Credit Card Fraud Detection Using Deep Learning

Jayshree Kathiriya

Abstract: When the word fraud comes in to the any discussion, the credit card frauds clicks in our mind immediately. Now peoples are using cards for the shopping and bill payments or any money transactions. Now a days we are using a cards installed with smart chip. But as we know there is two sides of coin. As the same way when any new technology arrives in to the market for the easiness of human's life it also comes with risk. Credit card fraud detection have been a very popular research topic since past years.

As per the recent trends we are using an applications like paytm, phone pe, google pay etc. for the usual needs of money expenses. We are using this kind of apps in any small grocery shop expense to big amount of fund transfers. This applications are directly connected to our bank accounts, and we have bank in one application. But the fraud can be done while using this kind of application while doing a money transaction. Up till now we are doing the analysis of bank data but in this paper we are going to use application data. Very less work is done based on this kind of data. As we know many data mining methods are applied for detection of the fraud and recently deep learning is also used for this purpose. We are going to apply various deep learning methods and approaches to get higher performance rate.

Keywords: credit card fraud, fraud detection, deep learning, fraud detection techniques, machine learning, neural networks.

I. INTRODUCTION

In the recent years by the improvement of machine learning methods it is beneficial to utilize these technics to prevent such difficulties and decide about the upcoming events [1]. After machine learning to get more accuracy we can apply deep learning. Deep Learning algorithms are a class of machine learning algorithms. Deep learning digs very deep for any processing feature. Deep learning uses multiple non-linear pre-processing units for feature extraction and transformation. These processing units discover intermediate representations in a hierarchical manner. The features discovered in one layer form the basis for processing of the other next layer. In this way, Deep Learning algorithms learn intermediate concepts between raw input and target variable [2].

In this paper, we will focus on credit card fraud and measures to detect the fraud. Now a day's machine learning and deep learning techniques are giving more efficient results. According to the complexity of such data and the user's behaviors, the realm of data mining suffers from the low accuracy comparing with the other subjects. In the data mining methods, the accuracy was about 76% and in the recent ones it reaches about 82% using machine learning methods [1].

According to one research paper there is future work which says that further research is needed to determine when model performances cease to improve with network size increases. Further research could also be directed towards assessing model sensitivity to hyper parameters not included in our initial grid search such as momentum, batch size, number of epochs, and dropout rate [2]. So in this paper we apply machine learning methods on data and also the deep learning techniques on the data and we will see the accuracy report of all applied methods.

II. BACKGROUND

In this section we discuss about some related concepts.

A. Machine Learning:

The machine learning is classified into two categories:

1. Supervised learning and
2. Unsupervised learning.

In supervised learning we train the system using the bunch of some data contain different behaviors. We train the system like wise so any new transactions comes with that fraud symptoms the system recognize it as fraud transition. In unsupervised learning there is no any training phase we directly give the data for the testing. So in that situation various clusters are generated having same behaviors and when any new transaction arrives than the system falls that transactions to matching clusters.

B. Deep Learning:

Deep learning also known as deep structured learning or hierarchical learning. It is part of a broader family of machine learning methods. Deep learning is based on learning data representations, as opposed to task-specific algorithms. Learning can be supervised, semi-supervised or unsupervised. Deep learning architectures such as: deep neural networks, deep belief networks and recurrent neural networks.

Deep learning models are mostly inspired by information processing and communication patterns in biological nervous systems of a hutments brain. Deep learning have various differences from the structural and functional properties of biological brains especially human brains, which make the deep learning incompatible with neuroscience evidences.

C. Recurrent neural network (RNN):

As a part of supervised deep learning I am using recurrent neural network approach in the further work. A recurrent neural network is a class of artificial neural network where connections between nodes form a directed graph along a sequence. This feature of sequence allows it to exhibit temporal dynamic behavior for a time sequence. Unlike feed forward neural networks, RNNs can use their internal state (memory) to process sequences of inputs backwards also.

Recurrent Neural Networks are adapted to the modelling of sequential data. Artificial neural networks do not offer the scalability required to model large sequential data [2]. In addition to links between layers, recurrent neural networks allow for the formation of links between neurons co-located in the same layer, which results in the formation of cycles or we can say a loop in the network's architecture.

Cycles allow the neurons in the model to share weights which are calculated from the inter dependencies of the parameters throughout successive values of a given input at different time steps. This allows for the activation function generally used relu or tanh to take into account the state of the neuron at a previous stage in time. Thus, the state can be used to transfer some aspects of the previous time stages to upcoming time stages. Important parameters that affect the performance of RNNs are activation function, dropout rate and loss function.

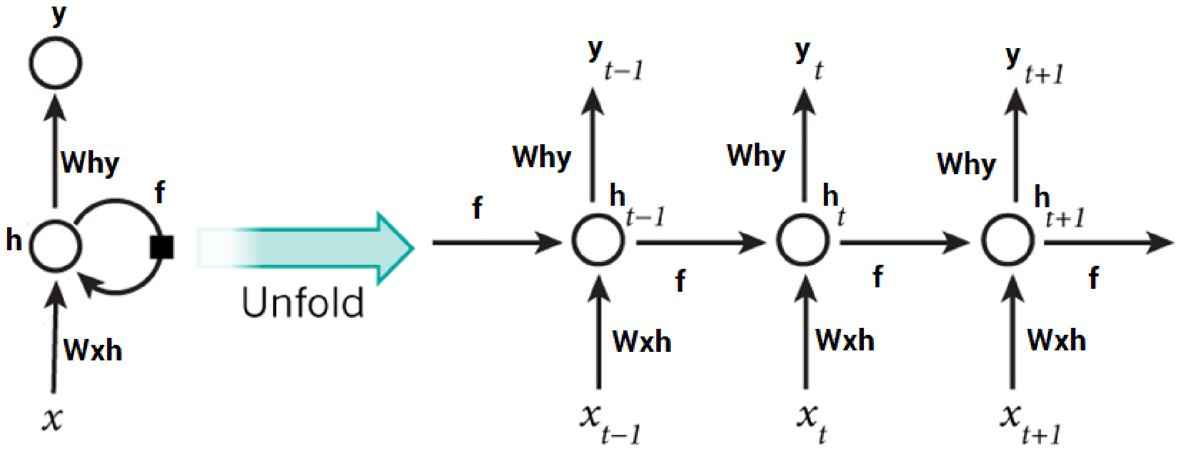


Fig. 1: Recurrent Neural Network

D. Autoencoders:

The autoencoder is similar to a simple multilayer perceptron (MLP). Its learning method is similar, but there is a major difference that is unsupervised learning. In such networks the input is the available features of data, like MLP, but instead of reaching a target the goal is to reach to the input again [1].

The procedure of converting raw data to a low dimension space named encoding and the reverse operation that reconstruct the original data is decoding. Given figure shows the structure of such a simple network. The results in such network is very similar to the results of linear feature extractions.

To improve the results a nonlinear function can be added to the neurons that leads to regarding the nonlinearity conditions. Then autoencoder can be used in several applications and the main advantage is to extract best features for data analysis.

More specifically, let’s take a look at Autoencoder Neural Networks. This Autoencoder tries to learn to approximate the following identity function:

$$f_{W,b}(x) \approx x$$

While trying to do just that might sound trivial at first, it is important to note that we want to learn a compressed representation of the data, thus find structure. This can be done by limiting the number of hidden units in the model. Those kind of autoencoders are called under complete.

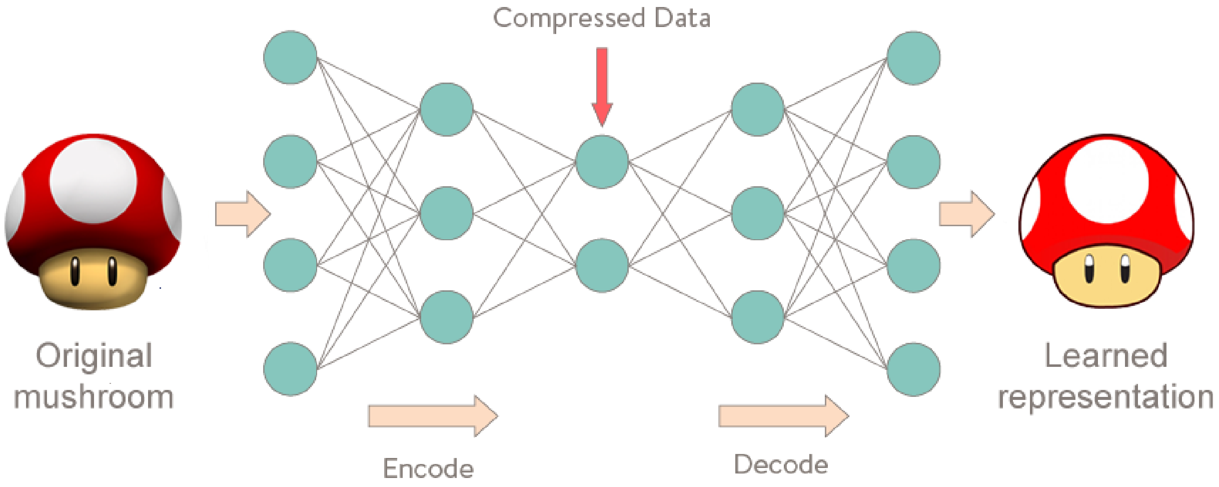


Fig. 2: Autoencoders

The result in this kind of network is similar to the result of liner feature extraction like PCA. The main difference is the constraint of the orthogonality, while the final result shows the same conditions. To improve the result a non-liner function can be added to the neurons the leads to nonlinearity conditions. [1]

III. PROPOSED METHOD

There are several behavior of the customers in the money transactions, extracting the appropriate pattern to detect fraudulent transactions is complex task. At the beginning level I have applied multiple supervised learning techniques on my data set. I applied decision tree, k nearest neighbor random forest and logistic regression on my data set. I split the data into 80:20 ratio of training data and testing data.

Further I applied Recurrent Neural Network as Deep Learning approach. In that I have applied different hidden layers as well as find the best sequential model which suites the data and behavior of transactions. I have also applied the different neuron values at different layers. I have also solve the work of future work of one latest IEEE paper. As per that I have change the batch size of the network and also change of activation function. In a result section I have generated one table with different modes and its parameters.

As the disadvantage gradient vanishing problem in RNN to overcome that I have also applied LSTM. Whenever any know behavior of the transaction is arrive the supervised learned technique recognize it either fraud or not fraud, but when any different behavior is arrived which is not there in training data set then this model fails to predict the fraud.

To overcome this problem I found the solution in unsupervised learning. In which I am using the autoencoders for predict the different behaviors of the transactions. Autoencoder is self-learning method and it does not need any training dataset so it learns automatically learn there is any odd or different transaction is arrived.

Table 1: The algorithm of data discrimination

Input: raw features
Output: class labels

1. Autoencoder uses 4 fully connected layers with 8, 5, 5 and 10 neurons respectively. The first two layers are used for our encoder, the last two go for the decoder. Additionally, L1 regularization will be used during training:
2. Seven different layers are used for the model and it contains encoder and decoder layers.
3. First input layer is encoder layer used for encoding.
4. Last layer is decoder which is output layer which removes the encoding.
5. Train the model for 100 epochs with a batch size of 256 samples and save the best performing model to a file.

IV. EXPERIMENTAL RESULTS

In this section we are going through the whole experimental process. Starting with the dataset description in brief. Then after data analysis process using statistical. Later on applying machine learning methods to the data for the accuracy rate of fraudulent transaction. And finally applying Recurrent Neural Network & Long Short Term Memory on the dataset. At the end compare the efficiency parameters and conclude these Deep Learning approaches are good or bed to detect fraud transaction.

A. Dataset: For prediction of the fraud transection, I need dataset of money transactions. This data was extracted from: https://www.kaggle.com/ntnu-testimon/paysim1[5]. It is a synthetic dataset of mobile money transactions. Each step represents an hour of simulation. This dataset is scaled down 1/4 of the original dataset which is presented in "PaySim: A financial mobile money simulator for fraud detection". Dataset contains 6362620 rows and 11 different columns. The columns are:

- step (numerical): Unit of time in the real world. 1 step is used as 1 hour of time.
- type (categorical): CASH-IN, CASH-OUT, DEBIT, PAYMENT and TRANSFER
- amount (numerical): amount of the transaction
- nameOrig: customer who started the transaction
- oldbalanceOrg (numerical): initial balance before the transaction
- newbalanceOrig (numerical): customer's balance after the transaction.
- nameDest: recipient ID of the transaction.
- oldbalanceDest (numerical): initial recipient balance before the transaction.
- newbalanceDest (numerical): recipient's balance after the transaction.
- isFraud (boolean): identifies a fraudulent transaction (1) and non fraudulent (0)
- isFlaggedFraud (boolean): flags illegal attempts to transfer more than 200.000 in a single transaction.

B. Results:

According to the complexity of the data and user's behavior different techniques generate different predictions. So firstly I have applied four different methods of Machine Learning approach. And efficiency parameters are shown by the below given table.

Table 2: Comparison of all ML methods

Method	Accuracy	Precision	Recall	F1 score
Decision tree	0.999613	0.987013	0.718676	0.831737
K nearest neighbor	0.999613	0.960123	0.739953	0.835781
Random forest	0.999645	0.975460	0.751773	0.849132
Logistic regression	0.999277	0.925110	0.49654	0.646154

Now moving to the Deep Learning approach I have applied Recurrent Neural Network and its different hidden layers. The given below table shows the accuracy and loss by using each different layers.

Table 3: Layering comparison of RNN

Total layers	Hidden layers	Accuracy	Loss
9	7	99.87%	02.05%
7	5	99.93%	00.03%
5	3	99.93%	00.28%
3	1	99.93%	00.34%

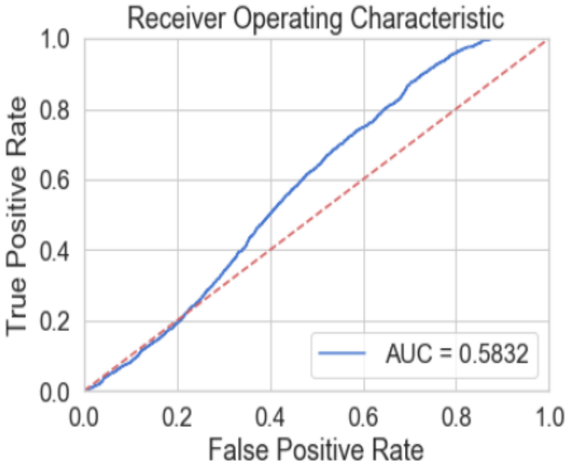
As per the future work of one paper I have prepared different models based on different parameters. For finding the best suite for the data set. Let's look in the table for performance measure based on different models.

Table 4: different models based on different parameters

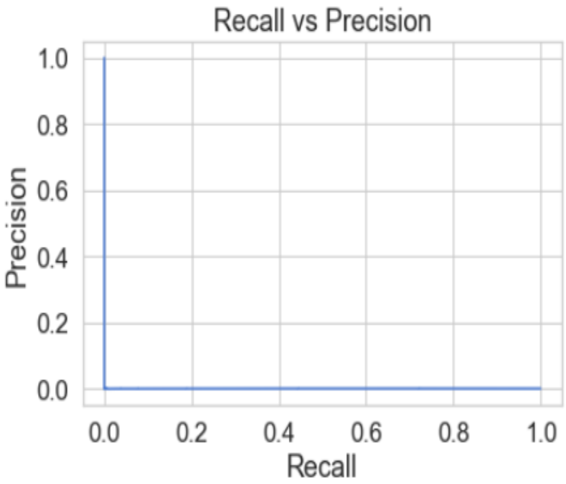
Parameters	Model-1	Model-2	Model-3	Model-4	Model-5	Model-6	Model-7
Hidden layers	7	5	6	6	6	6	6
Values of nodes	64 & power of 2	64 & power of 2	150 all	150 all	50,100,150 onwards	16 & power of 2	512 & power of 2
Learning rate	0.8	0.8	0.5	0.5	0.5	0.5	0.5
Activation function	Relu	Relu	Tanh	Tanh	Tanh	Tanh	Tanh
Batch size	128	128	128	256	256	64	512
epochs	7	5	10	20	10	10	5
Dropout rate	0.4	0.4	0.4	0.4	0.4	0.4	0.4
Loss	02.025%	00.03%	0.41%	0.42%	0.34%	0.42%	-
Accuracy	99.87%	99.93%	99.92%	99.93%	99.92%	99.92%	-

In a last model there is 2 hours and 50 minutes of processing time for 1 epoch so I pause that transaction in between. Based on the above model the best fit model is model-2 having less loss of function and higher accuracy. I have also applied one model of Long Short Term Memory which have 58% of accuracy with 42% of loss.

Then after I have applied the autoencoders for prediction of different behavior of the money transaction. I got the 0.6038 accuracy score while using 100 epoch with three different hidden layers as I explain in algorithmic table.



Graph 1: ROC based on TP rate and FP rate



Graph 2: ratio of precition and recall

ROC curves are very useful tool for understanding the performance of binary classifiers. This data is a very imbalanced dataset. Nonetheless, let's have a look at our ROC curve: The ROC curve plots the true positive rate versus the false positive rate, over different threshold values. Basically, we want the blue line to be as close as possible to the upper left corner. While this results look pretty good, we have to keep in mind of the nature of our dataset.

Precision measures the relevancy of obtained results. Recall measures how many relevant results are returned. Both values can take values between 0 and 1. High recall but low precision means many results, most of which has low or we can say no relevancy. When precision is high but recall is low we have the opposite—few returned results with very high relevancy. Ideally, you would want high precision and high recall—many results with that are highly relevant.

V. CONCLUTION

Fraud detection is a very much popular topic in the financial era and loss of the money. All the research papers I have referred are having the classical bank transaction data but my data is application data. I choose this kind of data because of now a days we are using multiple applications for all our money transactions. There are multiple techniques applied on the bank data to predict the frauds but very less work is done on this kind of data. As per the data and users behavior changes the resulting parameters also changes accordingly. On my data Decision Tree and Random Forest algorithm provides high accuracy but it has a major disadvantage of over fitting to the data.

So one approach of supervised Deep Learning namely Recurrent Neural Network comes as solution. I optimize multiple models on the data but as per my data behavior the model having 5 hidden layers is best feet which is providing 99.93% accuracy with lowest loss of 00.03%. And when talking to the odd behavior in the network this supervised techniques fails to predict. So I have applied autoencoders which have accuracy very less than the RNN but works well for the odd behaviors.

References

[1] Zahra Kazemi, Houman Zarrabi, "Using deep networks for fraud detection in the credit card transaction", 2017 IEEE.

[2] Abhimanyu Roy, Jingyi Sun, Robert Mahoney, Loreto Alonzi, Stephen Adams, Peter Beling, "Deep Learning Detecting Fraud in Credit Card Transactions" 2018 IEEE.

[3] Juan Luis López Herrera, Homero Vladimir Rios Figueroa, Ericka Janet Rechy Ramírez "Deep Fraud. A fraud intention recognition framework in public transport context using a deep-learning approach" 2018 IEEE

[4] Lusis "A Comparison of Machine Learning Techniques for Credit Card Fraud Detection" April 20, 2017

[5] Lopez-Rojas, Edgar Alonso, "Applying Simulation to the Problem of Detecting Financial Fraud", 2016

[6] John O. Awoyemi, Adebayo O. Adetunmbi, Samuel A. Oluwadare "Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis", 2017 IEEE

[7] Khyati Chaudhary, Jyoti Yadav Bhawna Mallick, "A review of Fraud Detection Techniques: Credit Card", International Journal of Computer Applications (0975 – 8887) Volume 45– No.1, May 2012

[8] Ishu Trivedi, Monika, Mrigya Mridushi, "Credit Card Fraud Detection", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 1, January 2016

[9] Masoumeh Zareapoor, Seeja.K.R, M.Afshar.Alam "Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria", International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, August 2012

[10] Apapan Pumsirirat, Liu Yan, "Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine" 2018 IJACSA.

[11] S.Vimala, K.C.Sharmili, "Survey Paper for Credit Card Fraud Detection Using Data Mining Techniques", 2017 IJIRSET.

[12] Masoumeh Zareapoor, Seeja.K.R, M.Afshar.Alam, "Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria", 2012 International Journal of Computer Applications.

[13] V.Dheepa, Dr. R.Dhanapal "Analysis of Credit Card Fraud Detection Methods" International Journal of Recent Trends in Engineering, Vol 2, No. 3, November 2009 126

[14] Suman "Survey Paper on Credit Card Fraud Detection" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 3, March 2014 ISSN: 2278 – 1323 All Rights Reserved © 2014 IJARCET 827

[15] Suman, Nutan "Review Paper on Credit Card Fraud Detection" International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013

[16] Wen-Fang YU, Na Wang "Research on Credit Card Fraud Detection Model Based on Distance Sum" 2009 International Joint Conference on Artificial Intelligence