Online Transaction Fraud Detection System Based on Machine Learning

Virjanand[1], Rajkishan Bharti[2], Shubham Chauhan[3], Suraj Pratap Singh[4], Chhiteesh Rai (Assistant Professor)[5]

[1-5]*Computer Science and Engineering, Institute of Technology and Management, Gida Gorakhpur, U.P*

ABSTRACT: - *Transaction fraud is a major cause of concern. As online transactions become more popular, so do the types of online transaction fraud that accompany them, affecting the financial industry. This fraud detection system is capable of restricting and impeding an attacker's transaction using credit card information of a genuine user.*

By allowing transactions that exceed the customer's current transaction limit, this system was designed to address these issues. In order to detect fraudulent user behavior, we gather the necessary information at registration. The details of items purchased by any individual transaction are generally unknown to any Fraud Detection System (FDS) running at the bank that issues credit cards to cardholders. BLA is being used to resolve this problem (Behavior and Location Analysis). A FDS is a credit card issuing bank. Every pending transaction is sent to the FDS for approval. To determine whether or not the transaction is genuine, FDS receives the card information and transaction value.

The FDS has no understanding of the technology purchased in that transaction. The bank refuses the transaction if FDS confirms it is fraudulent. If an unexpected pattern is identified, the system must be re-verified using the users' spending habits and geographic location. The system detects unusual patterns in the payment procedure based on the user's previous information. After three unsuccessful attempts, the system will ban the user.

The new electronic transaction era needs the detecting of fraud in online transactions. It's extremely difficult to improve the consistency and stability of the fraud detection model because customer transaction patterns and offenders' fraud behavior are constantly changing. In this report, we'll examine about how a deep neural network's loss function affects the acquisition of deep feature representations of legitimate and fraudulent transactions.

With the increasing use of technology, people all over the world were increasingly turning to online transactions rather than cash in their daily lives, opening up plenty of growth possibilities for fraudsters to use these cards in unscrupulous ways. According to the Nilsson research, global losses are estimated to exceed $35 billion by 2020. The credit card firm should create a programmer that protects these credit card users from any threats they may face in order to secure their security. As a result, we use Kegel's IEEE-CIS Fraud Detection dataset to demonstrate our system for predicting whether transactions are authentic or fraudulent.

Keywords: Fraud Detection, Fully Connected Neural Network, Online transaction, credit cards, Long bi-directional gated repeated unit and long bi-directional memory (BiLSTM)

1. INTRODUCTION

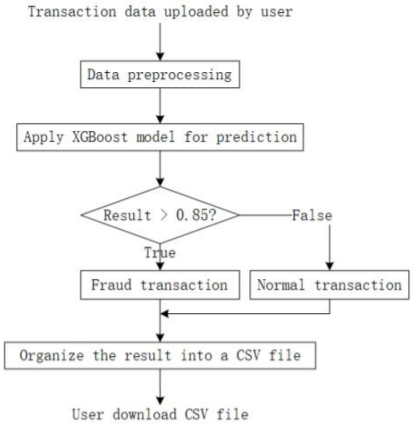
Online transaction fraudsters and detectors has performed a complex role for a long time. Transaction fraud is much more common than ever before, specifically in the Internet age, and it results in significant financial losses. The Nilsson study looked at the global scenario around online transaction fraud in great detail. In 2015, online transaction fraud cost the economy approximately $21 billion, $24 billion in 2016, and more than $27 billion in 2017. Year after year, the global rate of online transaction fraud is predicted to climb, reaching $31.67 billion in 2020.

As a result, banks and financial service providers may be required to develop an automated online fraud detection system to detect and monitor online transactions. Fraud detection systems are meant to discover and track incoming transactions by separating anomalous activity patterns from a large number of transactional records. Machine learning has proven to be extremely effective at identifying these patterns. Alternatively, a large number of transaction records could be utilized to train a high-performing fraud classifier. Despite the fact that supervised learning has proven to be incredibly effective in detecting fraudulent transactions, transactional fraud analysis technology will continue to progress. Small improvements might also save a lot of money for a company. The novel technique of unsupervised and controlled online fraud spotting has some flaws.

On the other side, classifiers were used to automatically distinguish between suspicious and non-suspect transactions using machine learning (ML) methods. As a result, by analyzing the patterns of data in a correctly classified dataset, a combination of machine learning and data mining algorithms was able to distinguish genuine

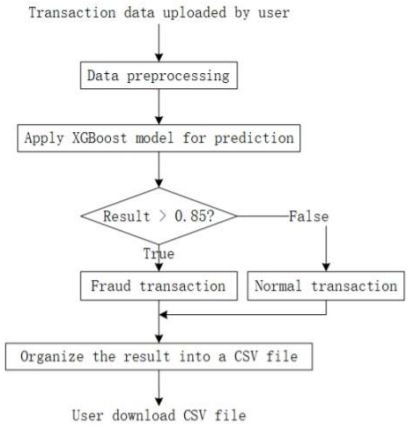
from non-genuine transactions. KNN, NB, and SVM are the most often utilized fraud detection approaches. These strategies can be used alone or in combination with group or meta learning techniques to build classifiers.

ACL, a new loss functionality, is introduced to improve the distinguishability of the functions that are learned. ACL is an improved SL feature since it overcomes the issue of maximum angle separation. We make a new FCL by merging ACL and DCL. FCL ensures a better potential to map initial transaction attributes into even more distinct deep representations by taking into consideration the distance and angle of transaction features. We explain and compare state-of-the-art loss functionality utilized in deep representation learning algorithms using two massive data sets. In terms of performance, we also show that our model is more accurate.



System Flow Chart

Information mining is the process of using big data analytical tools to find previously unknown, significant patterns and relationships in big data sets. Mathematical calculations, factual models, and machine learning methods are examples of these devices (for example, Neural Networks or Decision Trees). As a result, information mining entails more than just data gathering and maintenance; it also entails inquiry and prediction. Information mining can be done on textual, quantitative, or multimedia structures to extract information. Affiliation, characterization, sequence or way investigation, clustering, and forecasting are all examples of this. Detecting credit card fraud using standard methods is a risky undertaking.



Fraud Transaction Detection Model

As a result, whether in the academic, association, or business network recently, the creation of an online transaction fraud detection model has become increasingly important. Proposed or current models are typically insights-driven or AI-based, which have the potential advantage of not imposing counterfeit suspicions on the information variables.

2. LITERATURE REVIEW

S. Nami and M. Shagari [1] developed a strategy for detecting suspicious transactions. They've presented a transaction time-based similarity metric that gives recent transactions greater weight. They used a random forest method for early detection at first, and then a minimum risk model to detect payment fraud involving expenses later. Recent cardholder transactions had a stronger impact on assessing whether a transaction is fraudulent or not, according to the experimental results, which were done using a real dataset from a bank.

A.D. Pezzoli et al. [2] presented the performance measures for fraud detection. They've proposed a learning technique that takes class imbalance and verification latency into account. They put a lot of focus on using feedback to train the classifier. They demonstrated the influence of class imbalance and concept drift using a large dataset containing millions of credit card transactions.

A. Kumar and Gupta [3] used supervised machine learning techniques on credit card transactions to detect fraud. Nearest neighbor, logistic regression, linear SVM, decision tree, random forest, naive Bayes, and RBF SVM were all used, with logistic regression exceeding all of them.

The proposed Markov process structures are inefficient at representing habits [4-6]. We propose BP's abstract Graph (LGBP) as a command-based paradigm for capturing the reasoning link between transaction record characteristics in this study. Using LGBP transactions and user information, we can calculate a route dependent conversion Probability from one attribute to the next. Simultaneously, we construct a diversity coefficient based on knowledge entropy to evaluate a user's transaction behavior diversity. A transition probability matrix is also described for recording the time aspects of a user's transactions. As a result, we'll develop a BP that any user may use to assess whether or not an item is acceptable. The incoming transaction is valid. Our analysis of a real-world data set demonstrates that our method outperforms three other oneness models.

First, we propose formulating the issue of fraud detection with the use of a business associate [7], which explicitly specifies the operating conditions of FDSs that analyses large streams of online transactions on a regular basis. We'll show you how to detect fraud using the most effective performance criteria. Second, we develop and test a novel instructional strategy for dealing with problems. Third, we use nearly 75 million transactions in real-world outcomes accepted over a three-year period to demonstrate how class effects imbalance and concept swing in our investigations.

In present era, credit cards are commonly used as a necessary mode of payment. People used credit cards for a number of reasons, such getting credit, obtaining a loan, making quick payments, and using a charge card. There are some contentious issues that have been addressed, not just in terms of the amount of credit flooding the country's economy, but also in terms of the amount of transactions that result in payment default and the number of credit card fraud cases that have been recorded, both of which endanger the economy [8]. However, as technology has advanced and consumer behavior has changed, credit cards have become more prominent and useful in continuing to conduct business. According to the findings, there is a positive relationship between consumption rate and income. As according common perception, a substantial percentage of credit card issuers typically accept. According common belief, a large percentage of credit card issuers grant higher credit limits to people with higher incomes. In conclusion, it was noted that credit card issuers mostly target higher-income clientele. Massive purchases allow customers to avoid carrying cash and are helpful for online purchases and rental collateral. In any event, the emergency is that it is unsuitable for religious reasons because interest payments will be imposed if the unusual sum is not paid in full.

The ambiguity associated with card not present (CNP) [9] transactions, as well as the Internet, create unique fraud management issues. Authentication of the cardholder is a must when it comes to preventing Internet fraud. There aren't any standard setups. As a result, credit card theft on the Internet is significantly higher than in physical or even telephone situations.

3. CONCLUSION

In this review paper presents the various methods for detecting online transactions fraud. Its provide the insight of various research paper in the field of online transaction fraud detection which can be effectively applied to provide the solutions of the problems characteristic in the detection and prevention of fraud. In future studies, the machine learning algorithms may be used with different arrangements of input and output considerations for the detection of fraud online transactions.

REFERENCE: -

[1] S. Nami and M. Shajari, "Cost-sensitive payment card fraud detection based on dynamic random forest and k-nearest neighbors," Expert Syst. Appl., vol. 110, pp. 381–392, Nov. 2018.

[2] A. D. Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," IEEE Trans. Neural Netw. Learn. Syst., vol. 29, no. 8, pp. 3784–3797, Aug. 2018.

[3] A. Kumar and G. Gupta, "Fraud Detection in Online Transactions Using Supervised Learning Techniques," in Towards Extensible and Adaptable Methods in Computing, S. Chakraverty, A. Goel, and S. Misra, Eds. Singapore: Springer Singapore, 2018, pp. 309–321. https://doi.org/10.1007/978-981-13-2348-5_23

[4] X. Wu, R. He, Z. Sun, and T. Tan, A light CNN for deep face representation with noisy labels, IEEE Trans. Inf. Forensics Security, vol. 13, no. 11, pp. 2884–2896, Nov. 2018.

[5] Y. Wen, K. Zhang, Z. Li, and Y. Qiao, A discriminative feature learning approach for deep face recognition, in Proc. Eur. Conf. Compute. Vis. (ECCV). Cham, Switzerland: Springer, 2016, pp. 499–515.

[6] J. Dorronsoro, F. Ginel, C. Sgnchez, and C. Cruz, Neural fraud detection in credit card operations, IEEE Trans. Neural Netw., vol. 8, no. 4, pp. 827–834, Jul. 1997.

[7] D. Dighe, S. Patil, and S. Kokate, Detection of credit card fraud transactions using machine learning algorithms and neural networks: A comparative study, in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA). IEEE, 2018, pp. 1–6.

[8] Peter J. Bentley, Jungwon Kim, GilHo Jung and Jong-Uk Choi, "Fuzzy Darwinian Detection of Credit Card Fraud," In the 14th Annual Fall Symposium of the Korean Information Processing Society, 14th October 2000.

[9] Issue no. 4, pp.309-315, October December 2009