International Journal on Applications in Information and Communication Engineering
Volume 8 : Issue 2 : June 2022, pp 55 – 58 www.aetsjournal.com ISSN (Online) : 2394 - 6237

CREDIT CARD FRAUD DETECTION USING NEURAL NETWORKS

BALADITHYA P , VINAY KUMAR REDDY , NANDEESWAR P , VIVEKANANDA GN
SHIVA SAI T

Abstract — Credit cards have become the most prevalent method of payment for both online and normal transactions as communication technology and E-Commerce have advanced. As a result, security in this system is intended to be very good in order to avoid fraudulent transactions. Each year, the number of fraudulent credit card data transfers rises. Researchers are also experimenting with unique approaches to identify and prevent such scams in this field. However, certain strategies that may accurately and effectively detect these scams are constantly needed. This research provides a system for identifying credit card fraud using an unsupervised learning technique based on Neural Networks (NN). The suggested method outperforms existing clustering techniques such as Auto Encoder (AE), Local Outlier Factor (LOF), Isolation Forest (IF), and K-Means.The suggested NN-based fraud detection approach has a 99.87 percent accuracy, whereas current methods such as AE, IF, LOF, and K Means have accuracies of 97c/o, 98c/o, 97.92c/o, and 97.69c/o, respectively.

Keywords— Unsupervised Learning, Anomaly Detection, Fraud Detection, Auto-Encoder, Credit Card

I. INTRODUCTION

The unauthorised use of a customer's card details to make transactions or remove funds from the cardholder's record is known as credit card falsification. Extortion begins with a credit card when someone obtains the number displayed on the card or the necessary records for the card to work wrongly. The cardholder, the agent who issued the card, and even the card's guarantor may not be aware of the fraud until the record is used to make purchases. It is no longer necessary to use a physical card to make transactions because internet-based apps and online bill payment have become commonplace.

The most talked-about issue these days is fraud detection in online buying systems. To avoid fraud activities that change fast, fraud investigators, banking systems, and electronic payment platforms such as PayPal must have an efficient and complicated fraud detection system. According to a 2017 Cyber Source analysis, the current fraud loss per order channel was 74 percent in their web shop and 49 percent in their mobile channels. The lesson here is to look for abnormalities in patterns of fraud activity that have evolved over time based on this information.

The rise of the E-commerce industry has led to a gradual increase in the use of credit cards for online transactions and purchases. With the increased use of credit cards, the number of fraud instances has increased by a factor of two. Credit card fraud is when someone uses a credit card to obtain money without the cardholder's knowledge.

II. LITERATURE REVIEW

In [1], According to Altab Althar Taha and Sareef Jameel Malbery, advancements in e-commerce and communication technologies have made credit card usage a more common method of payment, and transaction fraud is also on the rise. They employed the improved light gradient boosting machine, which combines Bayesian based hyper-parameter optimization with light gradient boosting machine parameter tuning (LightGBM). They employed a real-world public dataset that included both fraudulent and non-fraudulent transactions in their technique. Their suggested approach exceeded other strategies in terms of accuracy when compared to other techniques. The suggested system achieves a

Baladithya P, Department of CSE, Madanapalle Institute of Technology & Science, Madanapalle, A.P., INDIA.
Vinay Kumar Reddy , Department of CSE, Madanapalle Institute of Technology & Science, Madanapalle, A.P., INDIA.
Nandeeswar p , Department of CSE, Madanapalle Institute of Technology & Science, Madanapalle, A.P., INDIA.
Vivekananda GN ,Associate Professor , Department of CSE, Madanapalle Institute of Technology & Science, Madanapalle, A.P., INDIA. (Email : drvivekanandagn@mits.ac.in)
Shiva Sai T , Department of CSE, Madanapalle Institute of Technology & Science, Madanapalle, A.P., INDIA.

98.40 percent accuracy, a 92.88 percent area under the receiver operating characteristics curve (AUC), a 97.34 percent precision, and a 56.95 percent F1-score.

In [2], According to studies by S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. Hacid, and H. Zeineddine, credit card theft results in significant financial loss. The majority of researchers have been working on this to come up with new ways to eliminate this loss, and the majority of the present approaches are expensive, time-consuming, and labor-intensive. After conducting several experiments, the authors discovered that the uneven categorization of the dataset is the primary cause of erroneous findings. These imbalance classifications are created by an unbalanced dataset, causing the model to forecast incorrectly and resulting in financial loss. Based on accuracy, AUCPR, and sensitivity, they discovered that LR, C5.0 decision tree method, SVM, and ANN are the top algorithms.In order to train these models, they employed a balanced dataset.

In [3]According to the study of Imane Sadgali, Nawal Sael, and Faouzia Benabbou, financial transactions such as internet transactions, credit card transactions, and smartphone transactions are increasing popularity these days since everyone prefers digital and paperless transactions. Millions of transactions were completed, each of which was subjected to some form of fraud. Many of the researchers have evaluated, constructed, and developed a machine learning model for identifying fraud. They compared the full machine-learning system to determine which model is superior at detecting fraud in card transactions.

In [4], To identify the accuracy in fraud identification, Debachudamani Prusti and Santhnu Kumar Rath created an application using machine learning algorithms such as Decision tree (DT), k-nearest algorithm (kNN), Extreme learning machine (ELM), Multilayer perceptron (MLP), and support vector machine (SVM). They suggested a model that used the approaches of DT, SVM, and kNN. For effective data sharing across numerous diverse platforms, they employed two web-based protocols: simple object access protocol (SOAP) and representational state transfer (REST). They compared the outcomes of five machine learning algorithms using the accuracy metric. Although SVM outperformed other algorithms by 81.63 percent, the hybrid system they presented had a higher accuracy of 82.58 percent.

In [5], M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika, and E. Aswini collaborated on a project that used Random forest techniques to create a model for detecting fraud in credit card transactions. The random forest algorithm (RFA) is a supervised machine learning approach that classifies credit card transactions using a decision tree and then calculates performance using a confusion matrix. The suggested system has a 90% accuracy rate.

In [6], To cope with the unevenness dataset and avoid the noisiness inherent in the transactions, Akila and Srinivasulu reddy suggested a misrepresentation localization framework using non-overlapped risk based bagging ensemble (NRBE) model. The bagging model eliminates any irregularities in the dataset as well as non-essential data. The sacking model is reached out to by a pack of creators and a pupil who is based on risk. Bag creation eliminates the issue of unbalanced data, while Nave Bayes eliminates the issue of transaction noise. Using the NBRE, the suggested model was beaten by 5% in BCR and BER, half of recall, and a 2x or 2.5x reduction in fraud detection costs. The NRBE model was shown to be the best for fraud detection and the most fit for business dynamic techniques.

In [7], According to Phuong Hanh Tran, Kim Phuc Tran, Truong Thu Huong, Cédric Heuchenne, Phuong HienTran, and Thi Minh Huong Le's research, credit card theft has progressively grown in recent years.

Many solutions employ machine-learning algorithms to detect and stop fraudulent transactions. They developed two novel data-driven methodologies that employ the best anomalous strategy for credit card fraud transactions. Kernel parameter selection and T2 control char are the two methods.

In [8]C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan presented a multi-stage procedure. They begin by collecting cardholder transactions, then

aggregate those transactions based on behavioural patterns, classify the dataset, train the model, and test it. If any aberrant behaviour occurs, a feedback mechanism is used to inform the system of the abnormal behaviour.

In [9] As the ratio of fraud to regular transactions is relatively adequate, Ishan Sohony, Rameshwar Pratap, and Ullas Nambiar presented an ensemble learning technique for credit card fraud detection. They discovered that random forest and neural networks are most suited for detecting fraud incidents and providing higher accuracy. They also tested with large-scale credit card transactions in the real world. Random forest and neural networks are used in ensemble learning.

III. PROPOSED SYSTEM

We propose this method to examine the subject of whether or not it is worthwhile to utilise machine learning approaches to detect whether or not a credit card is fraudulent using Neural Networks.

- Through this method we can able to find the count the count of genuine and fraud transactions and it also used for predicting the fraud transaction with high accuracy.
- By this method the performance of the system increases and we can train the model with multiple datasets to produce better results.

1) IMPLEMENTATION OF PROPOSED SYSTEM

We have successfully constructed supervised ML models to detect whether a credit card is fraudulent or not fraudulent in this application. With a 99 percent accuracy score, as well as precision and recall scores of 99 percent, we found that Networks performs well.

In this phase, the project's feasibility is assessed, and a business proposal is presented, along with a very generic project design and some cost estimates. A feasibility assessment of the proposed system is to be carried out during system analysis. This is to guarantee that the planned system will not cause the organisation any problems. Understanding the system's primary needs is necessary for feasibility study.

In fig 1 the process of detecting the fraud transactions in

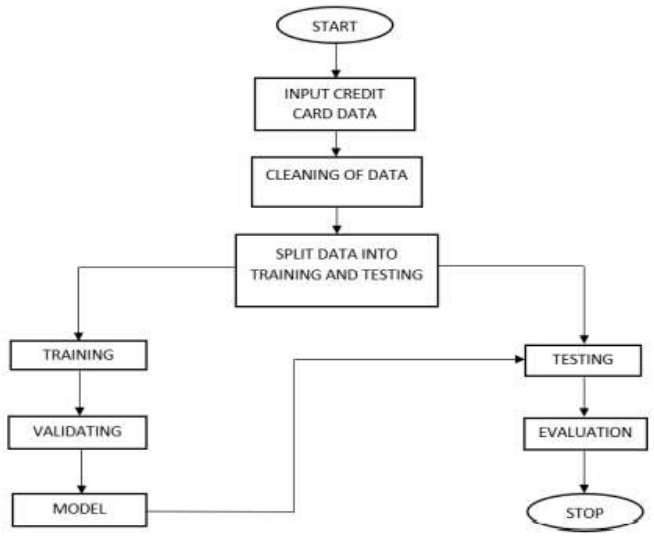

Figure 1 : flow diagram of credit card data

MODULES :

INPUT CREDIT CARD DATA : Collection of credit card transactions in a form of dataset.

CLEANING OF DATA : Check the whole dataset and should make any corrections needed.

SPLIT DATA INTO TRAINING AND TESTING : Check the dataset and should divide it into two as training dataset and testing dataset.

TRAINING : The separated training dataset will trained to execute the model .

VALIDATING : The separated dataset will be validated to create a model for testing.

MODEL : After the validating was done the perfect model dataset for testing will get ready to continue the process of testing.

TESTING : The model dataset will be tested as per the input to get output as how many genuine and fraud transactions has done as per dataset record.

EVALUATION : The output of the tested dataset will be considered and the evaluation will be done to know the output was perfect or not

STOP : If the output was perfect then the process was done successfully.

IV. RESULTS AND ANALYSIS

The analysis of model accuracy and model loss with the iterations (per tens) and cost as shown in below figures

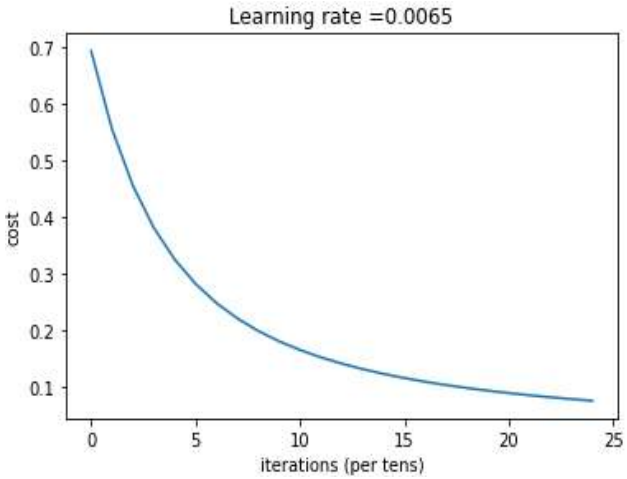

Figure 2: cost per iterations (per tens)

The above line graph explains about the credit card transactions in form of cost vs iterations.

The costs will be differentiated in 0.1units and the iterations will be differentiated in 5 units.

The count of transactions will be displayed as how many genuine and fraud transactions has done in hole dataset .

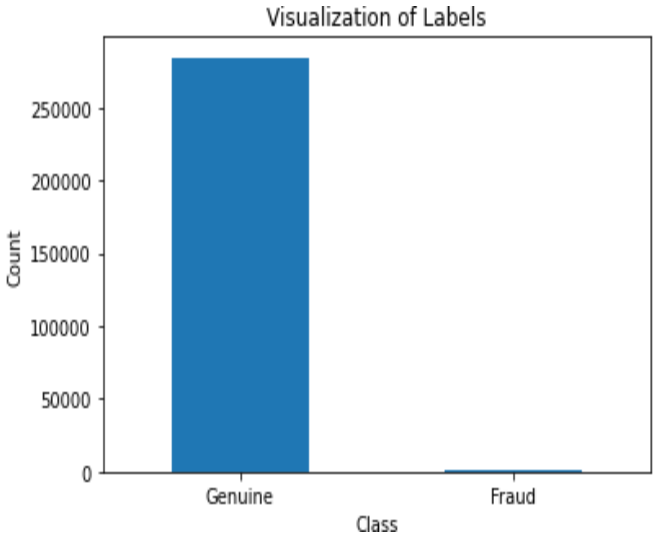

Figure 3 : visualization of labels

The above bar graph will explain about how many genuine and fraudulent transactions has occurred in whole transactions .The transactions count will be differentiated by every 50000 units and it will be differentiated in to two class as genuine and fraud.

V. CONCLUSION

Credit card fraud detection and classification could be a little tedious process because it is very hard to recognize characteristics of transactions. The characteristics could vary between genuine and fraud transaction. These kinds of problems can be handled by feature vector. Before extracting feature, pre-processing is done on every transaction. ANN model is constructed for CSV file which was created along with the transaction details. Finally, the count of the genuine transactions and the fraud transactions is evaluated with accuracy. The above said method was classifying credit card fraud detection. The proposed model has gone through preprocessing stage, feature generation stage and classifiers learning stage. The statically evaluation of the above proposed model is done in terms of precision, recall and accuracy.

REFERENCES

[1] A. A. Taha and S. J. Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine," in IEEE Access, vol. 8, pp. 25579-25587, 2020.

[2] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M. Hacid and H. Zeineddine, "An Experimental Study With Imbalanced Classification Approaches for Credit Card Fraud Detection," in IEEE Access, vol.7, pp. 93010-93022, 2019.

[3] Imane Sadgali, Nawal Sael, and Faouzia Benabbou. Fraud detection in credit card transaction using neural networks. In Proceedings of the 4th International Conference on Smart City Applications (SCA '19). Association for Computing Machinery, New York, NY, USA, Article 95, 2019.

[4] D. Prusti and S. K. Rath, "Web service based credit card fraud detection by applying machine learning techniques," TENCON IEEE Region 10 Conference (TENCON), Kochi, India, pp. 492-497,2019.

[5] M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika and E. Aswini, "Credit Card Fraud Detection Using Random Forest Algorithm,"3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2019.

[6] C. Jiang, J. Song, G. Liu, L. Zheng and W. Luan, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," in IEEE Internet of Things Journal, vol. 5, no. 5, pp. 3637-3647, Oct. 2018.

[7] Ishan Sohony, Rameshwar Pratap, and Ullas Nambiar. Ensemble learning for credit card fraud detection. In Proceedings of the ACM India Joint International Conference on Data Science and Management of Data Association for Computing Machinery, New York, NY, USA, 289–294,2018.

[8] Phuong Hanh Tran, Kim Phuc Tran, Truong Thu Huong, Cédric Heuchenne, Phuong HienTran, and Thi Minh Huong Le. Real Time Data-Driven Approaches for Credit Card Fraud Detection. In Proceedings of the International Conference on E-Business and Application. Association for Computing Machinery, New York, NY, USA,2018.

[9] M. Zamini and G. Montazer, "Credit Card Fraud Detection using autoencoders based clustering," 9th International Symposium on Telecommunications (IST), Tehran, Iran, pp. 486-491,2018.

[10] S. Akila and U. S. Reddy, "Credit Card Fraud Detection Using Non-Overlapped Risk Based Bagging Ensemble (NRBE),"IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, pp. 1-4, 2017.