IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AI POWERED FRAUD DETECTION FOR ONLINE TRANSCATION

Prof. Nagesh Patil[1], Sakle Nikita[2], Mohane Poonam[3], Waghmode Nikhil[4]

[1]Professor Vidya Prasarini Sabha's Collage of Engineering and Technology, Lonavala

[23456]Student Computer Engineering Vidya Prasarini Sabha's Collage of Engineering and Technology, Lonavala.

nageshpptil@gmail.com,nikitasakle721@gmail.com,nikhilwaghmode609@gmail.com, poonammohane5@gmail.com ,

Abstract

The rapid growth of online transactions has significantly increased the risk of fraudulent activities, posing serious challenges to financial institutions and digital platforms. Fraud detection systems are essential for identifying and preventing unauthorized or suspicious transactions in real time. Traditional rule-based approaches often fail to detect evolving and complex fraud patterns, leading to the adoption of advanced techniques such as machine learning and data mining. This study focuses on developing an efficient fraud detection system that analyzes transaction data to identify anomalies and classify fraudulent behavior accurately. Various algorithms, including classification models and anomaly detection techniques, are utilized to improve detection accuracy while minimizing false positives. The proposed approach aims to enhance security, protect user data, and maintain trust in online transaction systems. Overall, this work highlights the importance of intelligent and adaptive fraud detection mechanisms in ensuring safe and reliable digital financial services.

Keyword

Online Transaction Fraud, Fraud Detection, Machine Learning, Deep Learning,Hybrid Models, Anomaly Detection, Graph Neural Networks (GNN), Credit Card Fraud, Real-Time Detection, Explainable AI (XAI), Financial Technology (FinTech), Block chain Security.

Introduction

Fraud detection in online transactions has become a critical component of modern digital systems as the rapid growth of e-commerce, online banking, and digital payment platforms increases exposure to financial crimes. With the widespread adoption of technologies such as mobile wallets, credit cards, and internet banking, fraudulent activities like identity theft, phishing, and unauthorized transactions have also evolved in complexity and scale.

Traditional rule-based systems, which rely on predefined patterns to identify suspicious behavior, are no longer sufficient to combat sophisticated fraud techniques. As a result, advanced approaches using machine learning and data analytics are being widely adopted. These systems analyze large volumes of transactional data in real time to detect anomalies and predict potentially fraudulent activities with higher accuracy.

Fraud detection systems typically work by monitoring user behavior, transaction patterns, and contextual information such as location, device, and transaction history. By leveraging techniques such as anomaly detection, classification algorithms, and neural networks, these systems can identify unusual patterns that deviate from normal behavior.

Despite these advancements, challenges remain, including maintaining user privacy, minimizing false positives, and adapting to constantly evolving fraud strategies. Therefore, developing efficient, scalable, and adaptive fraud detection mechanisms is essential to ensure secure and trustworthy online transactions.

In summary, fraud detection plays a vital role in safeguarding financial systems and enhancing user confidence in digital platforms. Continued research and innovation in this field are necessary to keep pace with emerging threats and ensure the integrity of online transaction ecosystems.

Figure1.Fruad Detection Form

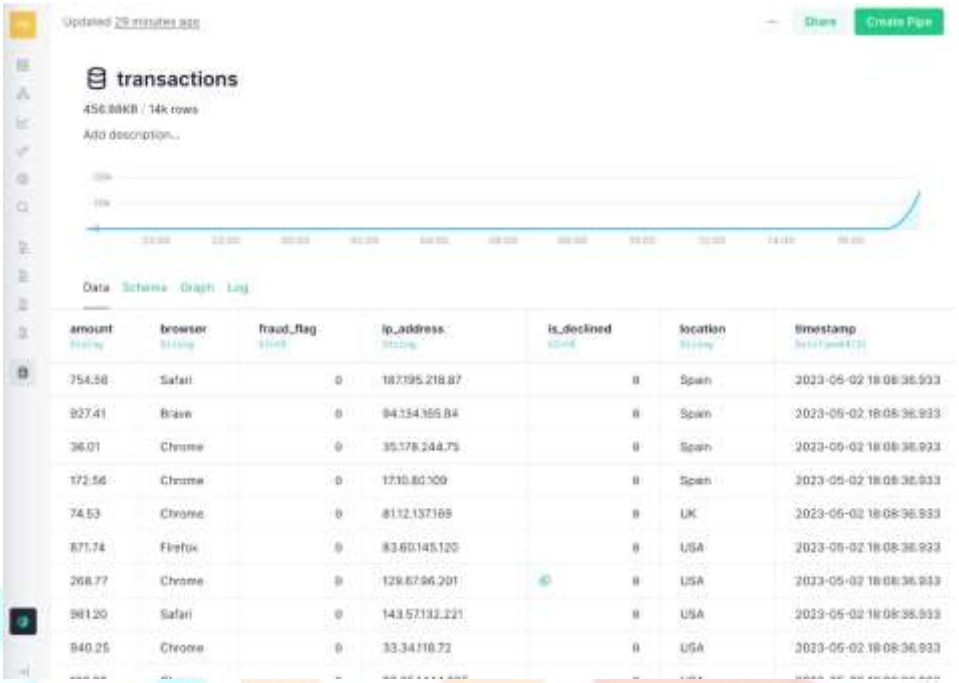

Figure 2. Transactions

A fraud detection system for online transactions collects user, transaction, device, and merchant data, along with behavioral logs. The data is pre-processed, features are engineered, and class imbalance is handled. Detection combines supervised models (Logistic Regression, Random Forest, XGBoost), unsupervised methods (Isolation Forest, Auto encoders), deep learning(LSTM,CNN) for temporal patterns, and graph-based models(GNNs)to identify fraud rings. A decision engine aggregates outputs to classify transactions as legitimate or fraudulent, while continuous monitoring updates models to handle concept drift. The system is deployed for real-time scoring to block or alert suspicious transactions immediately.

Literature Review:

Fraud detection in online transactions has evolved from traditional rule-based systems to more advanced machine learning techniques. Earlier methods relied on fixed rules to identify suspicious activities, but they were not effective against new and complex fraud patterns.

To improve accuracy, researchers introduced machine learning algorithms such as Logistic Regression, Decision Trees, and Random Forest. These models analyze past transaction data to detect fraudulent behavior. In addition, anomaly detection techniques are used to identify unusual patterns, especially when labeled data is limited.

Overall, modern fraud detection systems aim to be more accurate, adaptive, and efficient in handling evolving online fraud threats.

Machine Learning Techniques

Machine learning (ML) has become central to detecting fraudulent activities. A systematic literature review by Hernandez Aros et al. (2024) analyzed 104 studies published between 2012 and 2023, focusing on the application of ML in financial fraud detection. The review identified a trend towards using real datasets, with credit card fraud detection models being the most prevalent. It also noted a low usage of synthetic data (less than 7%) in experiments. Commonly employed ML algorithms include decision trees, support vector machines, and ensemble methods like XGBoost and AdaBoost. These models are evaluated using metrics such as accuracy, precision, recall, and F1-score to assess their effectiveness in identifying fraudulent transactions.

Handling Class Imbalance

Class imbalance, where fraudulent transactions are much fewer than legitimate ones, poses a significant challenge. To address this, researchers have explored various techniques. For instance, Darwish (2025) utilized Artificial Bee Colony-based sampling to balance datasets, enhancing the performance of fraud detection models. Similarly, the use of Synthetic Minority Over-sampling Technique (SMOTE) has been applied to generate synthetic samples, improving model sensitivity to fraudulent activities.

Explain ability and Interpretability

Understanding the rationale behind fraud detection decisions is crucial for trust and regulatory compliance. Researchers have developed models that offer explainable outputs. Zhu et al. (2022) introduced a Hierarchical Explainable Network (HEN) that models user behavior sequences, providing insights into the factors influencing fraud detection decisions. This approach enhances transparency and helps in understanding the underlying patterns.

Cross-Domain and Real-World Applications

Applying fraud detection models across different domains and real-world scenarios is essential for their generalization. Luo et al. (2025) proposed a framework combining Large Language Models (LLMs) and Graph Convolution Networks (GCNs) to detect fraud in online payment transactions across various-commerce platforms. This approach leverages both semantic and structural features, achieving high accuracy and demonstrating the scalability of the model in diverse settings.

Privacy-Preserving Techniques

With increasing concerns over data privacy, developing fraud detection systems that protect user information is paramount. About Grad et al. (2025) explored a decentralized anomaly detection frame work using deep auto encoders, ensuring that user data remains private while still effectively identifying fraudulent transactions. This approach aligns with regulatory requirements and enhances user trust in fraud detection systems.

Advanced Deep Learning Models

Deep learning approaches have been increasingly adopted for their ability to model complex patterns in large datasets. Studies have demonstrated the effectiveness of convolution neural networks (CNNs) and auto encoders in detecting anomalies indicative of fraud. For example, a study by Jin et al. (2025) proposed a multi-stage deep learning model optimized with a sparrow search algorithm, achieving high accuracy in credit card fraud detection.

Motivation for Fraud Detection:

The rapid growth of online transactions has increased opportunities for fraud, leading to significant financial losses and eroding customer trust. Traditional manual checks are insufficient against sophisticated and evolving fraudulent methods, making automated detection systems essential. Fraud detection not only helps prevent monetary loss but also ensures regulatory compliance and protects sensitive user data. Leveraging machine learning and AI enables faster, more accurate identification of suspicious transactions, fostering a secure.

System Architecture

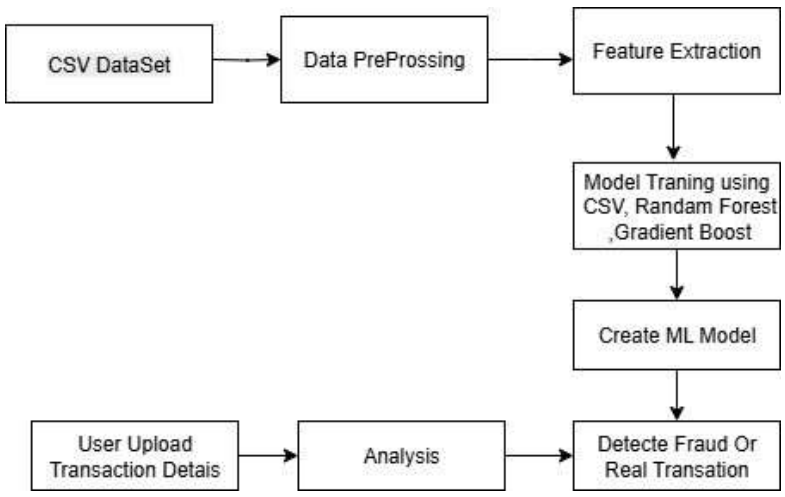

Figure3: System Architecture

1. CSV Dataset / Historical Transaction Data

- The system begins with a dataset of historical transactions stored in CSV format.
- This data set contains labeled example so fraudulent and legitimate transactions actions, which are essential for training machine earning models.

2. Data Preprocessing

- Raw transaction data is cleaned to remove duplicates, handle missing values, and normalize features.
- Data transformation and scaling may also be applied to ensure compatibility with ML algorithms.

3. Feature Extraction

- Key attributes are extracted from the raw data, such as transaction amount, frequency, user behavior, and merchant details.
- Feature engineering may include ratios, time-based features, and categorical encoding to improve model performance.

4. Model Training

- Machine learning models are trained using the preprocessed CSV data and extracted features.
- Common models include **Random Forest**, **Gradient Boosting**, and other ensemble methods.
- Thetrainingprocesslearnspatternsthatdistinguishfraudulenttransactionsfromlegitimate ones.

5. ML Model Creation

- A trained ML model is finalized and saved for deployment.
- This model serves as the core engine for fraud detection during real-time or batch transaction analysis.

6. User Upload/ Incoming Transaction Data

- New transaction data uploaded by users (or incoming live transactions) is fed into the system for analysis.
- The same preprocessing and feature extraction steps are applied to ensure consistency with the training data.

7. Analysis & Fraud Detection

- The trained ML model analyzes the new transaction data.
- Each transaction is classified as fraudulent or legitimate based on the learned patterns

8. Output/ Detection Results

- The system outputs the results of the analysis, flagging suspicious transactions for review or automated action.
- High-risk transactions may trigger alerts or additional verification steps.

Conclusions

Fraud detection in online transactions is essential for ensuring the security and reliability of digital financial systems. With the rise of online payments, traditional rule-based methods are no longer sufficient to handle complex and evolving fraud patterns. The use of machine learning and advanced techniques has significantly improved the accuracy and efficiency of detecting fraudulent activities.

Techniques such as classification algorithms, anomaly detection, and deep learning help identify suspicious transactions more effectively. However, challenges like data imbalance, false positives, and real-time processing still need to be addressed.

In conclusion, developing intelligent, adaptive, and scalable fraud detection systems is crucial to protect users and maintain trust in online transaction platforms. Continuous improvement and innovation in this field will help combat emerging fraud threats more effectively.

Reference:

[1] Bhattacharyya,S.,Jha,S.,Tharakunnel,K.,&Westland,J.C.(2011).Dataminingfor credit card fraud: A comparative study. Decision Support Systems, 50(3), 602–613.

[2] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.

[3] Carcillo,F.,DalPozzolo,A.,LeBorgne,Y.A.,Caelen,O.,Mazzer,Y.,&Bontempi,

G. (2019). Combining unsupervised and supervised learning in credit card fraud detection. Information Sciences, 557, 317–331.

[4] Zhang,Y.,Yang,Q.,& Wang,J.(2021).Deep learning for financial fraud detection: A survey. Big Data Research, 23, 100170.

[5] Jurgovsky,J., Granitzer,M., Ziegler, K.,Calabretto, S.,Portier, P.E., He-Guelton, L., & Caelen,O.(2018).Sequence classification for credit-card fraud detection. Expert Systems with Applications,

100, 234–245.

[6] Bauder, R., & Khoshgoftaar, T. M. (2018). A survey of credit card fraud detection techniques: Data and technology perspectives. Journal of Big Data, 5(1), 1–33.

[7] Douglass,R.,Zhao,Z.,& Khoshgoftaar,T.M.(2020).Financial fraud detection using graph-based deep learning. IEEE Access, 8, 129795–129807.

[8] Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009).Transaction aggregation as a strategy for credit card fraud detection. Data Mining and Knowledge Discovery, 18, 30–55.

[9] Li, W., & Sun, L. (2020). A survey on credit card fraud detection techniques using machine learning. Journal of Financial Crime, 27(3), 771–786.

[10] Bahnsen,A.C.,Aouada,D.,Stojanovic,A.,&Ottersten,B.(2016).Featureengineeringstrategies for credit card fraud detection. Expert Systems with Applications, 51, 134–142.

[11] Ahmed,F., Mahmood,A.N.,& Hu,J.(2016).A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.

[12] Roy,S.,& Jain,S.(2021).Credit card fraud detection using machine learning: A review. Materials Today: Proceedings, 45, 1633–1640.

[13] Phua,C., Alahakoon,D.,& Lee,V.(2004).Minority report in fraud detection: Classification of skewed data. ACM SIGKDD Explorations Newsletter, 6(1), 50–59.

[14] Dal Pozzolo, A.,Caelen, O.,LeBorgne, Y.,Waterschoot, S., & Bontempi,G.(2015). Calibrating probability with under sampling for unbalanced classification. 2015 IEEE Symposium Series on Computational Intelligence, 159–166.

[15] Ghosh, S., & Reilly, D. L. (1994). Credit card fraud detection with a neural-network. Proceedings of the 27th Annual Hawaii International Conference on System Sciences, 3,621– 630.