Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7-Issue 1, January 2024
Paper: 76

Detection of Trickery Credit Transaction

Sangeerani Devi A
Computer Science Engineering
Sri Sairam Engineering College
Chennai, India
sangeerani.cse@sairam.edu.in

Aishwaryaa S P
Computer Science Engineering
Sri Sairam Engineering College
Chennai, India
sec19cs128@sairamtap.edu.in

Srija G
Computer Science Engineering
Sri Sairam Engineering College
Chennai, India
sec19cs082@sairamtap.edu.in

Abstract**—** *In this digitally reformed world everything has been changed into digital form. So is transaction of money too, we pay, receive and transfer money online. We are able to collect money from the ATM which is available near us just by inserting the card and entering the unique card number. But as the technology is advancing day by day the fraudulent activities are also in rise. There are a lot of fraud credit card transactions taking place everywhere, in order to find a solution for this problem we are studying the past credit card transactions which are turned out to be fraud. After studying and analyzing the past transactions, the results are used to identify whether a present or future transaction is fraud or not. Therefore by the above process of analyzing the transaction data, which helps us by providing better results for detecting the transactions. Our research focuses on deep learning techniques, such as neural networks with activation functions, sigmoids, and reLU (rectified linear unit), which we employ to determine statistical measurements and model correctness.*

Keywords- Neural networks, Deep learning, sigmoid, reLU, statistical measurements.

I . INTRODUCTION

Credit card fraud is the illegal way of obtaining money using the credit card information of the cardholder without their knowledge. Fraud in credit card transaction is in rise as the technology has advanced and everyone are using their cards for payment in online and offline modes instead of cash. Inner card fraud and exterior card fraud are two types of credit card fraud.

Inner card fraud happens when cardholders and banks agree to conduct fraud by using a fictitious identity, but in case of external credit card fraud cases the credit card used for paying is stolen and is used to obtain money from the stolen card.

Whatever be the mode of payment (online or offline) when we use our credit card to pay or to collect money from ATM etc.., we should be careful while handling the card, entering the card number and receiving the money, because the fraudsters can employ your card without your knowledge, use it for their purposes while you are still unaware of it. Hence the data such as the cardholder's unique credit card number ans his card's expiry date must be very intimate (i.e., it must be kept safe). Sometimes the fraud information may be disclosed due to some reasons or else the card may be lost. In those situations, to determine whether a transaction is fraud or not we must study the behaviour of the customer's spending

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7-Issue 1, January 2024
Paper: 76

considering his past transactions and after that using Deep Learning algorithms we should determine whether the transaction is valid or not.

Types of Frauds:

- Online fraud
- Offline fraud
- Phishing fraud

II . NEURAL NETWORK CONSTRUCTION FOR TRICKERY CREDIT TRANSACTION

The neuron functioning of human brain principle is used to detect trickery credit transaction using neural networks. The use of neural network technology can enable a computer to think efficiently rather than a single model. Due to the neural network's ability to solve classification issues, it is possible to identify credit card fraud with it. The human brain majorly consist of neurons which is responsible for transmission of information from its surroundings. This technology works in a similar way. Customers that pay with a credit card establish a predictable trend. This pattern is then utilized to classify the data. By using the available dataset and training the model yields the required output. This data includes the cardholder's profession, income, credit card number, large-dollar transactions, frequency of transactions, location of purchases, information about the types of purchases made with the credit card previously (e.g. grocery store, gas stations, hotels, specific restaurants, etc..,), and the card's issue date.

The neural network process the given input to determine if the transaction is fraud or not. When a credit card is used, the system compares the transaction information to information saved from prior transactions. If the data follows the pattern, the card is probably certainly used by the owner. Of course, there are many possibilities where a transaction made by the card user differs significantly from previous transactions, as well as instances where the information follows the pattern but the transaction is not performed by the card user. On the other hand, in the worst-case, the transaction will not be completed. Pattern recognition is a difficult task in the credit card fraud detection. It does, however, have certain unique traits that make it challenging. The most concerning problem is the similarity between legitimate and fraudulent operations.

III . EXTRACTION OF DATASET

The dataset was extracted from the reliable online website Kaggle. It comprises credit card transactions details of European cardholders in September 2013. This dataset contains 492 frauds out of 284 807 transactions that occurred during the course of two days. The dataset is highly unbalanced, with the large number of normal transactions data.

IV. CLASS IMBALANCED PROBLEM

A dataset that is unbalanced is one in which the target variable of one class is in huge number compared to other, in which number of records are very less.When Machine Learning algorithms are trained on unbalanced datasets, there is huge possibility of the classifier model to give unexpected results. These trained models overfits the training dataset and miss to give performance in real-time inputs. There is a chance that many conventional classifier algorithms will classify the

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 7-Issue 1, January 2024
Paper: 76

minority class incorrectly.

There's also the issue of vanity metrics when it comes to evaluating algorithm performance on unbalanced datasets. An algorithm may forecast all cases as belonging to the majority class if we have an imbalanced dataset with 1% of a minority class and 99 percent of the majority class. This algorithm's accuracy score will return a score of 99 percent, which appears great, but is it really? In this situation, the minority class is completely neglected, which can be costly in some categorization issues, such as credit card theft, which can cost individuals and businesses a lot of money.

We employ strategies such as over-sampling. From the dataset, we oversample the records. The dataset rows are optimized by applying random oversampling. Supervised approaches rely on a set of previous transactions known as a transaction's label (also known as class). There are two types of labels in credit card fraud detection tasks: legitimate (the transaction was made by the original user.) and fraudulent (the transaction was done by someone else) (the transaction was made by a fraudster). The information used to define the label came from a customer complaint or a credit card company investigation. Supervised approaches employ tagged previous transactions to develop a fraud prediction model that returns the likelihood of a new transaction being a fraud for any new transaction.

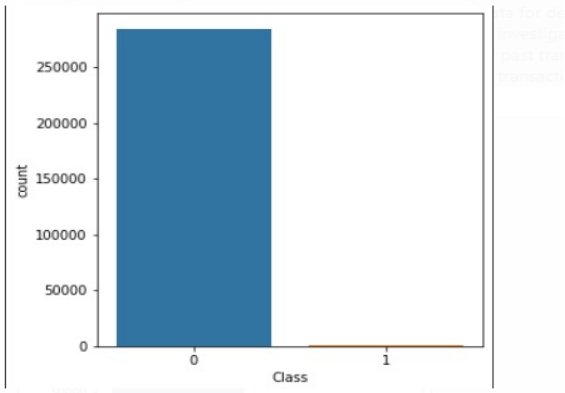


Figure 1. Class frequency distribution

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 7-Issue 1, January 2024
Paper: 76

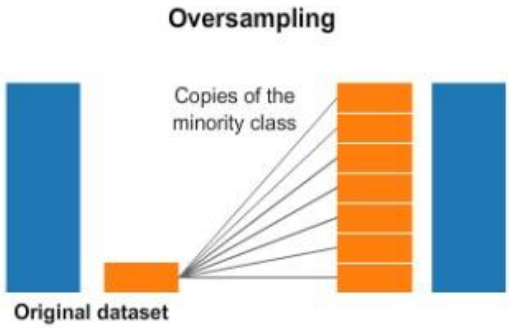
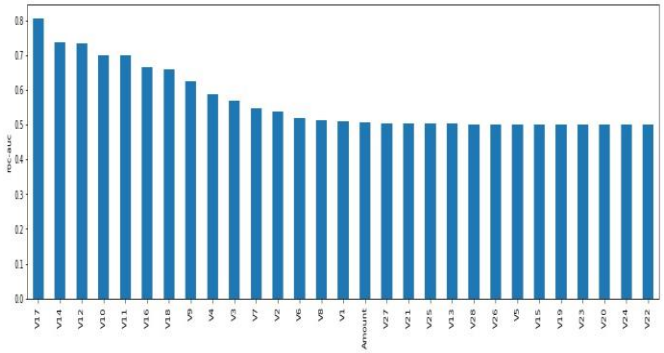


Figure 2. Oversampling of dataset

V . PROPOSED METHODOLOGY

The proposed model predicts the fraudulent transaction based on neural network. Performance effectiveness is evaluated and accuracy is calculated based on classification prediction. The real time dataset of European cardholders recorded for two days where we have normal and fraudulent transaction records. It contains 31 attributes each of which are encrypted with numerical values to ensure confidentiality of their customer's transaction. Numerical values are result of PCA transformation.

The goal is to develop a efficient model so that accuracy to find the fraudulent transaction is maximized. Since a neural network works better than a single machine learning algorithm, our model is designed using Artificial Neural Network with the activation function as Sigmoid and ReLU. The combination of these two functions yielded a better accuracy. After the data preprocessing steps, using the selected model forward propagation, cost function definition, backward propagation and cost optimization steps are carried out.



Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7-Issue 1, January 2024
Paper: 76

Figure 3. ROC-AUC bar graph

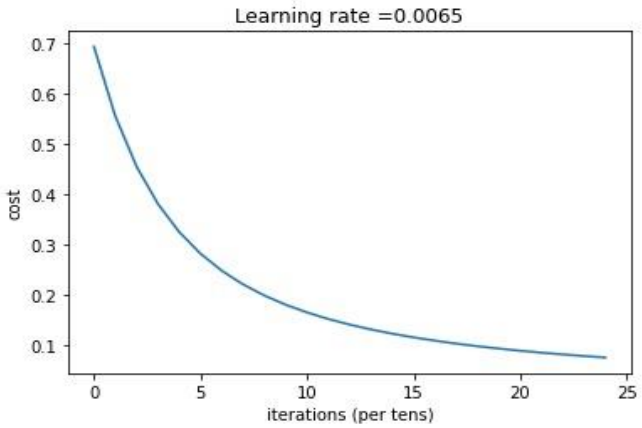


Figure 4. Iterations vs cost

VI . CONCLUSION

The proposed system provides a accuracy of 99.819% which is better than previous model is a result of experimenting different activation function in a neural network to improve accuracy. The recent advancement in technology has allowed many e-commerce platforms to access the bank details, hence the security of the customers are reduced. On using credit card fraud detection model the fraud activities faced by vulnerable group of people is reduced. The key objective to identify and report fraudulent transactions is attained by the proposed model.

VII. REFERENCES

[1] Najadat, H., Altiti, O., Aqouleh, A.A. and Younes, M., 2020, April. Credit card fraud detection based on machine and deep learning. In 2020 11th International Conference on Information and Communication Systems (ICICS) (pp. 204-208). IEEE.

[2] Lucas, Y. and Jurgovsky, J., 2020. Credit card fraud detection using machine learning: A survey. arXiv preprint arXiv:2010.06479.

[3] Zhang, X., Han, Y., Xu, W. and Wang, Q., 2021. HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Information Sciences, 557, pp.302-316.

[4] Chen, J.I.Z. and Lai, K.L., 2021. Deep convolution neural network model for credit-card fraud detection and alert. Journal of Artificial Intelligence, *3*(02), pp.101-112.

[5] Krishna Rao, N.V., Harika Devi, Y., Shalini, N., Harika, A., Divyavani, V. and Mangathayaru, N., 2021. Credit Card Fraud Detection Using Spark and Machine Learning Techniques. In Machine Learning Technologies and Applications (pp. 163-172). Springer, Singapore.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

[6] Nguyen, T.T., Tahir, H., Abdelrazek, M. and Babar, A., 2020. Deep learning methods for credit card fraud detection. arXiv preprint arXiv:2012.03754.

[7] Voican, O., 2021. Credit Card Fraud Detection using DeepLearning Techniques. Informatica Economica, *25*(1).

[8] Habibpour, M., Gharoun, H., Mehdipour, M., Tajally, A., Asgharnezhad, H., Shamsi, A., Khosravi, A., Shafie-Khah, M., Nahavandi, S. and Catalao, J.P., 2021. Uncertainty-Aware Credit Card Fraud Detection Using DeepLearning. arXiv preprint arXiv:2107.13508.

[9] Tanouz, D., Subramanian, R.R., Eswar, D., Reddy, G.P., Kumar, A.R. and Praneeth, C.V., 2021, May. Credit card fraud detection using machine learning.

[10] Forough, J. and Momtazi, S., 2021. Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing, 99, p.106883.

[11] Azhan, M. and Meraj, S., 2020, December. Credit card fraud detection using machine learning and deep learning techniques. In *2020* 3rd International Conference on Intelligent Sustainable Systems (ICISS) (pp. 514-518). IEEE.

[12] Sailusha, R., Gnaneswar, V., Ramesh, R. and Rao, G.R., 2020, May. Credit card fraud detection using machine learning. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1264-1270). IEEE.

[13] Trivedi, N.K., Simaiya, S., Lilhore, U.K. and Sharma, S.K., 2020. An efficient credit card fraud detection model based on machine learning methods. International Journal of Advanced Science and Technology, 29(5), pp.3414-3424.