Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 5, No. 3, May: 2023

ONLINE CREDIT CARD FRAUD DETECTION USING RULE-BASED ALGORITHM

Mrs. S. Priyanka, Assistant Professor, Dept. Of Information Technology, SNS College Of Engineering.
Email: priyankapriya710@gmail.com
Mrs. K. Revathi, Assistant Professor, Dept. Of Information Technology, SNS College Of Engineering.
Email: revathiks09@gmail.com
Mr. P. Mehesh, Student, Dept. Of Information Technology, SNS College Of Engineering.
Email: meheshmehesh131@gmail.com
Mr. M. UdhayaKumar, Student, Dept. Of Information Technology, SNS College Of Engineering.
Email: udhaya150313@gmail.com
Ms. T. Sneha, Student, Dept. Of Information Technology, SNS College Of Engineering.
Email: snehathangavelu146@gmail.com
Ms. P. Padma Chandini, Student, Dept. Of Information Technology, SNS College Of Engineering.
Email: chandiniammu191@gmail.com

Abstract

React Native is a popular open-source framework for building mobile applications using JavaScript and React. Fraud detection is the process of identifying fraudulent activities or transactions in a system. In this context, we can explore how React Native can be utilized for fraud detection in mobile applications. Fraud detection in mobile applications can involve a variety of techniques such as data analysis, machine learning, and pattern recognition. React Native can be used to develop custom user interfaces and visualizations for displaying relevant data to users. Additionally, React Native can be integrated with third-party libraries and APIs that provide fraud detection services, such as risk assessment, identity verification, and transaction monitoring.

One possible approach to fraud detection in React Native mobile applications is to use machine learning algorithms to analyse user behaviour and detect suspicious patterns. For example, algorithms could be trained to identify unusual login patterns or unusual purchase behaviour. The output of these algorithms could be displayed to users in real-time through custom React Native components. Another approach could be to integrate fraud detection APIs provided by third-party vendors. These APIs could be used to verify user identities, assess transaction risks, and monitor for fraudulent activities. The results of these APIs could be displayed to users through React Native components, allowing them to take appropriate actions such as cancelling transactions or reporting suspicious activities. In conclusion, React Native can be used to develop custom user interfaces and integrate with third-party libraries and APIs for fraud detection in mobile applications. Machine learning algorithms and fraud detection APIs can be leveraged to identify suspicious patterns and provide real-time feedback to users.

KEYWORDS: Credit card, electronic commerce, Fraud detection, Genetic algorithms.

1. INTRODUCTION

Ecommerce, also known as electronic commerce, has gained immense popularity since the advent of the World Wide Web (WWW). It enables Internet users to buy and sell products and services online, providing them with convenience and profitability. Websites such as eBay and Amazon are widely used for this purpose. The traditional model involves sellers setting a fixed price for their products or services, which buyers can purchase if they find it suitable. On the other hand, the online auction model works differently, where items are sold through price bidding. Sellers specify a starting price and an expiration time, and potential buyers bid against each other until the auction closes. The highest bidder wins the item.

However, like any other platform that supports financial transactions, online auctions also attract fraudulent activities by criminals. There are different types of auction fraud, which include non-delivery of purchased products by the seller, delivery of products that do not match their description, and the posting of non-existent items with false descriptions to deceive buyers. Some malicious sellers may also request payments to be wired directly to them via bank-to-bank wire transfer. In addition, criminals may use phishing techniques to steal high-rated seller accounts, which makes it easier for them to deceive potential buyers. Unfortunately, victims of fraudulent transactions often end up losing their money, which is usually irrecoverable. As a result, the reputation of the online auction services is hurt significantly due to fraud crimes.

2. LITERATURE SURVEY

The infrastructure that is expanding the quickest right now is the Internet. Many contemporary technologies are altering the nature of human activities in today's technologically advanced society. Despite the advancements in technology, it is difficult to completely protect our personal information, which has resulted in an increase in cybercrime. Brewer [1] claims that the phrases" ransom" and" malware" are the origin of the term" ransomware." It is a key element behind the surge of cyberattacks with the potential to make money off of victims. On the other hand, Noubir believes that in the past, hackers faced challenges in reaping the benefits of their attacks, but this is no longer true. Cybercriminals are rapidly using ransomware assaults, or attackers who access a victim's data, encrypt it, and demand a payment [2].

A form of virus called ransomware prevents users from using the attacked computer system. This type of technical extortion typically involves drive-by attacks on web pages that are intentionally designed to exploit software and hardware vulnerabilities.It appears in the form of Manamecrypt, CryptoWall, CryptoDefense, or Cryptolocker [3].

Most of the files they targeted were in document storage formats like Office, PDF, and CSV, so they utilized strong encryption to scrambled virtually all of them, rendering them hard to retrieve without the special, secret key used to encrypt them. After receiving money, the cracker posts a display notice on the computer screen outlining the steps to do in order to retrieve the encrypted files, which puts an end to crypto virology [4]. Ransomware is a highly advanced and malicious software that often masquerades as Crypto or Locker and is specifically designed to attack and seize control of computer systems and critical infrastructure. The great majority of these threats are intended to steal money from the victims either directly or indirectly by demanding a ransom in exchange for the decryption keys. To find possible solutions, this systematic research reviewed multiple academic resources and analyzed the structure, methods, and attack patterns of ransomware [5], [6].

Ransomware attacks have a severe impact on the information technology infrastructure. The impact of these attacks can cause system disruptions in most organizations, data loss due to file encryption, financial expenses for incident response, and other security-related challenges for businesses. Additionally, unplanned outages of critical medical equipment due to these attacks have resulted in fatalities [7].

Previous systematic reviews of ransomware have been documented in the literature. The fundamental problem with those earlier evaluations is that they mostly focused on ransomware in the healthcare industry and other specialized areas, despite the fact that it is generally recognized that ransomware has no clear domain boundaries. The comprehensive outline of the ransomware attack cycle and its characteristics discussed in this paper can serve as a foundation for further research on ransomware. Additionally, current ransomware detection methods are discussed, along with the advantages and disadvantages of each method. Furthermore, this paper will include a discussion on preventive measures and tools for defending against ransomware attacks.

Security lapses in computer networks can happen when a connection or network vulnerability is exploited to injure, undermine, or otherwise compromise the user. Attacks can be classified into two primary categories: active attacks and passive attacks. These use a variety of techniques and procedures to steal information, identities, or money actively or passively [8].

In 1989, Joseph L. Popp created the original ransomware virus. Joseph is acknowledged as the father of ransomware as well [9].

The Aids Trojan or PC Cyborg is a common reference to a ransomware threat. Both corporate and human adversaries can use ransomware. It may spread to PCs via infected USB sticks or any type of attachment or link in phishing emails. The most recent Trojan horse to emerge is ransomware, a serious threat that has been progressively increasing in recent decades. Ransomware poses a significant threat as it typically encrypts user

data or deletes vital information and only provides the decryption key after the victim pays a ransom. This is primarily because of... (the sentence is incomplete and needs more context to rephrase accurately) bitcoins' untraceable characteristics.

3. EXISTING SYSTEM

To provide some assurance against fraud, E-commerce sites often provide insurance to fraud victims to cover their loss up to a certain amount. To reduce the amount of such compensations and improve their online reputation, e-commerce providers often adopt the following approaches to control and prevent fraud. The identified registered users are validated through email, SMS, or phone verifications. A rating system where buyers provide feedbacks is commonly used in e-commerce sites so that fraudulent sellers can be caught immediately after the first wave of buyer com-plaints. Furthermore, proactive moderation systems are established to enable human experts to manually scrutinize suspicious buyers or sellers.

4. DRAWBACKS

- Even though e-commerce sites spend a large budget using manpower to fight frauds with a moderation system, there are still many outstanding and challenging cases.
- Criminals and fraudulent sellers frequently change their accounts and IP addresses to avoid being caught.
- Also, it is usually infeasible for human experts to investigate every buyer and seller to determine if they are committing fraud, especially when the e-commerce site attracts a lot of traffic.
- The patterns of fraudulent sellers often change constantly to take advantage of temporal trends. For instance, fraudulent sellers tend to sell the "hottest" products at the time to attract more potential victims.
- Also, whenever they find a loophole in the fraud detection system, they will immediately leverage the weakness.

5. PROPOSED SOLUTION:

The proposed application is to detect online auction frauds for a major Asian site where hundreds of thousands of new auction cases are posted every day. Each new case is forwarded to the proactive anti-fraud moderation system for pre-screening to evaluate the potential risk of fraud. The system will automatically detect auction frauds using machine learning.

6. FEATURES:

- By empirical experiments on a real-word online auction fraud detection data, the proposed system will combine online feature selection, bounding coefficients from expert knowledge and multiple instance learning.
- The system can significantly improve over baselines and the human-tuned model.
- This online modeling framework can be easily extended to many other applications, such as web spam detection, content optimization and so forth.

7. MODULES

- Rule-based features
- Linear scoring function
- Selective labeling
- Fraud churn
- User feedback

Rule-based features

Human experts with years of experience created many rules to detect whether a user is fraud or not. One instance of these rules is a "blacklist," which detects whether the user has a previous record of fraud or has been reported as fraudulent. Each rule can be considered as a binary feature that denotes the likelihood of fraud.

Algorithm

Rule-based algorithm for fraud detection:

Let's say we have a credit card processing system that needs to identify fraudulent transactions. We can develop a rule-based algorithm that flags transactions that meet certain criteria. For example:

1. If a transaction amount is above a certain threshold, say $10,000, flag it as suspicious.
2. If a transaction occurs outside of the cardholder's usual geographic location, flag it as suspicious. This can be determined by comparing the transaction location to the cardholder's previous transaction locations.
3. If a transaction occurs during unusual hours, flag it as suspicious. For example, transactions that occur between midnight and 6:00 am could be flagged as suspicious.
4. If multiple transactions occur in quick succession, flag them as suspicious. For example, if a cardholder makes three transactions within a minute, flag them as suspicious.
5. If a transaction is made using a card that has been reported stolen, flag it as suspicious.

These rules can be combined and weighted to calculate an overall risk score for each transaction. Transactions that exceed a certain risk score can be flagged for further review by fraud analysts. The rules can be adjusted over time based on the analysis of historical data and the evolving nature of fraud patterns.

Linear scoring function

The existing system only supports linear models. Given a set of coefficients (weights) on features, the fraud score is computed as the weighted sum of the feature values.

Selective labelling

If the score indicating the probability of fraud is higher than a set threshold, the case will be placed in a queue for manual examination by human experts. After the examination, the result will be marked as either fraud or not. Cases with higher scores will be given higher priority in the queue for review. Those with scores below the threshold will be automatically labeled as clean by the system, without requiring any human intervention.

Fraud churn

When a case is labeled as fraud by human experts, it indicates that the seller is not trustworthy, and there is a possibility that they are selling other fraudulent items as well. Consequently, all items submitted by the same seller are also marked as fraud. The website takes swift action to remove the fraudulent seller and their cases from the platform once detected.

User feedback

Buyers can lodge complaints to request N posterior samples of βt. The system can thus obtain the posterior loss if they are recently deceived by fraudulent sellers.

8. SYSTEM SPECIFICATION

HARDWARE SPECIFICATION

CPU	: Intel i5 3GHz
RAM	: 8 GB
Hard Disk	: 800 GB
Monitor	: 14 SVGA
Mouse	: 2 Button
Keyboard	: 104 Keys
System bus	: 64 bits
Mother Board	: Intel

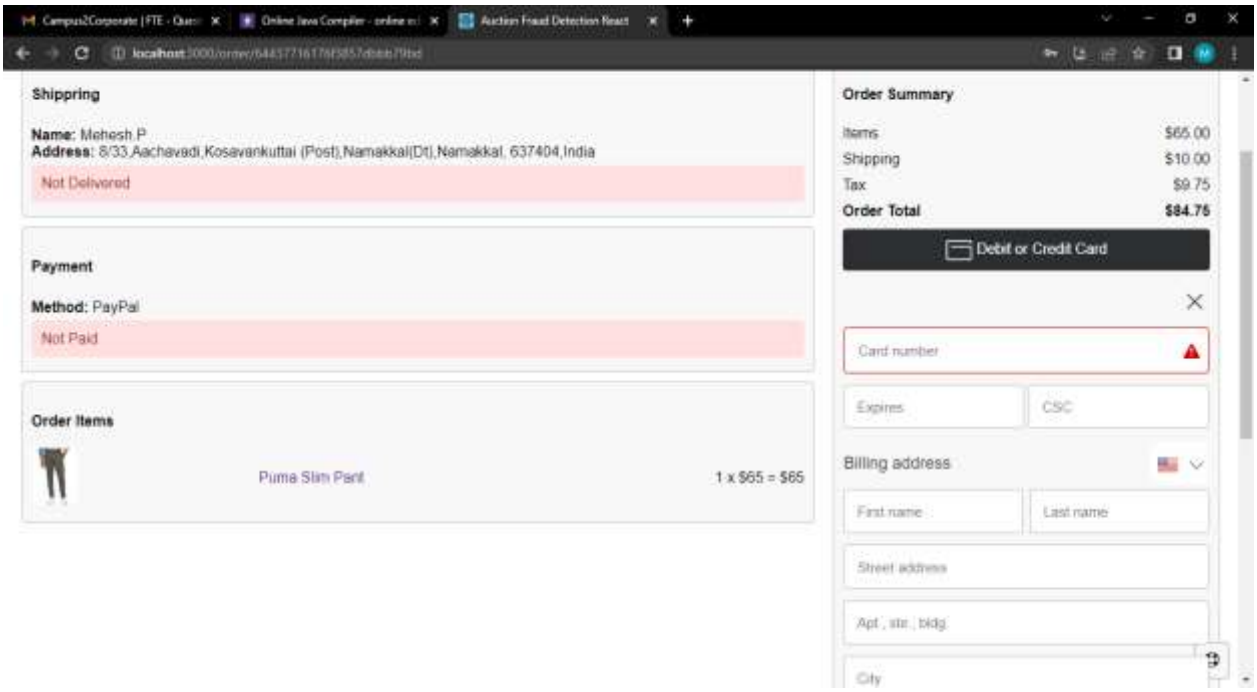
SOFTWARE SPECIFICATION

Operating System	: Windows 10
Front End	: Node JS, React Native CLI, NPM
Back End	: MySQL or MongoDB

Industrial Engineering Journal
ISSN: 0970-2555
Volume: 52, Issue 5, No. 3, May: 2023

IDE : Android studio / Visual code

9. SOURCE CODE:



10. CONCLUSION:

The software is completely menu driven and extremely user friendly since it is developed in an efficient front-end tool. Appropriate error messages are provided to guide the user in a proper and user-friendly manner. Time consumptions are reduced to a great extent and user has less complexity in handling the system. End users will be very much satisfied with the software. Tables are designed with primary keys and foreign keys in order to establish relationship between tables. Flow diagrams have been created to provide insights into the implementation process.

All the type of updating can be made through system whenever necessary. The software created is attractive and user-friendly. It is highly interactive too. The software's menu-driven approach provides greater flexibility and minimizes the need for extensive user typing. The system reduces workload and produces adequate and timely information as and when required. Software has been developed and tested.

SUGGESTIONS

Although this system almost satisfies all the requirements of the user (admin), there is further development in this system into a better from in the following are as follows.

- Further security can be improved.
- Check the availability of the products.
- The design of this package can be extended.
- Future enhancement can also be done.

11. REFERENCES:

1. S. Kamil, H. S. A. Siti Norul, A. Firdaus and O. L. Usman, ”The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges,” 2022 International Conference on Business Analytics for Technology and Security (ICBATS), 2022, pp. 1-7, doi: 10.1109/ICBATS54253.2022.9759000.
2. Yazdinejad, Abbas, Reza M. Parizi, Ali Dehghantanha, Qi Zhang, and Kim-Kwang Raymond Choo. ”An energy-efficient SDN controller architecture for IoT networks with blockchain-based security.” IEEE Transactions on Services Computing 13, no. 4 (2020): 625-638.

3. Ekta and U. Bansal, ”A Review on Ransomware Attack,” 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), 2021, pp. 221-226, doi: 10.1109/ICSCCC51823.2021.9478148.
4. C. C. Joseph, ”After Angler: Shift in Exploit Kit Landscape and New Crypto-Ransomware Activity”, Trend Micro White paper, 2017.
5. M. P. Zavarsky and D. Lindskog, ”Experimental Analysis of Ransomware on Windows and Android Platforms : Evolution and Characterization”, vol. 94, pp. 465-472, 2016.
6. Yazdinejad, Abbas, Reza M. Parizi, Ali Dehghantanha, and Kim-Kwang Raymond Choo. ”P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking.” Computers & Security 88 (2020): 101629.
7. Aaron Zimba, ”Malware-Free Intrusion: A Novel Approach to Ransomware Infection Vectors”, International Journal of Computer Science and Information Security, vol. XV, no. 2, pp. 317, 2017.
8. Zimba A, Wang Z, Chen H (2018) Multi-stage crypto ransomware attacks: a new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express 4(1):14–18.
9. Cohen A, Nissim N (2018) Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. Expert Syst Appl 102:158–178.