International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Online Payment Fraud Detection using Machine Learning in Python

Ms. Arokiya Abinaya A[1], Mr. V Murugesan[2]

[1]Student of 11 MSC (Computer Science), Department of Science with Computer Science,V LB Janakiammal College of Arts and Science, Kovaipudur , Coimbatore, India.

[2]M.Sc., M.Phil., (Ph.D)., Head of the Depatment, Department of Science with Computer Science, VLB Janakiammal College of Arts and Science, Kovaipudur, Coimbatore, India

ABSTRACT

The simplicity of making payments from anywhere in the world has made online payments increasingly attractive. Over the past few decades, there has been a significant rise in the use of e-payments. These electronic payment methods not only benefit consumers but also help businesses generate substantial revenue. However, the ease of electronic payments also comes with an increased risk of fraud. Consumers must ensure that their payments are directed exclusively to the correct service providers. Cases of online fraud can lead to the compromise of personal data and result in the inconvenience of needing to report the fraud, block payment methods, and take other necessary actions. For businesses, online fraud can lead to challenges as they may need to issue refunds to maintain customer trust. It is crucial for both consumers and businesses to be aware of potential internet scams. This study presents a model to determine whether an online payment is fraudulent. The model considers various factors, such as the type of payment and the identity of the recipient, to assess the legitimacy of online transactions.

Keywords: Online Fraud Detecion, Machine Learning (ML), .

INTRODUCTION

Online payments have become increasingly popular over the last few decades due to their convenience, allowing people to send money from anywhere. The pandemic has significantly contributed to the rise in e-payments as well. Numerous studies indicate that e-commerce and online payments will continue to grow in popularity in the coming years. However, with this increase in online payments, the risk of online payment fraud has also risen. Evidence shows that online payment fraud has escalated in recent years, making it essential for consumers and service providers to stay vigilant. It is crucial for users to ensure that the payments they make are going to legitimate recipients; otherwise, they risk having to report fraud, freeze their payment methods, and may even expose their data to criminals, which could lead to additional crimes. On the flip side, businesses must verify that their customers are not inadvertently sending money to fraudsters. Companies may be required to reimburse clients to maintain their trust, which can put a financial strain on them. Although many firms have developed fraud detection programs, only a few are effective in identifying online payment fraud. Despite companies' best efforts to make payment methods as secure as possible, fraudsters sometimes manage to bypass security measures and commit online payment scams.

OBJECTIVE

The primary objective of this project is to develop a secure web-based application that prevents credit card fraud by implementing multi-level authentication and real-time transaction monitoring. The system aims to provide enhanced security measures to protect users from unauthorized transactions and financial losses.

The specific objectives of the project are:

1. To develop a secure user authentication system that requires registration and loginwith a username, password, and two-factor authentication (2FA) using OTP verification.

2. To implement a purchase threshold mechanism, allowing users to set a transaction limit, preventing unauthorized high-value transactions.

3. To integrate a multi-level authentication system, where users must answer a security question and enter an OTP for verification if a transaction exceeds the set threshold.

4. To automatically block transactions and disable the credit card if authentication fails, preventing fraudulent activities.

5. To store and monitor transaction data securely, enabling users to track their purchase history and detect suspicious activities.

6. To enhance security through encryption techniques to protect sensitive user information, such as credit card details.

7. To provide an admin panel for monitoring fraudulent activities, managing users, and ensuring system security.

By achieving these objectives, the project will ensure secure digital transactions, minimize the risk of credit card fraud, and provide users with a reliable and fraud-resistant online payment system.

SCOPE OF STUDY

The scope of this study focuses on developing a secure web-based application that effectively prevents credit card fraud through multi-level authentication and threshold-based verification. The system begins with user authentication and registration, where users provide personal details such as email, phone number, and credit card information securely. A secure login process using a username and password is implemented, along with two-factor authentication (2FA)via OTP verification through email or SMS for added security.

Once logged in, users can browse, select, and purchase products within the application. All purchase transactions are securely stored in a database, allowing users to track and review their purchase history. A key feature of the system is the ability for users to set a purchase threshold limit, preventing unauthorized or high-value transactions. If a purchase exceeds the specified threshold, the system triggers a multi-level verification process to ensure the transaction is legitimate.

During high-risk transactions, the system first asks the user a pre-set security question. If the user provides the correct answer, an OTP (One-Time Password) is sent to their registered email. Only after both authentication steps are successfully completed will the transaction be processed. If the authentication fails, the system automatically blocks the transaction and the card, preventing any fraudulent activities.

To enhance security, the system integrates encryption techniques to protect sensitive user data and implements fraud detection algorithms to monitor transaction patterns. Additionally, automated alerts notify users and administrators of any suspicious activities. The admin panel allows for user management, fraud monitoring, and security settings adjustments, while users can update their security questions and threshold settings.

This system is highly applicable to e-commerce platforms, banking applications, and financial institutions, ensuring secure transactions and protecting users from unauthorized payments. By integrating multi-level authentication and threshold verification, this project aims to make online payments safer and more reliable, effectively reducing the risk of credit card fraud.

PROBLEM DEFINITION

With the rise of online shopping and digital transactions, credit card fraud has become a significant concern for both consumers and financial institutions. Cybercriminals often exploit vulnerabilities in e-banking systems, stealing sensitive user information such ascredit card details, usernames, and passwords for malicious purposes. Traditional fraud detection mechanisms often fail to prevent unauthorized transactions in real-time, leading to financial losses and compromised user trust.

To address this issue, a secure web-based application is needed to prevent credit card fraud by implementing multi-level authentication and transaction monitoring. This system will allow users to set purchase threshold limits, ensuring that transactions exceeding the limit trigger additional security verifications, such as security questions and OTP-based authentication. If an unauthorized user fails these verification steps, the system will block the transaction and disable the card to prevent misuse.

The absence of such a real-time fraud prevention system makes users vulnerable to financial threats, identity theft, and unauthorized purchases. Therefore, this project aims to enhance security in online transactions by integrating advanced authentication methods, reducing fraud risks, and ensuring safer digital payments for users.

LITERATURE REVIEW

Machine learning techniques like KNN, SVM, and Random Forest. When compared to the other algorithms employed in this study, Random Forest comes out to be the most accurate, with a 99.9 percent accuracy rate. Random forest also comes out to have the lowest rate of false alarms related to fraudulent transactions. Although Jain et al. (2020) did not use real-time data, it may still be useful in the future to help organizations like banks become aware of these scams. Ileberi et al. (2021) applied the AdaBoost method in addition to some supervised machine learning techniques like logistic regression, decision trees, and support vector machines (SVM) (2021).

Numerous research are being conducted using the data in a way that protects privacy. One of the experiments was carried out using blockchain technology and machine learning techniques, according to Kalbande et al. (2021). The usage of block chain technology, however, can be helpful in protecting the privacy of the data, but we cannot ignore the fact that it is a decentralized solution and has some drawbacks along with it, such as scalability issues and high energy consumption. A supervised machine learning strategy utilizing block chain technology was developed by Thennakoon et al. (2019).

These scammers' techniques change with time. Users learn that a certain transaction appears to be fraudulent as a result of the popularity of some approaches or procedures over time. The behavior of users or cardholders also evolves with time, making it challenging for new technology to keep up with fraud detection or protection. Therefore, it is crucial that the algorithms are updated frequently to keep up with these shifts in fraudsters' strategies. Saputra and Suharjito (2019). In order to create models, real-time 3 data is needed, but obtaining this data is challenging since it contains private information that can only be shared with corporations that collect payments and third-party companies that store the data.

METHODOLOGY

As the number of online auctions continues to rise, so does the prevalence of online auction scams. To avoid detection, scammers often mask their deceptive activities by posing as honest participants. Therefore, merely staying vigilant is insufficient for preventing scams. Online auction participants need a more proactive approach to protect their interests, such as implementing an early fraud detection system. Here are the steps to do this:

1. Install Required Libraries: Begin by installing the necessary libraries and dependencies for data preprocessing and model evaluation in Jupyter Notebook.

2. Obtain the Dataset: Download the online payment transaction dataset from Kaggle.

3. Clean the Dataset: Address missing values, outliers, and inconsistencies in the dataset. Additionally, convert payment types from categorical labels to numerical labels.

4. Split the Dataset: Divide the dataset into training and testing sets to evaluate the model's performance. Utilize a random forest classifier to train the model.

5. Evaluate Model Performance: Assess the trained model's performance on the testing dataset using metrics such as accuracy, precision, recall, and F1 score. Analyze the confusion matrix to gain insights into the model's ability to distinguish between fraudulent and non-fraudulent transactions.

6. Save the Model: Save the trained model to a file with a .sav extension for deployment. The Flask library will be utilized for deployment, as it is a micro web framework specifically designed for building web applications in Python.

7. Develop the Web Application: Using the Spyder application, develop the Python code within Flask to create a web app that can facilitate the detection of auction fraud.

FUTURE ENHANCEMENT

To enhance security and efficiency, future improvements to the credit card fraud detection system can include AI-based fraud detection using machine learnin to identify suspicious transactions in real-time. Biometric authentication (fingerprint, facial recognition) can provide an extra layer of security for high-risk transactions. Blockchain technology can be used to create tamper-proof transaction records, ensuring transparency and reducing fraud risks.

A mobile app with real-time fraud alerts via SMS, email, or push notifications can improve user experience. Geo-location tracking can detect unusual transaction locations, triggering additional verification. A voice-based OTP syste can replace traditional OTPs for faster authentication. Additionally, multi-bank integration will allow users to manage multiple credit cards and accounts in one platform.

For better fraud prevention, advanced reporting and analytics can help users track spending patterns and identify risks. Partnering with banks and financial institutions can enable automatic fraud reporting for immediate action. These enhancements will make the system more secure, intelligent, and user-friendly, ensuring safer online transactions.

CONCLUSION

In conclusion, the presented methodology offers a structured approach for developing and deploying a machine learning model aimed at online fraud detection. By adhering to these steps, organizations can effectively utilize data-driven techniques to reduce the risks associated with fraudulent online transactions. The process begins with the collection and preprocessing of relevant data, followed by the implementation of appropriate machine learning algorithms. This enables organizations to create models capable of differentiating between normal and fraudulent patterns. Through rigorous training, testing, and validation, the accuracy and reliability of the model are ensured before it is deployed in real-world settings. Once deployed, the model becomes a crucial part of the online fraud detection system. It continuously analyzes transactions in real time to identify suspicious activities. The model's effectiveness relies on ongoing monitoring and periodic updates to adapt to changing fraud tactics and maintain optimal performance. Ultimately, adopting machine learning for fraud detection not only enhances security but also strengthens the overall trust and integrity of online transactions, protecting both businesses and consumers from financial losses and reputational damage.

REFERENCES

[1]. Abdallah, Aisha, Mohd Aizaini Maarof & Anazida Zainal. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90-113.

[2]. Minastireanu, Elena-Adriana & Gabriela Mesnita. (2019). An analysis of the most used machine learning algorithms for online fraud detection. Informatica Economica, 23(1)

[3]. Zhang, Zhaohui, et al. (2018). A model based on convolutional neural network for online transaction fraud detection. Security and Communication Networks.

[4]. Minastireanu, Elena-Adriana & Gabriela Mesnita. (2019). Light gbm machine learning algorithm to online click fraud detection. J. Inform. Assur. Cybersecur, 263928.