ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# Credit Card Fraud Detection using Deep Learning

Yamini Pandey
Department of Computer Science
Indira Gandhi Delhi Technical University for Women
Delhi, India

*Abstract:* With the growth of ecommerce websites people and financial companies rely on online services to carry out their transactions that has led to an exponential increase in the credit card frauds.Fraudulent credit card transactions lead to a loss of huge amount of money. The design of an efficient fraud detection system is necessary in order to reduce the losses incurred by the customers and financial companies. Research has been done on many models and methods to prevent and detect credit card frauds. Fraudsters masquerade the normal behaviour of customers and the fraud patterns are changing rapidly so the fraud detection system needs to constantly learn and update.Deep Learning has been used in many fields like in speech recognition, image recognition and natural language processing. This paper aims to understand how Deep Learning can be helpful in detecting credit card frauds. Deep learning package H2O is used in this paper to train a deep learning model. H2O deep learning framework is an efficient framework to handle large datasets and perform deep learning. The performance evaluation of the deep learning model is done on the UCSD Data Mining Contest2009 data and it is found that deep learning models give a high accuracy to detect the fraudulent transactions.

***Keywords:*** deep learning; H2O; deep neural network; fraudulent; legitimate; frauds

## I. INTRODUCTION

In the online sector fraud is a major problem to merchants, financial companies and customers. It is not always possible for human analysts to detect fraudulent patterns in transactionswhich are characterized by a large number of samples,many dimensions and online updates so there is a need of automatic fraud detection systems [1].The cardholder is also not reliable in reporting the loss, theft or fraudulent use of the card [2]. Credit-card-based purchases can be divided into two categories: 1) physical card,2) virtual card. In a physical-cardbasedpurchase, the cardholder presents his card to a merchant for making a payment. The attacker has to stealthe credit card in order to carry out fraudulent transactions in this type of purchase. In the virtual card kind of purchase, someimportant information about the card such as the card number, expirationdate, secure code are required to make the payment. Thefraudster just needs to know the card details to commit fraud in such kinds of purchases[3].

Various challenges are faced by researchers while performing stud on credit card transactions. Finding a real dataset is a big challenge. Second challenge is to keep the system updated with the changing behaviour of the fraudsters. Another challenge is that the number of fraudulent transactions is much smaller than the genuine ones so the data distribution is unbalanced. Many machine learning algorithms underperform for unbalanced dataset and methods like undersampling, oversampling and SMOTE(synthetic minority oversampling technique) have been proposed to improve their performances [4].In [5] sampling method called Oversampling via randomly imputed features (ORIF) is used to deal with the imbalanced ecommerce transactions. ORIF generatesartificial instances for minority classes (i.e. fraudulent) and doesnot impose any restructuring on the data compared to SMOTE.

Statistical fraud detection methods are divided into two categories: supervised andunsupervised. In supervised fraud detection techniques, models are estimated based on the samples of fraudulent and genuine transactions in order to classify new transactions as fraudulent or genuine. While in unsupervised methods, outliers or unusual transactions are identified as potential cases of fraudulent transactions. Both these fraud detection techniques predict the probability of fraud in any given transaction. Thereare various algorithms used for fraud detection, each of them tries to increase the detection rate while reducing the false alarm rate. Different algorithms have been used for detecting frauds such as Bayesian algorithm [6], K-Nearest Neighbour [7], Support Vector Machine [7], and MarkovModel [4]. Most of the research found is based on learning the buyingbehaviour of the customers using various data mining techniques and usingthese learnings to predict unseen credit card transactions. In [8] customers historical transactions are aggregated and a logistic regression model is built to learn buying behaviour of customer and is used to predict the new transaction as genuine or fraudulent. In [9] and [10] a application of a biologicaltechnique, Artificial Immune System(AIS)is investigated to find detect fraud in credit card transactions. AIS learnsthe normal pattern of the customer buying behaviour and then detects the fraudulent transaction as soon as it enters the system. In [4]a fraud detection model is built using Hidden MarkovModel (HMM) based on normal customer spending behaviour. Transactions that are rejected by HMM are classified as fraudulent.In [11] a new framework called ’Fraud Miner’, is proposed which is based on Frequent Itemset Mining approach to learn customers normal buyingbehaviour. The matching algorithm tags every new incoming transaction as fraudulent or legitimate.

Fraudsters are becoming increasingly smarter and adaptive so there is a need of scalable and computationally efficient prediction models. In this paper a fraud detection system based on deep learning algorithm with H20 framework has been proposed. Deep learning helps to learn complex highly varying functions not present in the training examples. The performance of the deep learning model is observed on the UCSD-FICO data mining contest 2009 data. With the evolution of new technology like H2O andnew evolving machine learning techniques like Deep Learning, there is a need to study the application of these new techniques for fraud detection.

## II. MATERIALS AND METHODS

### A. *Deep Learning*

Machine-learning technology find man application: from web searches to content filtering on social networks to recommendations on e-commerce websites. Systems based on machine learning algorithms are used in image recognition, speech recognition and semantic analysis. These applications make use of a class of techniques known as deep learning [12].

Deep learning is a branch of machine learning algorithms that [13]:

- use many layers of non-linear processing units for feature extraction as well as transformation. Output of each successive layer is the input of the previous layer. Deep learning algorithms may be unsupervised or supervised and the applications include pattern analysis (unsupervised) and classification(supervised).
- learn multiple levels of features or representations of the data. Features at the higher level are derived from lower level features to form a hierarchical representation.
- are part of the broader machine learning field that learn representations of data.

Deep learning architecture consists of multilevel hidden layers of non-linear processing units in which each neuron sends the data to a connected neuron present within the hidden layers [14]. A weighted combination of all input signals is aggregated andthen an output signal transmitted by the connected neuron. Deep learning consists of many hyper parameters which are used to tune the models. There aremany hyper parameters in deep learning which are used totune the models [15].

### B. *H2O's Machine Learning Framework*

H2O is the open source in platform for predictive analytics on Big Data. Several algorithms like neural networks, random forests, linear modes and gradient boosting are available [15]. The H2O software runs can be called from python, the statistical package R, and other environments.

**H2O package in R:** H2O package provides h2o.deeplearning function for building models. It is built on Java. It is used to build multilayer feed forward neural networks. It has the following features:

- Adaptive learning rate
- Distributed and parallel computation
- Regularization options to prevent over fitting
- Hyper parameter optimization using random/grid search
- Automatic missing values imputation

**H2O Deep Learning Architecture**: H2O follows the model of multi-layer, feed forward neural networks for predictive modelling as shown in figure.2. Multi-layer, feed forward neural networks comprise of multiple layers of interconnected neurons, starting with an input layer in order to match the feature space followed multiple layers and ending with a classification layer to match the outer space[15].

The inputs and outputs of the model's units follow the basic logic of the single neuron, a biologically inspired model of the human neuron as shown in figure.1.The weighted combination $\alpha = \sum_{i=1}^{n} w_i \, x_i + b$ of input signals is aggregated, an output signal f (α) is then transmitted by the connected neuron. The function f is a non-linear activation function and bias b is neuron's activation threshold [15].Non –output layers consists of Bias units. The output of the network is determined by the weights linking the neurons and biases.

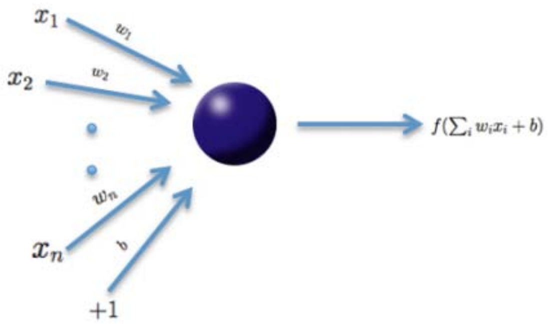


Figure 1 Neuron[15]

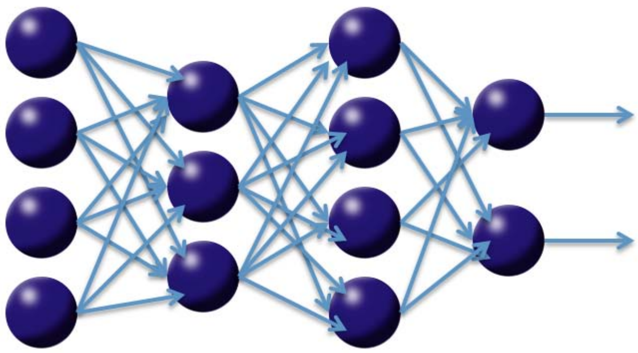


Figure 2. Multi-layer feed forward neural network [15]

### C. *Problem Data*

UCSD-FICO Data miningcontest 2009 data set is used is order to evaluate the proposed model [16].The dataset is a real dataset of e-commerce transactions.There are two datasets of which dataset used consists of 19 attributes. The dataset consists oftraining set and testing set. Thetraining set is labelled and the testing set is unlabelled. The labelled training dataset is used for performance evaluation of the proposed model.

## III. IMPLEMENTATION OF DEEP LEARNING MODEL USED FOR CREDIT CARD FRAUD DETECTION

The performance evaluation of Deep Learning model on the credit card dataset is done using on Rstudio using the H2O package. The following steps are performed to evaluate model performance:

- Data preprocessing
- Set up and connect to a local H2O cluster from R and load the input dataset
- Train a deep neural networks model
- Evaluate Performance

### A. *Data preprocesing*

The dataset consists of 94682 transactions with 20 fieldsincludingclass labels—amount, hour1, state1, zip1, field1, domain1, field2, hour2, flag1, total, field3, field4, field5, indicator1,indicator2, flag2, flag3, flag4, flag5, and Class.The fields total and amount as well as hour1and hour2 are same so total and hour2 are removed. The dataset now consists of 18 attributes: amount, hour1, state1, zip1, field1, domain1, field2, flag1, field3, field4, field5, indicator1, indicator2, flag2, flag3, flag4, flag5, and Class.

### B. *Set up and connect to local H2O cluster from R and load the input dataset*

1. Start of H2O cluster:We can work with data in two ways on H2O. We can use commands in RStudio or we can use H2O flow interface. The following command is used to start a local cluster:
   *localH2o <- h2o.init(nthreads = -1, max_mem_size ="20G")*
2. After starting H2O cluster the dataset named df is loaded on H2O by the name h2odf:
   *h2odf <- as.h2o(df)*
3. The input data loaded on to H2O is then split into training, testing and validation dataset. 60% of the data forms the training data, 20% forms the validation data and rest 20% forms the testing data
   *split <- h2o.splitFrame( h2odf, c(0.6,0.2), seed = 1234)*
   *train <- h2o.assign( split[[1]], "train" ) # 60%*
   *valid <- h2o.assign( split[[2]], "valid" ) # 20%*
   *test <- h2o.assign( split[[3]], "test" ) # 20%*

### C. *Train a deep neural network model*

A deep neural network model is then trained :

```
model_dl_1 <- h2o.deeplearning(
model_id = "dl_1",
training_frame = train,
validation_frame = valid,
x = input,
y = output,
activation = "Rectifier",
hidden = c(200, 200),    # default = 2 hidden layers with
200 neurons each
epochs = 1,
variable_importances = TRUE
)
```

The deep learning model uses the following parameters: 1. hidden - It specifies the number of hidden layers and number of neurons in each layer in the deep learning architecture.

2. epochs - It represents the number of iterations to be done on the data set.

3. activation - It represents the type of activation function to use. The major activation functions in h2o are Tanh, Rectifier, and Maxout.

4. variable_importance: It gives the importance of variables listed from greatest importance, to least importance.

### D. *Evaluating model performance*

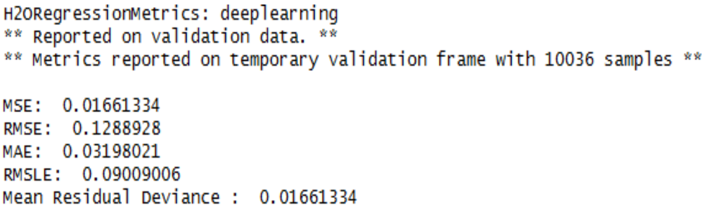
The performance of the model is evaluated by running the following command:

*h2o.varimp_plot(model_dl_1)*

We obtain a table giving the importance of the different attributes to classify a transaction as genuine or legitimate.

## IV. Results

The deep learning model gives the following performance metrics:



```
H2ORegressionMetrics: deeplearning
** Reported on validation data. **
** Metrics reported on temporary validation frame with 10036 samples **

MSE:  0.01661334
RMSE:  0.1288928
MAE:  0.03198021
RMSLE:  0.09009006
Mean Residual Deviance :  0.01661334
```

Figure 3 Performance Metrics

MSE: Mean Squared Error
RMSE: Root Mean Squared Error
MAE:Mean Absolute Errors
RMSLE:Root Mean Squared Log Error

The variable importance plot is obtained in order to check the importance of the various attributes in classification:

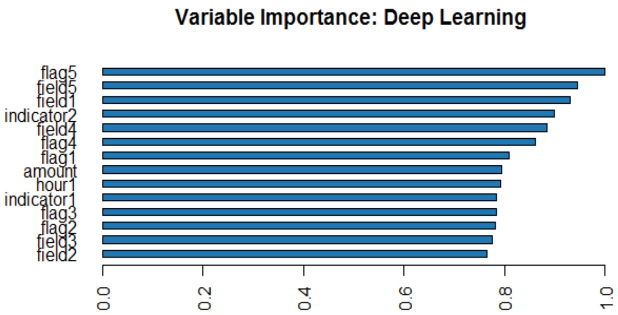


Figure 4 Variable Importance Plot

## V. Conclusion

Credit card fraud is a rapidly growing problem due which financial institutions are losing huge amount of money. Researchers are implementing various new techniques to enhance the credit card fraud detection systems so that credit card frauds can be decreased. Many machine learning methods have been implemented to prevent credit card frauds. Deep learning is a branch of machine learning that is used in many fields like image recognition, speech recognition and many more. Deep learning provides a way to explore complex features within the data so that the model can learn better to predict frauds more efficiently with less false alarms. In this paper deep neural network model is used on the UCSD-FICO DataMining Contest 2009 data.The model is trained on the credit cardtransactions using R integration with

H2O.Performance metrics of the deep learning model has been obtained that shows the model gives very less error hence the accuracy of the model is high. The model accurately classifies the fraudulent transactions. The importance of the various attributes on the classification is also obtained that shows which attribute is the most and the least important for classification of transactions as fraud or legitimate. It has also been studied that H2O provides an efficient framework in order to model the deep learning models and the performance of the model can be easily evaluated on the framework.

In this study only the H2Odeep learning library was used, further other deep learning libraries like MXnet, Torch,TensorFlow, MLLibcan also be used in the field of credit card fraud detection in order to explore the power of deep learning.

## VI. References

[1] Dal Pozzolo, Andrea. "Learned lessons in credit card fraud detection from a practitioner perspective." Expert systems with applications 41.10 (2014): 4915-4928.

[2] Pavía, Jose M., Ernesto J. Veres-Ferrer, and Gabriel Foix-Escura. "Credit card incidents and control systems." International Journal of Information Management 32.6 (2012): 501-503.

[3] Japkowicz, Nathalie, and Shaju Stephen. "The class imbalance problem: A systematic study." Intelligent data analysis 6.5 (2002): 429-449.

[4] Srivastava, Abhinav. "Credit card fraud detection using hidden Markov model." IEEE Transactions on dependable and secure computing 5.1 (2008): 37-48.

[5] Lee, M., & Ham, S. (n.d.). E-commerce Transaction Anomaly Classification, 6-10.

[6] Excell, David. "Bayesian inference–the future of online fraud protection." Computer Fraud & Security 2012.2 (2012): 8-11.

[7] Zareapoor, Masoumeh, K. R. Seeja, and M. Afshar Alam. "Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria." International Journal of Computer Applications 52.3 (2012).

[8] Jha, Sanjeev, Montserrat Guillen, and J. Christopher Westland. "Employing transaction aggregation strategy to detect credit card fraud." Expert systems with applications 39.16 (2012): 12650-12657.

[9] Wong, Nicholas, et al. "Artificial immune systems for the detection of credit card fraud: an architecture, prototype and preliminary results." Information Systems Journal 22.1 (2012): 53-76.

[10] Brabazon, Anthony, et al. "Identifying online credit card fraud using artificial immune systems." Evolutionary Computation (CEC), 2010 IEEE Congress on. IEEE, 2010.

[11] Seeja, K. R., and Masoumeh Zareapoor. "FraudMiner: a novel credit card fraud detection model based on frequent itemset mining." The Scientific World Journal 2014 (2014).

[12] LeCun, Yann, Yoshua Bengio, and Geoffrey Hinton. "Deep learning." Nature 521.7553 (2015): 436-444.

[13] Deng, Li, and Dong Yu. "Deep learning: methods and applications." Foundations and Trends® in Signal Processing 7.3–4 (2014): 197-387.

[14] Miškuf, Martin, and Iveta Zolotová. "Comparison between multi-class classifiers and deep learning with focus on industry 4.0." Cybernetics & Informatics (K&I), 2016. IEEE, 2016.

[15] Arora, Anisha, et al. "Deep Learning with H2O." H2O. ai (2015).

[16] UCSD: University of California, San Diego DaMining Contest 2009 https://www.cs.purdue.edu/commugrate/data/credit_card/

[17] UCSD: University of California, San Diego Data Mining Contest https://www.cs.purdue.edu/commugrate/data/credit_card/