Original Research Paper

Volume -10 | Issue - 3 | March - 2020 | PRINT ISSN No. 2249 - 555X | DOI : 10.36106/ijar

Computer Science

ANALYSIS FOR CREDIT CARD FRAUD DETECTION THROUGH DEEP LEARNING

Jasmin B. Parmar Assistant Professor, Sarvodaya College of Computer Science, Rajkot

Dr.Achyut C.Patel* Professor, SMT. M.T. Dhamsania College of Commerce, Rajkot *Corresponding Author

ABSTRACT In the Current Scenario of World, digitalization looks expanding ubiquity as a result of consistent, helpful and advantageous utilization of ecommerce. It has demonstrated to be a slam gasp and simple method of installment passage. Purchasers pick online installment and e-shopping; due to time comfort. Because of this, an enormous measure of online business use, there is an immense addition in credit card frauds moreover. Fraudsters attempt to abuse the card and straightforwardness of online installments. To beat the fraudster's action become fundamental, the primary point is to verify credit card transactions; in this way, individuals can utilize e-exchanges securely and effectively. To identify the charge card misrepresentation there are different methods which depend on Deep learning, Logistic Regression, Naïve Bayesian, Support Vector Machine (SVM), Neural Network, Artificial Immune System, Nearest Neighbor, Data Mining, Decision Tree, Fuzzy Logic based System, Genetic Algorithm and so on.

KEYWORDS : Fraud, Credit Card, Deep Learning

INTRODUCTION

Ongoing investigations show that the number of bank exchanges by means of charge cards raised radically and with it the number of cheats and card burglary. The charge card is mainstream and assumes a significant job in ecommerce and online cash exchange which is developing. Because of the developing use of charge card, fraudsters attempt to discover more chances to submit cheats that can make colossal misfortunes cardholders and banks. Credit card fraud takes many forms, namely [5]

1. Offline credit card fraud: Happens when the plastic card is stolen by fraudsters, using it in stores as the actual owner.
2. Online credit card fraud: A popular and very dangerous fraud, credit cards' information is stolen by fraudsters to be used later in online transactions by Internet or phone.

Fraud means obtaining services/goods and/or money by unethical mean and is a growing problem all over the world nowadays. Fraud deals with cases involving criminal purposes that, mostly, are difficult to identify. Credit card fraud detection is one of the most explored domains of fraud detection. Numerous authorization techniques are used to prevent credit card frauds, such as signatures, credit card number, identification number, cardholder's address, expiry date, etc. However, these techniques are not enough to hinder credit card fraud. Therefore, there is a need to use fraud detection approaches which analyze data that can detect and eliminate credit card fraud.

Today, with the development of web-based business, it is on the web that half of all credit card fraud is led. Deceitful exercises can't be adequately identified with basic example coordinating calculations. Productive fraud discovery is expected to assert the exactness and small size bogus identification.

Since Credit Card Fraud has enormously expanded, it is essential to comprehend the strategy for recognizing and finding credit card fraud. In actuality, the information or tasks with inconsistencies are insufficient to effectively distinguish frauds. The main practical arrangement is robotization by PC. The PCs can be utilized to evaluate credit card exchanges as 'suspicious" and this can be performed by basic factual techniques. Along these lines, customary strategies don't do the trick and more current methods like Machine Learning & AI are required.

Another attribute of this space is that the dataset is lopsided, that is, the "not fraud" class is substantially more successful than the "fraud" class. Significant contemplations incorporate how quick the cheats can be distinguished, what number of styles/kinds of frauds are identified, regardless of whether the location was in on the web/constant (occasion driven) or group mode (time-driven).

In the present fraud discovery frameworks, the "suspicious" exchange is stamped and afterwards physically examined by human administrators for the last decision to disambiguate questionable cases. There are specific challenges with credit card fraud detection because it is challenging. However, there are several constraints associated with the problem. In what follows, we mention a few important points [2]:

- Unavailability of Datasets
- Dynamic Fraudulent Behavior
- Highly Skewed Dataset:
- Right Evaluation Parameters

TYPES OF FRAUD

- **Bankruptcy Fraud**

Bankruptcy fraud educates the utilization with respect to a credit report from acknowledging agency as a wellspring of data seeing the candidates' open records just as a potential implementation of a Bankruptcy Model. It is the most troublesome kinds of fraud for anticipating Liquidation misrepresentation implies utilizing a Credit Card while being indebted.

- **Theft Fraud/Counterfeit Fraud**

Theft Fraud implies utilizing a card that isn't yours. The culprit will take the card of another person and use it however many occasions as would be prudent before the card is blocked. The sooner the proprietor will respond and contact the bank, the quicker the bank will take measures to stop the criminal. At a certain point, one will duplicate your card number and codes and use it through specific sites, where no signature or physical cards are required.

- **Application Fraud**

In many banks, to be qualified for a credit card, candidates need to finish an application structure. Every one of those qualities might be utilized while scanning for copies. Instead of utilizing factual procedures, another method simple to actualize is cross-coordinating. Conversely, personality wrongdoing, as it is named, is executed by genuine crooks filling application information incorrectly intentionally.

- **Behavioral Fraud**

It happens when subtleties of genuine cards have been gotten deceitfully and deals are made on a 'cardholder present' premise. These businesses incorporate phone deals and internet business exchanges, where just the card subtleties are required.

Theoretical Background Of Deep Learning

Deep learning is an amazing asset to make forecast a significant outcome. It is computer programming that imitates the system of neurons in a mind. It is a subset of AI and utilizes deep neural systems. A deep neural system gives best in class precision in numerous assignments, from object discovery to discourse acknowledgement. They can adapt naturally, without predefined information expressly coded by the developers.

The Process of Deep Learning like:
Understand Problem > Identify Data > Select Algorithm > Trail the Model > Test Model

There are two types of classification under Deep Neural Network namely; Shallow Neural Network which has only one hidden layer between the input and output. Another is Deep Neural Network which has more than one layer.:

EXISTING TECHNIQUES

Artificial Neural Network

Artificial Neural Networks (ANNs) are multi-layer completely associated neural nets that resemble the figure beneath. They comprise of an input layer, multiple hidden layers, and an output layer. Each node in one layer is associated with each other node in the following layer. We make the system more profound by expanding the quantity of hidden layers.

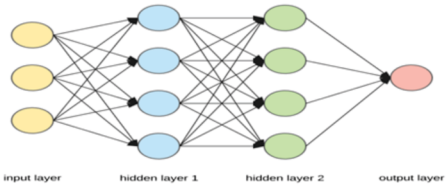

Figure 1: Basic Flow of ANN with 2 hidden layer

The building block of a neural network is the neurons. An artificial neuron works much the same way the biological one does. Artificial Neural Networks (ANNs) are computing systems that is designed a similar way to human brain analysis and process the information. Single artificial neurons called a perceptron.

Deep Learning Auto Encoder

Auto-Encoder neural system is unsupervised learning calculation that applies back-engendering, settings the objective qualities to be equivalent to the sources of info, for example, it utilizes Y(I) = X(i). Stacking layers of Auto encoders produce more Deep engineering known as stacked or Deep Auto encoders. Auto-Encoders are neural systems with equivalent info and out-put. It is made out of two sections:

1. *Encoding Network:* This part of the network compresses the input into a latent space representation. The responsibility of the Encoder layer is to take input and reduce in some form.
2. *Decoding Network:* This layer decodes the encoded input back to the original dimension. The decoded output is some form of original input and it is reconstructed from the latent space representation.

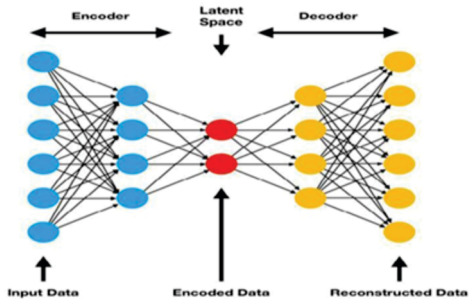

Figure 2: Basic Flow of Deep Auto encoder

Feed Forward Neural Network

Neural system rose up out of an extremely well-known AI calculation named perceptron. Deep feed forward systems, likewise regularly called feed forward neural net-works, or multilayer perceptrons (MLPs), are the quintessential Deep learning models. Joining numerous layers of perceptrons is known as multilayer perceptrons or feed-forward neural systems.

With this sort of engineering, data streams in just a single course, forward. That is to say, the data's streams start at the information layer, goes to the "covered up" layers, and end at the yield layer. The system doesn't have a circle. Data stops at the yield layers.

There are two different classes of network architectures:

Single-layer Feed-Forward (neurons are sorted out): Neurons with this sort of activation work are additionally called fake neurons or straight edge units. It very well may be prepared by a straightforward learning calculation that is generally called the Delta rule.

Multi-layer Feed-Forward (in non-cyclic layers): the units of these systems apply for a sigmoid work as an actuation work. It very well may be prepared by a learning calculation that is normally called Backpropagation.

Convolutional Neural Network

In case of Convolutional Neural Network (CNN or ConvNet) the neuron in a layer will only be connected to a small region of the layer before it, instead of all of the neurons in a fully connected manner. It is a special type of feed forward artificial neural network which is inspired by visual cortex. CNN has following layers:

Convolution layer: To move the feature/filter to every possible position on the image.

Step-1: Line up the feature and the image

Step-2: Multiply each image pixel by the corresponding feature pixel.

ReLU layer: To remove every negative value from the filtered images and replaced it with zero's. This is done to avoid the values from summing up to zero. ReLU transform function only activates a node if the input is above a certain quantity, while the input layer is below, the output is zero, but when the input rises above a certain threshold, it has a linear relationship with the dependent variable. Function of ReLU like:

F(x) = 0 if x<0
{x if x>=0

Pooling layer: To shrink the image stack into smaller size *Fully Connected layer*: Final layer, where the actual classification happens.

Here we take our filtered and shrinked images and put them into single list.

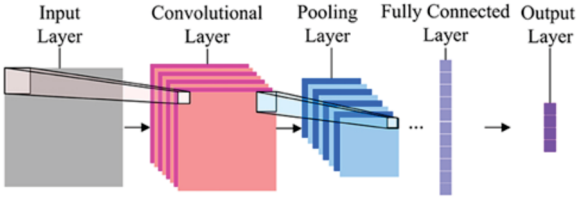

Figure 3: Layers of CNN model

Recurrent Neural Network

Recurrent Neural Networks (RNNs) are a type of Neural Network where the output from previous step is fed as input to the current step. It can handle sequential data, considers the current input and also the previously received inputs, can memorize previous inputs due to its internal memory. Important parameters that affect the performance of RNNs are activation function, dropout rate and loss function [6].see figure II for a diagram of a RNN

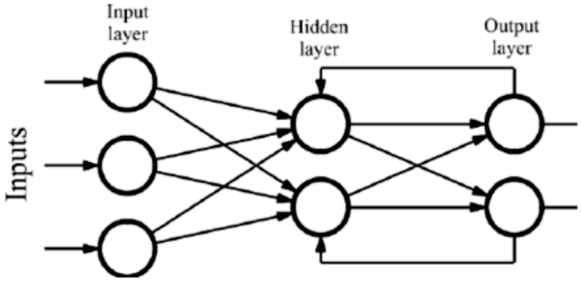

Figure 4: RNN with 1 hidden layer

Long Short Term Memory systems

Standard RNNs experience the ill effects of evaporating or detonating inclination issues. To address these issues, the Long Short-term Memory architecture was proposed. LSTMs contain a memory cell which keeps up its state after some time. Also, gating units are utilized to direct the data stream into and out of the memory cell. All the more explicitly, an input entryway can enable the info sign to change the cell state or counteract it (i.e., sets the input gates to zero). An output gate can permit the cell state to influence neurons in the shrouded layers or square it. An overlook door empowers the cell to recollect or overlook

its past state. Initially. The relative importance of each component is not clear [7]. Important LSTM parameters that affect the quality of the output are the number of neurons in the hidden layers, activation function and inner activation function and dropout rate [8].

Gated Recurrent Unit

A gated recurrent unit makes each intermittent unit adaptively catch conditions of various time scales. Albeit like a LSTM, the GRU has gating units that tweak data stream into the unit, nonetheless, GRUs doesn't have separate memory cells. Unlike LSTMs, GRUs exposes their whole state each time [9]. The same parameters that affect LSTMs apply to GRUs too [10].

COMPARATIVE ANALYSIS OF RECENT STUDY

After the literature review the deep learning methods were studied for credit card fraud detection. Following is the table for the relative analysis of various deep learning methods for credit card fraud detection.

Table – 1 Comparative Analysis Of Deep Learning Methods For Credit Card Fraud Detection

Sr No	Title & Publication	Learning Paradigm	Techniques	Challenges
1	Title: An Effective Real-Time Model for Credit Card Detection Based on Deep Learning [1] Publication: ACM-Conference, 2019	Unsupervised	Deep Neural Network (DNN) With Auto-Encoder	Cannot effectively handle confusion matrix parameter, Highly Unbalanced Dataset
2	Title: Ensemble Learning for Credit Card Fraud Detection [2] Publication: ACM-Conference,2018	Unsupervised	Feed Forward Neural Networks	Limited to dataset having numeric value
3	Title: Credit Card Fraud Detection Using Convolutional Neural Networks [3] Publication: Springer - Conference,2016	Supervised	Convolutional Neural Network	Data imbalance is too high
4	Title: Deep Learning Detection Fraud in Credit Card Transactions [4] Publication: IEEEJournal,2018	Supervised	Artificial Neural Network(ANN), Recurrent Neural Network(RNN), Long Short-term Memory(LSTM), Gated Recurrent Units(GRU)	Hyper parameter like momentum, batch size, number of the epoch, dropout rate not included

Studies of parameter evaluation from different deep learning methods were analyzed. This parametric evaluation gives some new ideas to propose a novel approach for deep learning method.

PROPOSED APPROACH

After the study of comparative analysis of deep learning methods for credit card fraud detection, different parameters were evaluated using different deep learning methods like DNN with Auto-Encoder, Feed Forward Neural Network, CNN, ANN, RNN, LSTM, GRU was studied. The literature study helps us to find that some more parameters can be evaluated using supervised deep learning methods.

Following are the some of the objectives find out after the detailed review from different deep learning methods:

- To achieve High Non-linearity of Dataset
- To work on large amount of Data
- To analyze lots of features of dataset
- To work on mostly unlabeled Data in the dataset
- To analyze various other parameters of deep learning methods

Detailed steps for deep learning involves pre-processing of dataset, feature extraction, training the dataset, reduction in errors, testing the dataset & generating the output are shown in following proposed system.

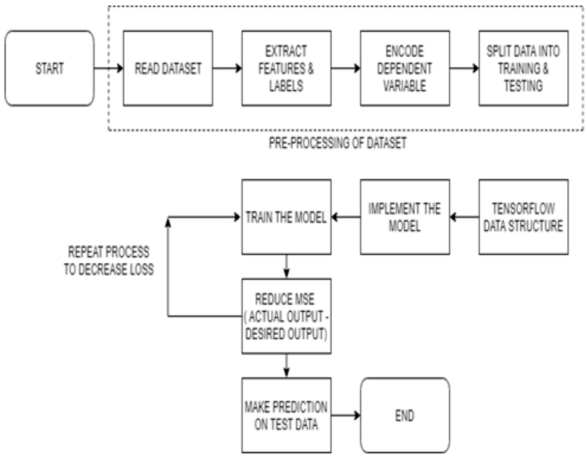

Figure 5: Proposed System for Credit Card Fraud Detection with Deep Learning Method

CONCLUSION & FUTURE WORK

Credit Card Fraud is a demonstration of criminal deceptive nature. This article has audited late discoveries in the charge card field. This paper has distinguished the various sorts of frauds, for example, bankruptcy fraud, counterfeit fraud, theft fraud, application fraud and behavioral fraud, and talked about measures to identify them. Such measures have included pair-wise coordinating, decision trees, clustering systems, neural networks, and genetic algorithms.

From a moral viewpoint, it very well may be contended that banks and Credit Card organizations should endeavor to recognize every deceitful case. However, the amateurish fraudster is probably not going to work on the size of the expert fraudster thus the expenses to the bank of their identification might be uneconomic. The bank would then be looked with a moral situation. As the subsequent stage in this examination program, the center will be upon the execution of a 'suspicious' scorecard on a genuine informational collection and its assessment.

After the investigation of similar examination of deep learning strategies for credit card fraud recognition, there is a tremendous extension for various parameter assessments. A portion of the hyper parameters like confusion matrix, momentum, batch size, and number of epoch can be taken care of adequately.

REFERENCES:

[1] Abakarim, Y., Lahby, M., & Attioui, A.: An Efficient Real-Time Model for Credit Card Fraud Detection Based on Deep Learning. In Proceedings of the 12th In International Conference on Intelligent Systems: Theories and Applications (p. 30). ACM, (2018)
[2] Sohony, I., Pratap, R., & Nambiar, U.: Ensemble learning for credit card fraud detection. In Proceedings of the ACM India Joint International Conference on Data Science and Management of Data (pp. 289-294). ACM, (2018)
[3] Fu, K., Cheng, D., Tu, Y., & Zhang, L.: Credit card fraud detection using convolutional neural networks. In International Conference on Neural Information Processing (pp. 483- 490). Springer, Cham, (2016)
[4] Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P.: Deep learning detecting fraud in credit card transactions. In 2018 Systems and Information Engineering Design Symposium (SIEDS) (pp. 129-134). IEEE, (2018).
[5] Abdallah, A., Maarof, M. A., & Zainal, A.: Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90-113, (2016)
[6] Bengio, Y., Boulanger-Lewandowski, N., & Pascanu, R.: Advances in optimizing recurrent networks. In Acoustics, Speech and Signal Processing (ICASSP), IEEE International Conference on (pp. 8624-8628). IEEE (2013)
[7] Wu, Zhizheng, and Simon King.: Investigating gated recurrent networks for speech synthesis. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2016)
[8] Greff, Klaus, et al. "LSTM: A search space odyssey." IEEE transactions on neural networks and learning systems 28.10 2222-2232 (2016):
[9] Chung, Junyoung, et al. "Empirical evaluation of gated recurrent neural networks on sequence modeling." arXiv preprint arXiv:1412.3555 (2014).
[10] Wen, Ying, et al. "Learning text representation using recurrent convolutional neural network with highway layers." arXiv preprint arXiv:1606.06905 (2016).