verification methods. These systems use predefined rules such as transaction limits, unusual order amounts, or restricted locations to detect fraud. In many cases, human intervention is required to review suspicious transactions. The system typically considers limited parameters and does not analyze user behavior in depth. It lacks the ability to process large volumes of data efficiently. Traditional methods are often static and cannot adapt to new fraud patterns. The detection process is slow and may not support real-time monitoring. These systems are dependent on historical rules, which may become outdated over time. As a result, they fail to detect complex or hidden fraudulent activities. Overall, the existing system is less effective in modern digital supply chain environments.

Disadvantages of Existing System

The existing fraud detection systems have several limitations that affect their performance. They rely heavily on predefined rules, which makes them inflexible and unable to detect new fraud patterns. These systems often produce false positives and false negatives, reducing reliability. Manual verification increases processing time and operational cost. They cannot efficiently handle large-scale transaction data. The systems lack real-time detection capabilities, leading to delayed responses. Limited use of behavioral data reduces detection accuracy. They are not adaptive and require frequent updates to rules. Traditional methods fail to identify complex and hidden fraud patterns. Overall, these systems are less accurate, less efficient, and not suitable for modern supply chain needs.

Proposed System

The proposed system uses machine learning and behavioral signal analysis to detect fraudulent orders in supply chain transactions. It collects and analyzes data such as user activity, transaction frequency, location changes, and purchasing behavior. The data is preprocessed and relevant features are selected for model training. Machine learning algorithms such as Random Forest, Decision Trees, or Neural Networks are

used to build predictive models. The system learns normal user behavior from historical data. It compares new transactions with learned patterns to detect anomalies. The system operates in real time to identify suspicious activities instantly. Alerts are generated automatically when fraud is detected. The model continuously improves with new data. Overall, the proposed system provides an intelligent and automated fraud detection solution.

Advantages of Proposed System

The proposed system offers improved accuracy in detecting fraudulent transactions using advanced machine learning techniques. It can analyze large volumes of data efficiently and handle complex patterns. The system reduces human intervention and minimizes errors. Real-time detection enables quick response to suspicious activities. Behavioral analysis improves the identification of hidden fraud patterns. The system is adaptive and can learn from new data continuously. It reduces false positives and enhances reliability. The solution is scalable and suitable for modern supply chain systems. It improves transparency and operational security. Overall, the proposed system provides a robust, efficient, and intelligent fraud detection mechanism.

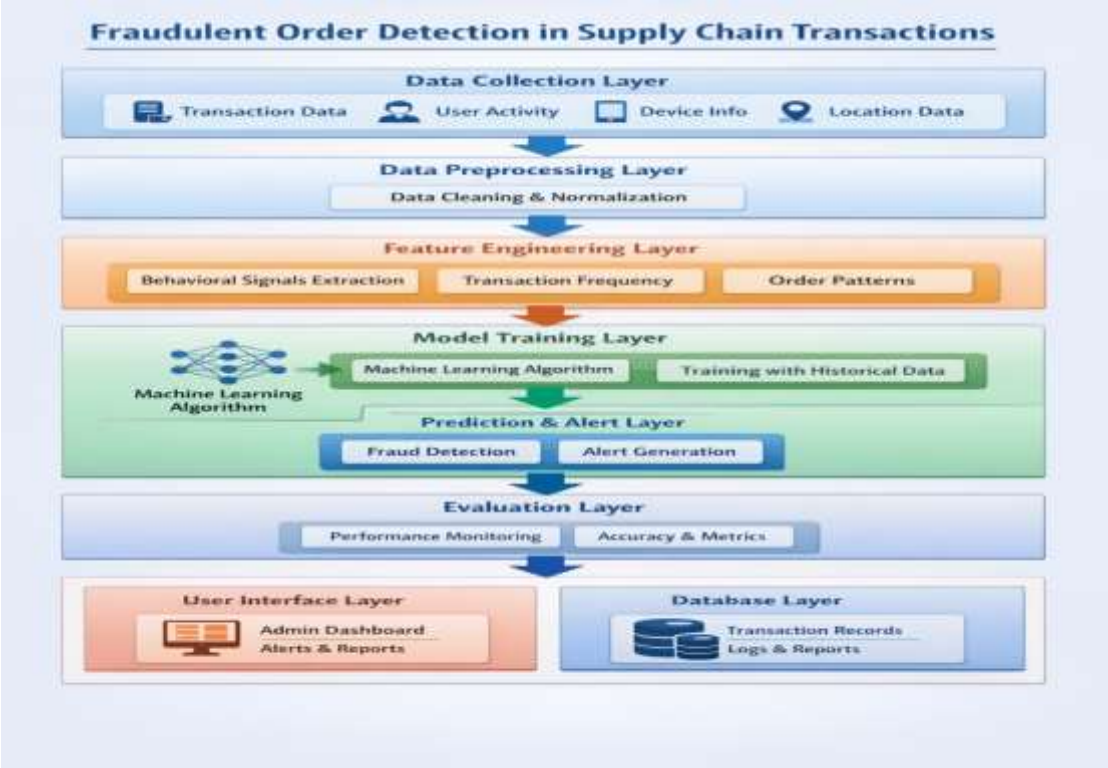
IV. Methodology

The methodology for fraudulent order detection in supply chain transactions using behavioral signals follows a systematic and data-driven approach. Initially, transaction data is collected from supply chain systems, including order details, user activity logs, login information, device details, location data, and purchasing behavior. The collected data is then preprocessed by handling missing values, removing duplicates, and normalizing numerical features to ensure data quality and consistency. Feature engineering is performed to extract meaningful behavioral signals such as transaction frequency, unusual order patterns, and location changes. The dataset is then divided into training and testing sets for model development. Machine learning algorithms such as Random Forest, Decision Trees, or Logistic Regression are applied to train models that can distinguish between normal and fraudulent transactions. The model learns patterns of legitimate behavior and identifies deviations as potential fraud. Performance is evaluated using metrics such as accuracy, precision, recall, and F1-score. Once the model achieves satisfactory performance, it is deployed for real-time monitoring of transactions. The system continuously analyzes incoming data and generates alerts when suspicious activities are detected, enabling timely intervention and fraud prevention.

System Architecture

The system architecture for fraudulent order detection in supply chain transactions is designed as a layered structure to efficiently process and analyze transaction data. The process begins with the data collection layer, where transaction and behavioral data are gathered from various sources such as ERP systems, e-commerce platforms, and user activity logs. The collected data is passed to the preprocessing layer, where it is cleaned, normalized, and prepared for analysis. Next, the feature extraction layer identifies important behavioral signals such as transaction patterns, frequency, and

anomalies. These features are then fed into the model training layer, where machine learning algorithms are trained using historical data to recognize normal and fraudulent behaviors. In the prediction layer, the trained model evaluates new transactions in real time and classifies them as genuine or suspicious. The evaluation layer monitors model performance using metrics to ensure accuracy and reliability. A user interface layer allows administrators to view alerts and monitor system outputs. Finally, a database layer stores transaction records, model results, and logs for future analysis and continuous improvement. Overall, the architecture ensures efficient, scalable, and real-time fraud detection in supply chain systems.



V. Result and Output

VI. Conclusion

In conclusion, the project on fraudulent order detection in supply chain transactions using behavioral signals provides an effective and intelligent solution to identify and prevent fraudulent activities. By analyzing user behavior patterns such as transaction frequency, location changes, and purchasing habits, the system is able to detect anomalies that indicate potential fraud. The integration of machine learning techniques enables the system to learn from historical data and improve detection accuracy over time.

The proposed approach overcomes the limitations of traditional rule-based systems by offering real-time monitoring, higher accuracy, and adaptability to evolving fraud patterns. It reduces manual effort and enhances the efficiency of fraud detection processes. The system also helps organizations minimize financial losses, improve transparency, and strengthen the overall security of supply chain operations.

Overall, this project demonstrates the importance of combining behavioral analytics with machine learning to build robust fraud detection systems. It can be further enhanced by incorporating advanced algorithms, larger datasets, and real-time deployment, making it suitable for modern, large-scale supply chain environments.

References

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.

[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.

[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm

[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.

[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, "Real-Time Object Detection in Drone Surveillance Using YOLOv5," in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.

[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, "Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks," in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.

[7] R. D. Kumar, V. N. S.Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.

[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.

[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.

[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.

[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.