International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-5, June 2020

Credit Card Fraud Detection using Deep Learning based on Neural Network and Auto-encoder

Priyanka Sharma, Santoshi Pote

Abstract*: Credit card fraud is an event problem and fraud detecting techniques getting more sophisticated each day. Mainly internet is becoming more common in almost every domain. Online transactions, shopping, and e-commerce are expanding step by step. Due to which in the online payment system, fraudulent activities have also increased. It has cost banks and their customers a loss of billions of rupees. The techniques used now a day detects the anomaly only after the fraud transaction takes place. The intruders have found ways to crack the system loopholes and defeat the security. These frauds are not consistent in their actions, they constantly alter. Thus, Artificial Intelligent (AI) algorithms are used to detect the behavior of such activity by learning the past behavior of the transaction of the users. An unsupervised algorithm is used to detect online transactions, as fraudsters commit fraud once by online media and then move on to other techniques. This paper discusses the performance analysis and the comparative study of the two Deep Learning algorithms which include auto-encoder and the neural network. In this paper accuracy, precision, recall, and AUC curve are considered as a model evaluation factor.

***Keywords*: Credit card, fraud detection, Artificial Intelligent (AI), Unsupervised Learning, Deep Learning, Neural Network, auto-encoder.**

I. INTRODUCTION

Nowadays, numbers of people prefer to buy services and goods with credit cards [1]. Both online shopping and online payment of bills and taxes are very useful with credit cards. It's not just convenient, but also time-saving. Many find payment by credit card much more convenient in shops than cash. As a consequence of which there has been a dramatic increase in the number of bank transactions through credit cards and the amount of fraud and card fraud. In the era of digitalization, the need to identify credit card frauds is mandatory. Based on historical information, credit card screening aims to decide whether a transaction is fraudulent or not. The decision is not easy because, when there is any kind of emergency happens, we can see changes in customer expenditure. Fraudsters utilize various methods to conquer extortion assurance.

Machine learning has achieved significant results in several areas of data processing and classification over the last decades. There are two main types of tasks in the field of machine learning: supervised and unsupervised. Supervised learning uses defined data sets to train and make correct learning by adjusting the learning rate parameters. The main drawback of supervised learning is that if new misrepresentation transactions happen that don't match with the records of the database, then these transactions will be seen as genuine. Although, unsupervised learning acquires new transaction knowledge and discovers anomalous trends from new transactions. This unsupervised learning is tougher than supervised learning, as we need effective methods for identifying irregular behaviors.

Now, let us focus on deep learning, which is a part of machine learning (ML). As online transactions are exponentially growing, the amount of data simultaneously increases, leading to unbalances data sets. This increase in data generation is one explanation for the fact that in recent years, deep learning has evolved since deep-learning algorithms need a lot of data to understand. Deep learning makes it possible for a machine to tackle complex issues even with an extremely differing, unstructured, and interconnected informational collection. Besides, various deep learning algorithms are used for detection of fraud, but in this paper, Neural Network and Auto-encoder is used to detect whether the usual data set transaction is eligible as new fraud. We assume that certain regular transactions in data sets classified as fraud also have suspicious transaction behavior.

The remaining paper as per the following, section 2 explains all the current system use in fraud detection. Followed by section 3 portrayed the proposed technique, section 4 shows the performance analysis and results and last section 5 shows the conclusion.

II. RELATED WORK

Yusuf Sahin and Ekrem Duman [2] demonstrate the benefits of using credit card fraud detection techniques, like ANN and LR, to reduce the bank's risk. The results show that the proposed ANN classifiers surpass LR graders to solve the investigated problem.

Revised Manuscript Received on June 25, 2020.
* Correspondence Author
Prityanka Sharma*, Department of Electronic and Communication, Usha Mittal Institute of Technology, SNDT University, Mumbai, India. E-mail: sharmasc06@gmail.com
Santoshi Pote, Department of Electronic and Communication, Usha Mittal Institute of Technology, SNDT University, Mumbai, India. E-mail: santoshipote@yahoo.co.in.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

However, with the distribution of the information sets being more partial, the efficiency of the models in fraudulent transactions decreases.

According to [3], they have proposed the utilization of HMM in credit card extortion discovery.

It has likewise been clarified how the HMM can identify whether an approaching exchange is fake or not. Trial results show the presentation and adequacy of the framework and show the convenience of learning the spending profile of the cardholders. Relative examinations uncover that the Accuracy of the framework is near 80% over a wide variety in the information. The framework is moreover adaptable for taking care of huge volumes of exchanges.

M.Suresh Kumar, V.Soundarya and others [4] proposed the Random Forest Algorithm (RFA) for finding the false transactions and the precision of those transactions. This algorithm relies upon a supervised learning algorithm where it uses decision trees for classification of the dataset. After the classification of the dataset, a confusion matrix is acquired. The presentation of the Random Forest Algorithm is assessed depending on the confusion matrix. The outcome got from handling the dataset gives a precision of around 90-95%.

Ayahiko Niimi [5], led tests that affirm that deep learning has a similar precision as the Gaussian kernel SVM. Likewise, the 10-fold cross-validation analysis demonstrates that it is deep learning offers higher exactness. In this experiment, they had utilized the H2O library for deep learning, with the deep learning modules are written in Java were actuated each time. Thusly, they can't evaluate the execution time. Deep learning parameter alteration is troublesome. By upgrading the parameters, it is conceivable to build the learning exactness.

Pooja Chougule, A.D. Thakare and others [6] work mirror an endeavor to distinguish false card transactions by utilizing k-means alongside a genetic algorithm. Genetic Algorithm is an incredible optimization method. The k-means algorithm bunches the MasterCard transaction dependent on autonomous quality qualities. Be that as it may, with the expansion in the information size, it brings about anomalies. Consequently, to give enhanced recognition of cheats, they had utilized a hereditary calculation. The huge outcomes by the proposed model are seen over straightforward K-means and Simple Genetic Algorithm.

III. PROPOSED TECHNIQUE

This paper uses the methods suggested to identify credit card fraud. Comparisons are made with various deep learning, including auto-encoders or neural networks, which algorithm is better suited to classify fraud transactions by credit card dealers.

A. Deep Learning

In today's world, deep learning is modern technology. The principle of deep learning is an ANN with many layers that are known as hidden layers. Now, AI, Machine Learning, and Deep Learning (DL) are well known. Those three terms would be equivalent if metaphorically equated with the human body: artificial intelligence is like the body that includes the characteristics of comprehension, reasoning, communication, emotion, and sentiment.ML resembles one system that demonstrations in the body, particularly the visual system. Lastly, deep learning is practically identical to the visual signalling component. It comprises of various cells, for example, retina that goes about as a receptor and makes an interpretation of light signals into nerve signals. Presently, we will contrast all the three classes and the human body. Currently, each of the three kinds is to be applied to the human body.

Deep learning is a typical term for a neural network with numerous layers. Deep learning allows for the implementation of other algorithms, such as AE, deep convolutional network, neural network, SVM, and many more. Unsupervised learning immediately extracts the relevant features of your data, makes unlabeled data more available, and offers daily training for data-dependent training.

B. Auto-Encoder

In this examination, we use AE for credit card fraud detection. Auto-encoder is designed to remake high-dimensional information utilizing a neural system model with a narrow bottleneck layer at the center. AE has the input equivalent to the output in the output layer that has pretty much the sort of input units.

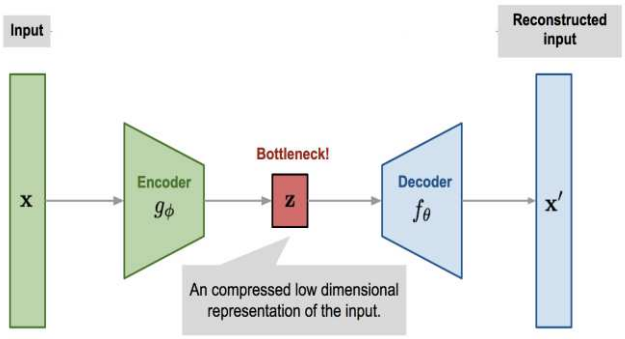

Figure 1: Auto-Encoder [7]

In this experiment to execute AE, we utilize the hyperbolic tangent function or "tanh" function to encode and decode the contribution to the yield. Fig.1. shows the structure of auto-encoder which comprise of input, encoder, bottleneck, decoder, and reconstructed input layers. Encoder figures out how to decrease the input dimension and compress the input data into an encoded portrayal. Bottleneck contains the compress representation of input data. This is the least conceivable dimension of input data. Then again, the decoder figures out how to recreate the information from the encoded representation to be as near as could be expected under the circumstances. Ultimately reconstructed input gauges how well the decoder is performing and how close the output is to the original input. However, the main drawback of auto-encoder is that, while compressing the information they may miss significant parameters that prompt a decline in the accuracy of the model.

C. Neural Network

Another algorithm is the neural network. Neural networks are a set of algorithms; demonstrate after the human brain, which is intended to perceive designs. The systems are worked from singular parts of approximating

© Copyright: All rights reserved.

neurons, normally called units or just "neurons." Each unit has some number of weighted sources of input. These weighted information sources are added together at that point went through an activation function to get the unit's output.

There are fundamentally three sorts of nodes in the neural network:

- Input unit: Input unit provide network information from outside world. These nodes do not compute they simply pass the information on to hidden node.
- Hidden unit: It calculates and transfers the information from input node to output node. A hidden node forms a set of "Hidden Layer". Although there may be one input layer and only one output layer in a feed-forward, it may have no or several Hidden Layers.
- Output unit: The output node is known as "Output Layer". Output unit calculates and transmit the data from the system to the outside world.

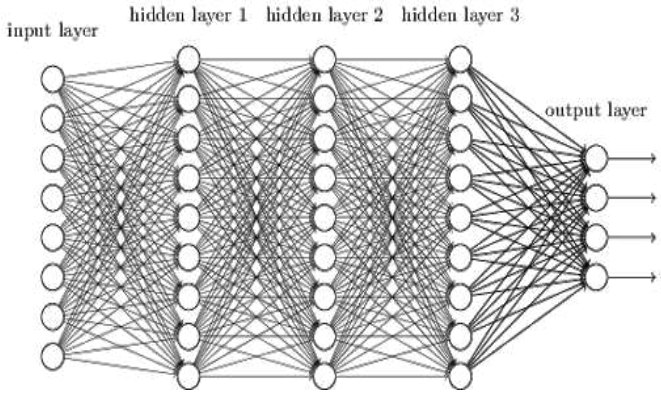

Figure 2: Neural Network [8]

PyTorch [9] is a Python AI package dependent on Torch, which is an open-source machine learning package. PyTorch utilizes the style and intensity of python which is straightforward and useful. Its core gives two essential parts, for instance, an n-dimensional Tensor, like NumPy, yet can run on GPUs and customized partition for building and planning neural systems.

In this experiment, NN consisted of 4 hidden layers, and each layer is backed with a non-linear activation function – The Rectified Linear Unit (ReLU). The input features of each hidden layer are set to 30, 50, 32, and 16 respectively. After this experiment, we started slowly by increasing a smaller number of layers to obtain appropriate results. Therefore, based on extensive analysis, the best hyper-parameters were chosen. Adaptive Moment Estimation (Adam) is a stochastic gradient descent (SGD) and RMSprop-based optimizer, accomplished weight optimization.

D. Dataset

The European dataset of 284, 807 transactions will be utilized for two days in 2013 this incorporates 492 misrepresentation transactions which are named 1 and others are marked as 0 the extent of fraud to no fraud transactions is 0.17%, which indicates that the dataset is extremely imbalanced. Due to customer privacy, the original features of this dataset are not presented and it includes 28 features resulting from the PCA mapping function plus two unmapped features called time and transaction number.

IV. PERFORMANCE METRICS AND EXPERIMENTAL RESULTS

The result of auto-encoder algorithms appeared in fig 3 and 4. The dataset was isolated for training and testing in a proportion of 80:20. The basic performance measures derived from the AUC and confusion matrix. The confusion matrix is a 2 by 2 matrix table contains four results delivered by the paired classifier. The area under an ROC curve is a measure of the usefulness of a test in general, where a greater area means a more useful test, the areas under ROC curves are used to compare the usefulness of tests.

Different estimates, for example, accuracy, precision, recall and F1 score are gotten from the confusion matrix.

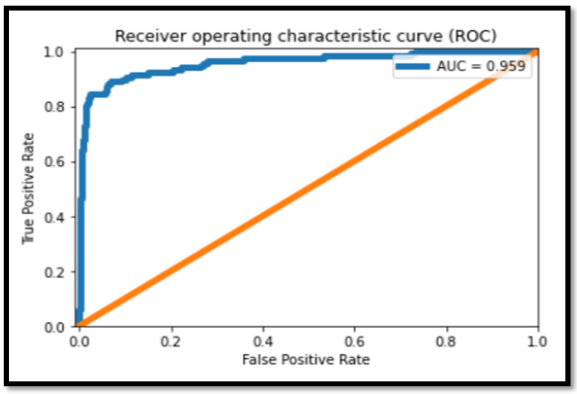

Figure 3: AUC of Auto-encoder

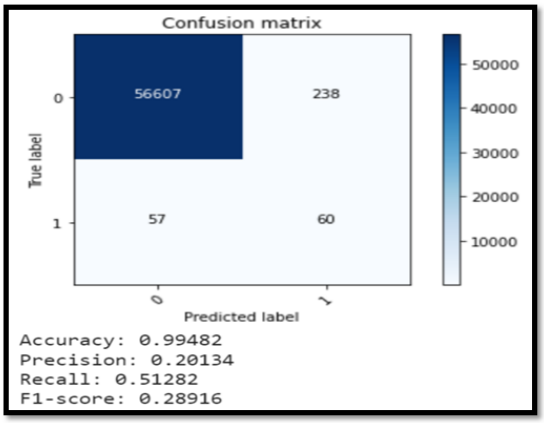

Figure 4: Confusion Matrix of Auto-encoder

Here, we move on to another deep learning algorithm which is a neural network. The results are shown in Fig. 5 and Fig.6.

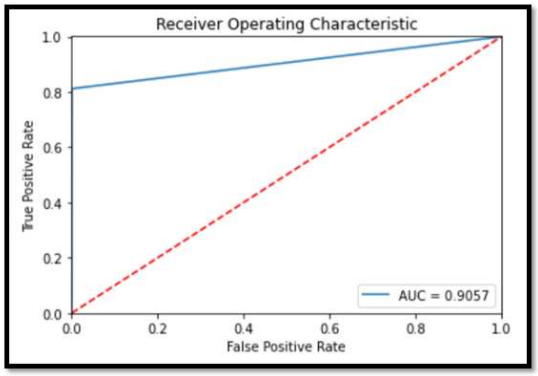

Figure 5: AUC of Neural Network

© Copyright: All rights reserved.

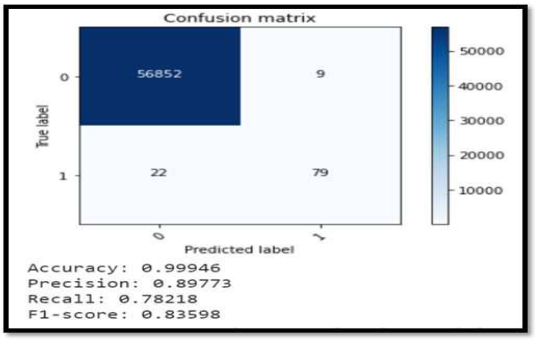

Figure 6: Confusion Matrix of Neural Network

Accuracy, precision, recall, and F1-score are utilized to report the presence of the framework to identify the fraud in the credit card. In this paper, two deep learning algorithms are utilized to identify fraud in the credit card system. To evaluate the algorithms, 80% of the data set is utilized for training and 20% is utilized for testing and validation.

Accuracy, precision, recall, F1-score are used to evaluate for different variables for three algorithms as shown in Table I. The accuracy result appears for Auto-encoder and Neural Network is 99.48%, and 99.94% respectively. In such a case where data is critical, the system cannot rely only on accuracy. The system has to be more precise than being accurate. It should recognize less number of false-negative and false-positive cases.

Table- I: Performance analysis of auto-encoder and Neural Network algorithms

Algorithms	Accuracy	Precision	Recall	F1-score
Auto-encoder	99.48%	20.13%	51.28%	28.91%
Neural Network	99.94%	89.77%	78.21%	83.59%

V. CONCLUSION

To make the final comparison of the above algorithms concerning their classification accuracy, the best results have been taking from Table 1.

As shown in the confusion matrix above, a fine-tuned Neural Network-based system has detected fewer false positives compared to Auto-encoders hence giving the highest precision. So in such a case while dealing with sensitive data, it becomes important to consider the precision of the system than accuracy. Adding more layers will make Auto-encoders more complex to train to result in delayed output. The comparative results show that the neural network performs better than auto-encoder algorithms.

In the future, one can further fine-tuning hyperparameters the neural network, perform boosting techniques on different Machine Learning algorithms. One can also compare the results of different deep learning libraries like fast.ai.conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

REFERENCES

1. F. Carcillo, Y. A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, "Combining unsupervised and supervised learning in credit card fraud detection," Inf. Sci. (Ny)., no. xxxx, 2019, doi: 10.1016/j.ins.2019.05.042.
2. Y. Sahin and E. Duman, "Detecting credit card fraud by ANN and logistic regression," INISTA 2011 - 2011 Int. Symp. Innov. Intell. Syst. Appl., no. June 2011, pp. 315–319, 2011, doi: 10.1109/INISTA.2011.5946108.
3. A. Srivastava, A. Kundu, S. Sural, and A. K. Majumdar, "Credit card fraud detection using Hidden Markov Model," IEEE Trans. Dependable Secur. Comput., vol. 5, no. 1, pp. 37–48, 2008, doi: 10.1109/TDSC.2007.70228.
4. M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika, and E. Aswini, "Credit Card Fraud Detection Using Random Forest Algorithm," 2019 Proc. 3rd Int. Conf. Comput. Commun. Technol. ICCCT 2019, pp. 149–153, 2019, doi: 10.1109/ICCCT2.2019.8824930.
5. A. Niimi, "Deep learning for credit card data analysis," 2015 World Congr. Internet Secur. WorldCIS 2015, pp. 73–77, 2015, doi: 10.1109/WorldCIS.2015.7359417.
6. P. Chougule, A. D. Thakare, P. Kale, M. Gole, P. Nanekar, and A. K. Algorithm, "Genetic Kmeans Algorithm for Credit Card Fraud Detection," Int. J. Comput. Sci. Inf. Technol., vol. 6, no. 2, pp. 1724–1727, 2015.
7. Available:https://lilianweng.github.io/lil-log/2018/08/12/from-autoencoder-to-beta-vae.html
8. Available: http://neuralnetworksanddeeplearning.com/chap5.html.
9. Available: https://pytorch.org/.

AUTHORS PROFILE

Priyanka Sharma, M.Tech. Scholar (Electronic and Communication Engineering) from Usha Mittal Institute of Technology (Mumbai), Maharashtra. I completed my B Tech in Electronic Engineering in 2018 from Usha Mittal Institute of Technology.

Santoshi Pote, pursuing Ph.D. (Electronics Engineering) from Ramrao Adik Institute of Technology (Navi Mumbai). Working as Associate Professor in Electronic and Communication Engineering department in Usha Mittal Institute of Technology (Mumbai).

© Copyright: All rights reserved.