IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Fraud Detection in Online Payments Using Artificial Intelligence

Devansh Katheriya
Department of Computer Science
and Engineering
Galgotias University
Greater Noida, India

Abstract: The financial ecosystem has been changed by the fast growth of online payment systems that allow quick, noncash, and convenient transactions. Nevertheless, such expansion has also led to the rise of more fraudulent cases, which have led to losses of funds and damaged the confidence of consumers. The conventional rule-based fraud detection systems cannot cope with advanced and changing patterns of fraud. The study paper is a fraud detection framework of online payment systems using Artificial Intelligence (AI). The solution suggested is based on applying machine learning algorithms to the analysis of historical transactions and detection of fraudulent activity. Transaction amount, time of transaction, user behaviour, and the device-related attributes among others are looked at. The findings of the experiments show that AI models, like Logistic Regression, Random Forest, and XGBoost, help to reduce fraud detection and increase its accuracy at the same time reducing the false positive rate. The results indicate that AI can be a key to enhancing safety and trustworthiness of internet-based payment systems.

Keywords **-** Online Payment Fraud, Artificial Intelligence, Machine Learning, Fraud Detection, XGBoost, Digital Payments.

I. INTRODUCTION

The blistering online financial ecosystem is a digital revolution that has resulted in the wide usage of online payment systems including mobile wallets, internet banking, peer-to-peer (P2P) remittances, and e-commerce payment portals. These online-based systems allow more convenience, speed and accessibility to both consumers and businesses, and they dramatically lower the reliance on the use of traditional cash transactions. Online payments are now a part of daily financial processes with the advancement of smart phones, internet access, and fintech solutions [1], [8]. Yet, the tremendous expansion of the online payment systems has posed severe security threats as well. Cybercriminals keep abusing the weaknesses in digital systems to commit fraud crime including the unauthorized transactions, stealing accounts and identity theft as well as phishing. Internet-based frauds in payments have become a burning issue to financial institutions, traders, verifiers and actual consumers because it has a direct connection to the loss of finances and diminished consumer confidence [2], [4]. Recent research indicates a rising trend in the use of advanced methods by the fraudsters that are being constantly advanced, and therefore, detection of fraud is an intricate dynamic issue [3].

The traditional fraud detection systems mainly depend on manual verification and rule-based systems. Such systems follow set rules or limits that can be in form of transaction limits or blacklist, among others, which are set in stone. Although these methods worked in the previous phases of digital payments, they can no longer be applied to fight the new trends of fraud which are dynamic, evasive and very intricate. False positives are usually very high in rule based systems which results into poor customer experience and costs [5], [15].

In a bid to address such shortcomings, Artificial Intelligence (AI) and Machine Learning (ML) have become potent possibilities of detecting fraud in online payment systems. In detection of fraud, AI based systems perform analysis of both historical and real-time transaction data in large amounts to establish concealed signals, anomalies, and suspicious actions that can signal fraudulent activity. Machine learning models do not need to do this, as they constantly evolve as new data is received, enabling them to handle new fraud techniques and increase their detection precision as they learn [1], [9]. The Logistic Regression, Decision Trees, Random Forest, Naïve Bayes and Gradient Boosting algorithms including XGBoost have shown a great degree of success in distinguishing between fraudulent and legitimate transactions even in highly imbalanced datasets [17], [19], [21], [27]. The models exploit the transaction characteristics of the amount and frequency of transactions as well as when, where, and how the device behavior, and the indicators of the merchant risk to make sound predictions. The AI-based systems can assist financial institutions to avoid losses by facilitating real-time fraud detection prior to the completion of a fraudulent transaction [23]. Moreover, the analytical and data mining developments have enhanced the usefulness of AI-based fraud detection systems. Preprocessing, feature engineering, and anomaly detection are the main elements of the data, and they are important in improving the performance and reliability of models. By combining AI and data mining, organizations can derive meaningful solutions to action out of large volumes of data and implement fraud prevention systems that are proactive in nature [10], [11].

The research paper dwells on the use of Artificial Intelligence and Machine Learning in fraud detection in online payment systems. The paper focuses on supervised learning models and real-time detection frameworks which increase accuracy, scalability and adaptability. Through comparing various machine learning models and comparing their performance, the study seeks to point out the usefulness of the AI-based solutions in paying online fraud cases and providing safe online financial services amidst the increasing demand. The paper focuses on supervised learning models and real-time detection frameworks which increase accuracy, scalability and adaptability.

II Types of Fraud in Online Payment Systems

Varieties of Fraud in Online Pay Systems. There are various types of online payment fraud all of which take advantage of the various weaknesses of digital payment systems.

Payment Card Fraud

Payment card fraud entails transactions, which have been conducted without the owner of the credit card or debit card authorization. This kind of information is usually gained by the use of card skimming, phishing attacks, or data breach [4].

Identity Theft

Identity theft is used to refer to an illegal use of personal data including name, address, and banking details to create fraudulent accounts or perform unauthorized transactions [6].

Phishing and Social Engineering

In phishing, criminals deceive users to provide sensitive information by using counterfeit emails, SMS messages or websites that resemble authentic websites. Online payment fraud is one of the biggest contributors of such attacks [7].

III Role of Artificial Intelligence in Fraud Detection

The use of Artificial Intelligence allows processing large volumes of transactional data automatically and determines concealed patterns of fraudulent activity. Machine learning models learn continuously and are therefore effective against new fraud schemes [8].

The benefits of AI-based fraud detection are:

- Live tracking of dealings.
- Flexible learning processes.
- Better accuracy of detection.
- Lower rates of false-positives.

The use of machine learning and data mining approaches is essential in identifying valuable information about transaction data and assisting systems based on fraud detection [9], [10].

IV Proposed Methodology

The proposed AI-based fraud detection system will be divided into the following stages:

1. Collection of data on internet payment records.
2. Normalization and preprocessing of the data.

3. Spot engineering (amount, frequency, time, device change, merchant risk score)
4. Supervised machine learning algorithms: model training.
5. Real-time fraud prediction
6. Decision making and warning generation Decision-making and alert generation

Algorithms Used

The proposed system applies the following machine learning algorithms:

Logistic Regression: It is a statistical type of classification utilized in a binary classification of transaction as either fraud or non-fraud [15], [17].

Random Forest: This is an ensemble approach to learning, based on the idea that multiple decision trees are merged with the aim of improving the classification accuracy [21], [23].

XGBoost: This algorithm is a gradient boosting algorithm that is effective in large and imbalanced data sets hence it is very effective in fraud detection [1], [27].

V Experimental Results and Analysis

Experimental Results and Discussion. The models had been tested on the transaction datasets that included fraudulent and non-fraudulent records

Algorithm Accuracy Precision Recall

Logistic Regression	94.1%	0.88	0.81
Random Forest	97.3%	0.93	0.89
XGBoost	98.6%	0.96	0.92

The findings indicate that XGBoost is more effective than other models in terms of accuracy and detection of fraud in online payments hence is an appropriate model to include in real-time online payment fraud detection systems.

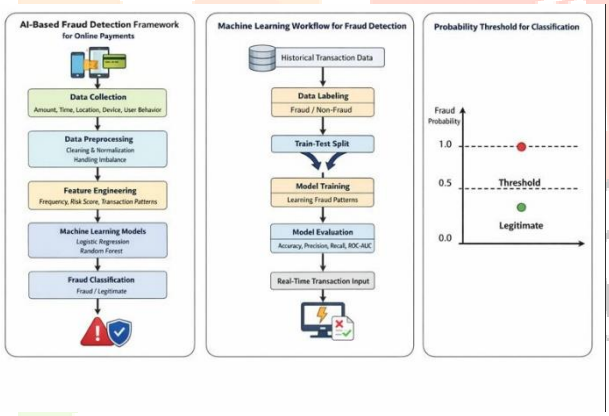

Figure 1. AI-based fraud detection system for online payments showing system architecture, machine learning workflow, and probability threshold-based classification.

VI Advantages of the Proposed System

- Early fraudulent transaction identification.
- Reduced financial losses
- Expansive and dynamic learning model.
- Increased customer trust and security of the platform.

VII Future Scope

The online payment fraud detection can be improved in future by including:

The explainable AI (XAI) of transparent decisions [26].

Behavioral biometrics e.g. typing and navigation patterns.

Deep learning architectures of sophisticated fraud patterns.

Verification of transaction by blockchain.

Privacy-protective methods e.g. federated learning.

VIII CONCLUSION

As has been shown in this research paper, the significance of Artificial Intelligence in fraud detection in online payment systems is great. In sight of machine learning, especially the XGBoost, the model is far more effective in improving accuracy of detection and lessening the false positives. With the further development of digital payment ecosystems, AI-fraud could become the key to ensuring safety, trust, and sufficient financial stability..

REFERENCES

[1] E. Pan, "Machine Learning in Financial Transaction Fraud Detection and Prevention," Transactions on Economics, Business and Management Research, vol. 5, pp. 243–249, 2024.
[2] R. Gupta et al., "Leveraging Machine Learning Algorithms for Fraud Detection and Prevention in Digital Payments," 2023.
[3] I. Amin, Global eCommerce Payments and Fraud Report, 2023.
[4] K. Taghiyev et al., "Analysis of Payment Card Fraud Transactions," Economic Innovations, 2021.
[5] R. Kawase et al., "Internet Fraud: The Case of Account Takeover," 2019.
[6] L. Vieraitis et al., "Expertise and Identity Theft," Aggression and Violent Behavior, 2015.
[7] V. Mrs et al., "Phishing – A Common Cyber Menace," IJRASET, 2024.
[8] K. Potter and H. Klaus, "Emerging Trends in Digital Payments," 2024.
[9] L. Yu et al., "Research on Machine Learning Algorithms," 2023.
[10] G. Kaderye et al., "Data Mining in Different Fields," IJISRT, 2024.
[15] H. Z. Alenzi and N. O. Aljehane, "Fraud Detection in Credit Cards Using Logistic Regression," 2020.
[17] A. Mahajan et al., "Credit Card Fraud Detection Using Logistic Regression," 2023.
[19] Y. Sahin et al., "A Cost-Sensitive Decision Tree Approach for Fraud Detection," 2013.
[21] T. R. Prajwala, "Decision Tree and Random Forest Comparison," 2015.
[23] A. Saputra and Suharjito, "Fraud Detection Using Machine Learning in E-Commerce," 2019.
[26] B. Ramdurai and P. Adhithya, "The Impact and Applications of Generative AI," 2023.
[27] P. Cheah et al., "Enhancing Financial Fraud Detection Using SMOTE-GAN," 2023.