IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Literature Review On Identification Of Fraudulent Credit Card Fraud Detection Using Deep Learning

[1]Prof.Avinash Ingole, [2]Niyati Wagh, [3]Shrishti Nandanwar, [4]Ruchita Bharsakale, [5]Janhavi Raut

[1]Professor, [2]Student, [3]Student, [4]Student, [5]Student

[1]Department of computer engineering,

[1]Bharati Vidyapeeth College of Engineering Lavale, Pune, India

Abstract— Financial organisations, merchants, and cardholders are all concerned about credit card fraud. Various approaches and techniques have been developed and applied to reduce the dangers associated with fraudulent activity. The purpose of this literature review is to provide an overview of current research and achievements in credit card fraud detection. It discusses the primary approaches, algorithms, and datasets utilised in this discipline, emphasising the advantages and disadvantages of each approach. In addition, the paper analyses new trends, difficulties, and future perspectives for credit card fraud detection.

Keywords— Machine Learning, Fraud Detection, Auto-encoder, restricted Boltzmann algorithm.

I. Introduction

Fraud is a criminal offence committed with the intent of gaining financial gain. We are attempting to avoid losses due to fraud by employing two mechanisms: fraud detection and fraud prevention. Fraud prevention prevents fraud cases from occurring, while fraud detection occurs when an attacker performs a fraudulent transaction. These types of attackers use the owner's credit card to purchase online goods, and the owner is completely unaware of the process and is forced to pay for items that he or she did not acquire. Credit card fraud can occur both digitally and physically. Credit theft is common in physical transactions, but digital transactions occur when purchasing anything online. Credit card holders may enter credit card information when purchasing things on the internet or on a website. As a result, attackers strike when a person makes a purchase. We use machine learning to solve problems like these. However, this problem is difficult. It must look for the customer's number of transactions. In addition, the pattern must update or vary over time in accordance with statistical properties. There may be numerous hurdles in implementing these initiatives, such as payment requests being quickly evaluated by automated tools that choose which transactions to authorise. The algorithms utilised in this project have been trained to detect the appropriate output or report. These reports are then analysed by professionals.[10]

Types of Electronic Frauds-

Bankruptcy fraud: This section focuses on bankruptcy fraud and suggests using credit reports from credit bureaus as a source of information about the applicants' public histories, as well as a possible bankruptcy model implementation. One of the most difficult types of fraud to foresee is bankruptcy fraud. Some approaches or practises, however, may aid in its prevention. Bankruptcy fraud involves the use of a credit card while insolvent. In other words, buyers utilise credit cards knowing they will not be able to pay for their goods. The bank will send them a payment order. Customers will, however, be recognised as being in personal bankruptcy and unable to reclaim their debts. The bank will be required to cover the losses. This form of fraud loss is often excluded from the calculation of the fraud loss provision because it is considered a charge-off loss. The best method to prevent bankruptcy fraud is to conduct a pre-check with credit bureaus to learn about the customers' financial history.[11]

Theft fraud/counterfeit fraud: theft and counterfeiting are both types of fraud. This section discusses theft fraud and counterfeit fraud, which are connected. Using a card that is not yours is theft. The criminal will steal someone else's credit card and make use of it as frequently as feasible until the card is blocked. The sooner the owner reacts and contacts the bank, the sooner the banking institution may take steps to stop the thief. Similarly, counterfeit fraud happens when a credit card is used remotely; all that is required is the information associated with the card. At some point, someone will steal your card number and codes and use them on websites that do not require a signature or real cards. It is difficult to acknowledge and define a fraudulent transaction. Nonetheless, large-amount ATM transactions are suspicious and necessitate engagement with the customer. Purchases of goods for a higher value than usual will also be reported to the consumer, as will unusual overseas spending trends. Fraudulent transactions are frequently impossible to avoid since they take place in such a short period of time. However, once a card has been detected, it is prohibited[11].

Credit Card: Credit cards are used to purchase products and services. Both virtual and physical cards are available. Virtual cards are used to perpetrate fraud online, primarily via the internet or phone, by obtaining credit card information in an unauthorised manner. Offline, physical cards are utilised to commit fraud; the attacker must steal the credit card. When someone uses your credit cards without your consent, this is referred to as credit card fraud. They might use it to make purchases or withdraw money. When someone steals your physical credit card, credit card fraud occurs. It may also occur if your credit card information is stolen and used online. Identity theft is another type of credit card fraud. When someone uses your personal information to open a credit card in your name, this can happen. A burglar, for example, may apply for a credit card using your Social Security number without your knowledge. In 2019, there were over 270,000 cases of credit card fraud.[11]

Computer intrusion - Computer intrusion and computer security are two of the most important topics of research. There are numerous intrusion detection approaches offered to ensure network security, protect network resources, and protect network infrastructure. Intrusion detection systems (IDS) try to detect assaults by collecting network data and analysing it across several domains to identify potential incursions. This work offers an intrusion detection system (IDS) that combines three methodologies, such as anomaly detection, abuse detection, and a decision-making model, to improve detection accuracy and reduce false positives. The integrated IDS may be created to identify attacks in credit card systems using the Hidden Markov technique in the anomaly detection module, lowering the fraud rate and making the system more secure.[11]

II. LITERATURE REVIEW

Rimpal R. Popat with Jayesh Chaudhary:

They conducted a survey on credit card fraud detection, taking into account the three main types of fraud: insurance, corporate, and bank. The two methods of credit card transactions—i) virtually (card not present) and ii) with card or physically present—have been the focus of these. They concentrated on techniques including regression, classification, logistic regression, support vector machines, neural networks, artificial immune systems, K-nearest neighbour, naive bayes, genetic algorithms, data mining, decision trees, and fuzzy logic-based systems, among others. In which they provide theoretical foundation on the six data mining techniques of classification, clustering, prediction, outlier identification, regression, and visualisation. The discussed current statistical and computational techniques, including Artificial Immune System (AIS), Bayesian Belief Network, Neural Network, Logistic Regression, Support Vector Machine, Tree, Self-Organizing Map, and Hybrid Methods. They came to the conclusion that all of the current machine learning approaches listed above can offer high accuracy for the detection rate, and industries are eager to uncover new strategies to boost their profit and lower their expenses. A decent option for it is machine learning.[8]

Shiyang Xuan:

They compared the results of two random forests. Random forest using a random tree called CART. To train the behaviour aspects of regular and abnormal transactions, they employ various random forest algorithms, each of which has a different performance and base classification. On the dataset from the Chinese e-commerce company, they used both methods. where the subsets' fraud transaction ratios range from 1:1 to 10:1. The accuracy of the random-tree based random forest is therefore 91.96%, whereas the accuracy of the CART based random forest is 96.7%. Numerous issues, such as uneven data, have arisen as a result of the data being from the B2C dataset. Consequently, the algorithm can be enhanced.

Dejan Varmedja: He presented various machine learning algorithms and examined them in relation to techniques for detecting credit card fraud. Logistic Regression, Naive Bayes, Random Forest, and Multilayer Perceptron are some of the different machine learning techniques. Here, a multilayer perceptron (ANN) is employed, an artificial neural network that has four hidden layers and relies on relu activation to prevent negative results. Adam is used as the optimizer for the optimal performance. As a consequence, the accuracy score for the Logistic regression model is 97.46%, and the data set contains 56962 samples, 98 of which are fraud transactions. Naive Bayes and Random Forest both achieved accuracy scores of 99.23% and 99.96% for the same dataset.[8]

Changjun Jiang: He put forth a brand-new approach to detecting fraud that consists of four phases. In the first stage, they use past transaction data to organise transactions into clusters based on behaviour, and then they develop a sliding window mechanism to aggregate transactions.After aggregation, we use the newly generated window to perform feature extraction. This approach is used to characterise a cardholder's behavioural pattern. Finally, classification occurs, classifying behavioural patterns and assignments. As a result, their Logistic Regression with raw data (RawLR), Random Forest with aggregation data (AggRF), and Random Forest and feedback technique with aggregation data (AggRF +FB) methods are the top methods with 80% accuracy in comparison to other methods.

Kuldeep Randhawa: For the purpose of detecting credit card fraud, they deployed 12 machine learning methods, ranging from deep learning to ordinary neural networks.

The effectiveness of benchmark and real-world datasets is being tracked. In order to create the hybrid models, the AdaBoost and majority voting methods are also used. Single and hybrid models are discussed in the associated study. They had provided the results for both parameters (Benchmark and real-world datasets) using their twelve chosen algorithms: Nave Bayes, Random Forest, Decision Tree, Gradient Boosted Tree, Decision Stump, Random Tree, Neural Network, Linear Regression, Deep Learning, Logistic Regression, SVM, Multilayer Perceptron. As a result, the Random Forest algorithm obtained the best accuracy and sensitivity when employed with AdaBoost and majority voting techniques under benchmark data, with 95% and 91%, respectively. Even with 30% noise in the dataset, the accuracy rate is still around 90% when tested with real-world data. Matthews correlation coefficient, or MCC, is a commonly used metric to assess a model's performance. In the instance of majority voting, the best MCC score is 0.823, while the score increases to 0.942 when 30% more noise is given to the dataset.

Sai Kiran: He suggested a more effective algorithm for detecting credit card fraud. The Naive Bayes enhanced K-nearest Neighbour approach (NBKNN) is what it is known as. To find the fraudulent transaction in the stolen dataset, they used a dataset on which they applied algorithms. The dataset contains information about European Cardholders who used their credit cards to make a purchase within 2 days. Of the 284,807 transactions they performed, 492 were fraudulent. Despite working differently on the same dataset, the approaches that were utilised are classification techniques. They had combined the two methods (Naive Bayes and k-nearest neighbour) to increase the algorithm's precision and adaptability.

Zahra Kazemi et al.: In order to retrieve the most valuable information from a credit card transaction, he introduced Deep autoencoder. The class labels difficulties will be resolved by adding additional Softmax software as a result. To map the data into a high dimensional space, an overcomplete autoencoder is utilised, and a sparse model was used in a descriptive way, which has advantages for the classification of a type of fraud. One of the most effective and driven technologies being used to find credit card fraud is deep learning. These networks have a complicated data distribution that is particularly challenging to identify. The best features of the data were extracted at specific points and used for classification by using a deep autoencoder. Additionally, these networks exhibit low variance and improved accuracy.[9]

Sharmistha Dutta et al.: He presented research on the crimes that are frequently discovered when applying for credit cards. When using the current non-data mining methods to prevent identity theft, there are some challenges that arise. The solution to these problems is a fresh data mining layer of defence. Two techniques, known as Communal Detection and Spike Detection, which produce unique layers, are used to find frauds in a variety of applications. The moving window is big, and there are more qualities and connection kinds that CD and SD algorithms can search through. As a result, the system can produce outcomes by spending a considerable amount of time.

Even after a regular update of the algorithms, a true evaluation cannot be obtained since the attackers do not have enough time to alter their behaviour in response to the algorithms being used in real-time. As a result, it is impossible to illustrate adaptation in its right context. These issues can be resolved by making certain enhancements in the proposed algorithm in future work.[9]

III.FUTURE SCOPE:

While we couldnt reach out goal of 100% accuracy in fraud detection, we did end up creating a system that can, with enough time and data, get very close to that goal. As with any such project, there is some room for improvement here.The very nature of this project allows for multiple algorithms to be integrated together as modules and their results can be combined to increase the accuracy of the final result.This model can further be improved with the addition of more algorithms into it. However, the output of these algorithms needs to be in the same format as the others. Once that condition is satisfied, the modules are easy to add as done in the code. This provides a great degree of modularity and versatility to the project.More room for improvement can be found in the dataset. As demonstrated before, the precision of the algorithms increases when the size of dataset is increased. Hence, more data will surely make the model more accurate in detecting frauds and reduce the number of false positives. However, this requires official support from the banks themselves

IV.CONCLUSION:

Credit card fraud is a persistent problem that can lead to significant financial losses for individuals and businesses alike. With the increasing reliance on electronic payments, detecting and preventing fraud has become a crucial task for financial institutions. In recent years, various techniques and algorithms have been developed to improve the accuracy and efficiency of credit card fraud detection. These techniques include rule-based systems, statistical methods, machine learning, and deep learning. Machine learning algorithms have shown promising results in detecting credit card fraud, as they can learn from large datasets and identify patterns that are difficult for human analysts to detect. Deep learning techniques, such as neural networks, have also shown great potential for detecting fraudulent transactions. However, credit card fraudsters continue to develop new and sophisticated methods to evade detection, and fraud detection systems must continue to evolve and adapt to these changing threats. Credit card fraud is the biggest frauds that are being happened right now around the whole ground. This paper has explained how credit card frauds have been happening and we studied these frauds using a dataset that consists of transactions made in the real world. We saw how different machine learning algorithms are used to predict the fraud transactions on our dataset and we also addressed the class imbalance issue of our dataset and used oversampling to finally use Random Forest classifier that got a good accuracy score.

REFERENCES

[1] Xiaohui Yang, "The Prediction of Gold Price Using ARIMA Model", 2nd International Conference on Social Science, Public Health and Education 2019.

[2] Mrs. B. Kishori 1, V. Preethi, "Gold Price forecasting using ARIMA Model", International Journal of Research, 2018.

[3] R. Hafezi*, A. N. Akhavan, "Forecasting Gold Price Changes: Application of an Equipped Artificial Neural Network", AUT Journal of Modeling and Simulation, 2018.

[4] Shian-Chang Huang and Cheng-Feng Wu, Energy Commodity Price Forecasting with Deep Multiple Kernel Learning, MDPI Journal, 2018.

[5] Wedad Ahmed Al-Dhuraibi and Jauhar Ali, "Using Classification Techniques to Predict Gold Price Movement",4th International Conference on Computer and Technology Applications, 2018

[6] NalinipravaTripathy, "Forecasting Gold Price with Auto Regressive Integrated Moving Average Model", International Journal of Economics and Financial Issues, 2017.

[7] Hossein Mombeini and AbdolrezaYazdani-Chamzini, "Modeling Gold Price via Artificial Neural Network", Journal of Economics, Business and Management, 2015.

[8] Credit Card Fraud Detection Using Machine

[8] Sonal Mehndiratta, Mr. Kamal Gupta:International Journal of Computer Science and Mobile Computing, Vol.8 Issue.8, August- 2019

[9] Nayan Uchhana, Ravi Ranjan, Shashank Sharma, Deepak Agrawal, Anurag PundeInternational Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075 (Online), Volume-10 Issue-6, April 2021

[10] Credit Card Fraud Detection Using Machine Learning Algorithms , GIS SCIENCE JOURNAL,(ISSN NO : 1869-9391)

[11]Credit card fraud and detection techniques: a review Delamaire, L, Abdou, HAH and Pointon,