An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning

Conference Paper · October 2018

DOI: 10.1145/3289402.3289530

3 authors:

Youness Abakarim
École normale supérieure de Casablanca, Morocco, Casablanca
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Mohamed Lahby
Université Hassan II de Casablanca
34 PUBLICATIONS **394** CITATIONS
SEE PROFILE

Abdelbaki Attioui
ENS- Université Hassan II de Casablanca Morocco
13 PUBLICATIONS **11** CITATIONS
SEE PROFILE

An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning

Youness Abakarim, Mohamed Lahby, Abdelbaki Attioui
Laboratory of Mathematics and Applications, University Hassan II of Casablanca, Ecole Normale Superieure (ENS)
Casablanca, Morocco
y.abakarim@gmail.com,mlahby@gmail.com,abdelbaki.attioui@gmail.com

ABSTRACT

In the last decades Machine Learning achieved notable results in various areas of data processing and classification, which made the creation of real-time interactive and intelligent systems possible. The accuracy and precision of those systems depends not only on the correctness of the data, logically and chronologically, but also on the time the feed-backs are produced. This paper focuses on one of these systems which is a fraud detection system. In order to have a more accurate and precise fraud detection system, banks and financial institutions are investing more and more today in perfecting the algorithms and data analysis technologies used to identify and combat fraud. Therefore, many solutions and algorithms using machine learning have been proposed in literature to deal with this issue. However, comparison studies exploring Deep learning paradigms are scarce, and to our knowledge, the proposed works don't consider the importance of a Real-time approach for this type of problems. Thus, to cope with this problem we propose a live credit card fraud detection system based on a deep neural network technology. Our proposed model is based on an auto-encoder and it permits to classify, in real-time, credit card transactions as legitimate or fraudulent. To test the effectiveness of our model, four different binary classification models are used as a comparison. The Benchmark shows promising results for our proposed model than existing solutions in terms of accuracy, recall and precision.

KEYWORDS

Deep Learning, Real-Time Data, Binary Classification, Fraud Detection.

ACM Reference Format:
Youness Abakarim, Mohamed Lahby, Abdelbaki Attioui. 2018. An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning. In *Proceedings of October 2018 (SITA'18).* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

In the recent years the number of bank transactions via credit cards raised drastically and with it the number of frauds and card theft. The 2018 Association for Financial Professionals Payments Fraud Survey, underwritten by J.P. Morgan [1], reported a new increase in payments fraud. An unprecedented record of 78 percent of all organizations experimented payments fraud last year, a total of 700 treasury and finance professionals according to the survey. With the rise of digital payment, finance institutions has lost billions due to credit card fraud [2]. Due to this issue banks and financial institutions are faced with the challenge to build effective and proactive fraud detection systems. Machine learning represents a promising solution to deal with this problem, and this by using the gathered historical customers data and their real-time transaction details [3].

In banking and financial sectors, machine learning is used actively today for different applications, notably in portfolio management, trading, risk analysis, prevention and fraud detection . In the financial landscape, for example, Machine Learning is used to build Chatbots, an artificial intelligence software that can interact with the customers and respond to there queries. In trading, Decision Trading Support Systems or Algorithmic Trading, is used to make extremely fast decisions [4]. Moreover, one of the primary use of machine learning in the banking industry is the protection against fraud. With the help of ML algorithms, detecting suspicious activities became and easier task. Based on the transactions history, machine learning showed promising new methods to analyze the behavior of users and detect if there is a fraud or not [12] [14] [15]. In this work, we are aiming our attention on one aspects of the latter : Credit Fraud detection.

In a McKinsey article published in 2017 [5] Deep Learning is presented as a very promising solution to deal with fraud in financial transactions, making to best use of banks big-data. Deep learning is a generic term that refers to machine learning using deep multilayer artificial neural network (ANN). It is a biologically inspired model of human neurons; composed of multilevel hidden layers of nonlinear processing units, where each neuron is able to send data to a connected neuron within hidden layers [7]. Deep neural networks attracted much attention in the field of machine learning. It's currently providing the best precision and accuracy to many problems; providing promising results in many field, notably in binary classification.

In a data analysis view, Fraud detection is a binary classification problem, the transactions data is analyzed and classified in "legitimate" or "fraudulent". Binary classification is a simple case of classification, where a collection of data is classified into two classes, based on some features. It is mainly used in situation where we want to predict a specific outcome, that can only take two distinct values. Some typical examples include medical diagnosis, spam detection, or in our case : fraud detection. Although fairly simple, binary classification is a very basic problem. There are numerous paradigms used for learning binary classifiers, such as: Decision Trees, Neural Networks, Bayesian Classification, Support Vector Machines, Logistic regression, K-nearest neighborhood, ect. [8]

In the other hand, Real-time data processing has become an important field of research. We speak of Real-time data when the information is delivered directly after it has been gathered, making

SITA'18, Rabat, Morocco,
2018. ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

the data accuracy time dependent. A Real-time system has been described by John A. Stankovic(1988) as : " One which controls an environment by receiving data, processing them, and returning the results sufficiently quick to affect the environment at that time" [11]. The novelty of our work, is the Real-time approach to credit card fraud detection, using state of the art machine learning technology. By using Deep neural network based on an auto-encoder, our model classifies live feed of consumer transactions, and gives a real-time decision - are they legitimate or fraudulent.

To test the effectiveness of our model, different binary classification models are used for benchmark. Although the criteria used by banks, differs for one institution to another, the use of linear models is well known in the banking sector [17]. Therefor, in the present work, we have selected logistic regression as a comparison, as well as linear SVM regression. Support vector machines (SVM) were introduced for the first time by Vapnik [6], as a state-of-the art technique to solve binary classification problems. SVMs have drawn a lot of attention in recent studies due to their major performance as classifiers. However, in some cases using non linear regression ANN has given good results in comparison with other linear models [18]. Hence, we have also selected a non linear artificial neural network algorithms as a benchmark. As for the data sample, in this exercise we have used, the publicly available, European cards transaction of September 2012.

This paper presents two key point. First, a real-time deep learning approach to the credit card fraud detection problem, based on an auto-encoders. Second, a comparison of different binary classification methods applied to this financial problem. We observe that our model based on deep machine learning with auto-encoder gives promising results on this binary classification problem.

The rest of the paper is organized as follows: In Section 2 we give a short review our problem's related works. In section 3, we describe the architecture of our deep neural network prediction model. In section 4, we give a description of our testing environment, then we show and analyze the test results. Finally, in section 5 we draw some conclusions and indicate the future works.

2 RELATED WORK

Over the past few years, many solution have been proposed to cope with the problem of credit card fraud. The major approaches are either statistical (a survey of Boltan and Hand in 2002 [9]) or based on artificial intelligence [10]. Various paradigms have been used, some notable examples are : Regression models, Support Vector Machines, Restricted Boltzmann Machines, Artificial Neural network, ect.

Statistical models are increasingly applied to financial data mining task, including logistic regression, regression analysis, multiple discriminant analysis, and Probit method, ect [23]. In the literature Logistic regression is widely used for binary classification problems [24]. In [15] the author compared various traditional model for fraud detection, Logistic regression is found to be the most accurate of the traditional methods. SVMs have drawn a lot of attention in recent studies due to its major performance as a classifier. Unlike ANNs which minimize empirical risk, SVMs are based on structural risk minimization. They use a nonlinear mapping to transform the input data into a multidimensional feature space. In recent years there have been many researchers around the use of SVMs in binary classification problems, in particular for image classification problems [25], and in the financial related problems [26]. In [27], compared SVM with various other paradigms in solving credit card fraud, the authors focused on creating new inputs by aggregating common transactional variables.

Artificial neural network (ANN) is a computing system that consists of networks interconnected elementary computing units, designed to imitate the functioning of neurons in the human brain. Ghosh and Reilly [16] used data from a credit card issuer, one of the neural network based fraud detection system was trained on a large sample of labeled credit card account transactions and tested on a holdout data set that consisted of all account activity over a subsequent two-month period of time. The method gave good results with high fraud account detection with fewer false positives by a factor of 20 compared with traditional methods. Cardwatch [19] developed in 1997 is a data mining system based on an artificial neural network, trained with historical data of customers. By processing the transaction of a specific customer it detect possible anomalies. Dorrronso et al. [20] presented an online system for fraud detection of credit card operations based on a neural classifier. The system was installed in a transactional hub and relies on the information of the operation and its previous history. A nonlinear version of Fisher's discriminant analysis was used to overcome imbalance of the rate of normal and fraudulent operations. In 2014 [21] the authors proposed a credit card fraud detection model using frequent item set mining. in [22] the authors used a feed forward ANN for detecting fraudulent transactions, the method is found to be effective.

Recently, and with the hype surrounding deep learning, some works have shown that deep neural network, such as recurrent neural networks, have promising results in this field. However, since deep learning is a new approach in machine learning, the use and analysis of various deep learning paradigms remains scarcely explored. In [29] the authors used a convolutional neural network, a feed forward neural network inspired form the animal visual cortex, to classify a set of card transaction in being fraudulent or not. In [30] the authors used a Hidden Markov Model in a eCommerce fraud detection model, the method is found to detect 80% of fraudulent transaction. In [31] the authors found that deep learning method based on auto-encoder performed better than gradient boosted trees for fraud detection. However, the proposed works don't consider the importance of a Real-time approach for this type of problems, and to our knowledge, comparison studies exploring Deep learning paradigms are scarce. To cope with this situation we introduce a live binary classification method based on a deep learning auto-encoder. In the second contribution, we propose an exhaustive comparison with some typical binary classification algorithms. Our motivation about the benchmark algorithms is shown in Tab. 3.

3 OUR REAL-TIME CLASSIFICATION APPROACH

3.1 Prediction Model

As a first approach we propose a classification method based on two stages: a periodical offline training of the historical data, by which we build our machine learning models. This stage first consists of a

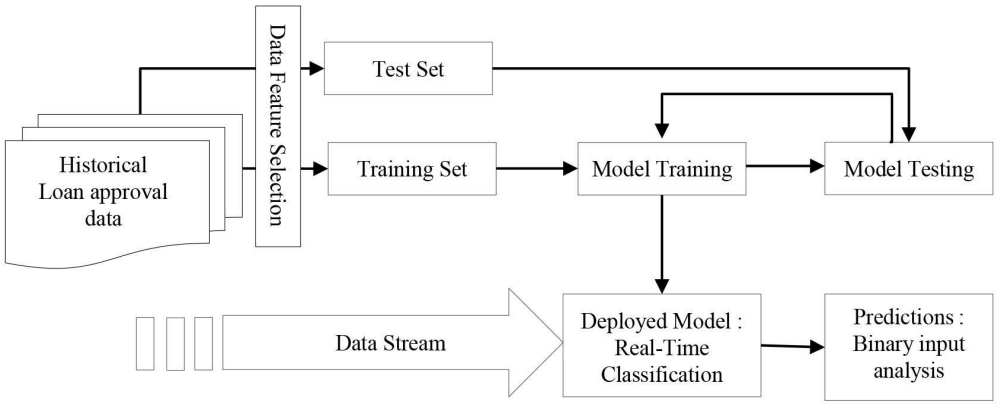


Figure 1: Architecture of the Real-Time classification model

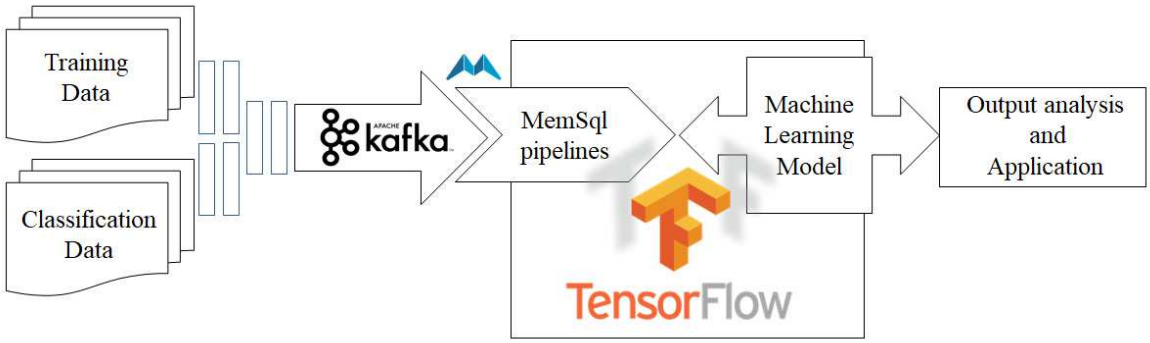


Figure 2: Implementation model of the live data classification technologies used.

feature engineering process, to transform the transaction data into features and labels for our machine learning classification. The data is then split into test and training sets. Afterward, Our models are build with the training features and labels. We test the models with the test features to get our first predictions and then compare the test prediction with our test labels. The process is redone multiple times until we are satisfied with the models accuracy. In the second stage the models are used for prediction on a live stream of new data. Fig. 1 shows the methodology followed to produce the results.

To build the mentioned model we used the following technologies :

- Tensorflow : For building our machine learning model
- Kafka : For building our RealTime streaming data pipeline.
- Memsql : For data pipelines.

Fig. 2 shows how the different technologies are implemented to build our live classification model.

For experiments, implementation and analysis we are using the following environment: Python 3.5, Keras over Tensorflow Backend, GPU GTX 660, Memory 8 GB.

TensorFlow is an open-source software library for machine learning across a range of tasks [34]. In our study, we used it's symbolic math library. Tensorflow is the main used here for building and training our ML algorithms.

Keras is an open source neural network library written in Python [36]. Due of it's capability to run over Tensorflow, it's a good choice in our study.

Kafka is an Apache distributed streaming platform. It is used to build real-time streaming application that react and transforms the streams of Data. In our study, Kafka is used for building the real-time streaming data pipes lines.

Memsql is a distributed SQL data base. We have chosen this distribution for it's wide use with Apache Kafka, and the amount of documentation available on its implementation.

3.2 Deep Auto-Encoder

For deep Learning we use an Auto-Encoder. Auto-Encoders are neural networks with an equal input and output. There architecture is basically a two stacked Restricted Boltzmann Machines parallel to each other, see Fig. 3. An auto encoder consists on two part, the encoder and the decoder :

- Encoder : compressing of the input into a fewer number of bits. The part of the network with fewer bit is called

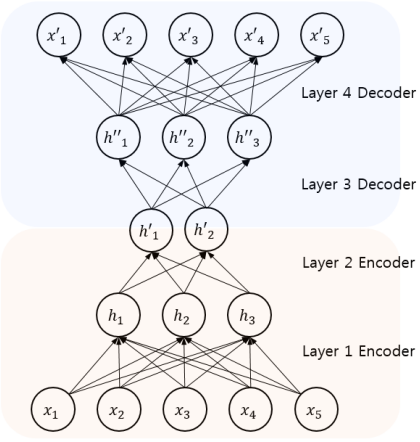


Figure 3: Auto-encoder

bottleneck or the "maximum point of compression" since at this point the input is compressed the maximum. These compressed bits that represent the original input are together called an "encoding" of the input.

- Decoder : here the input is reconstructed using the encoding of the input. A successful encoding is when the decoder is able to reconstruct the input exactly as it was fed to the encoder.

In this work we use an hyperbolic tangent function "tanh" for the encoding and decoding of the input to the output. The equations are as follows :

Encoder

$$h(x) = tanh(W_x) \quad (1)$$

Decoder

$$\hat{a} = tanh(W * h(x)) \quad (2)$$

The error reconstruction is done by back-propagation; the error signal is computed and propagated backward in the network. The errors form desired and actual output values is used as condition. Parameter gradients is used for the back-propagation realization.

3.3 Deep Neural network

For our Auto encoder deep neural network we used 3 encoders and 3 decoders for a total of 6 hidden layers. The composition of the neural network is shown in Fig. 4. Due to the high metrics of the "Tanh" activation function, it has been used in every hidden layer for the Auto-encoder neural network.

4 EXPERIMENTAL RESULTS

4.1 Dataset

The Data-set used in this work contains the transactions made in two days by European cards in September 2012, gathered and analyzed during a research collaboration of Worldline and the Machine Learning Group of ULB on big data mining and fraud detection. It is freely available on Kaggle. See Tab. 1.

The data contains only numerical values. Due to confidentiality the values where changed by PCA transformation. The features

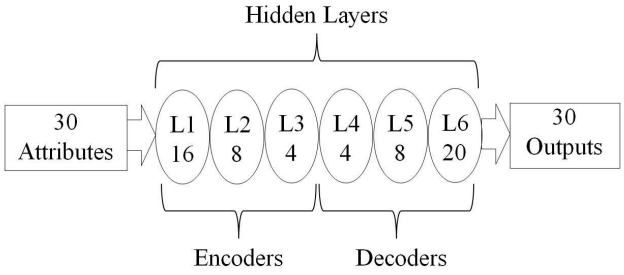


Figure 4: Neural network design: Each hidden layer is noted by L1, L2... followed by the number of neurons in each layers

Table 1: Dataset features

Data set Characteristics	Multivariate
Attribute characteristics	Categorical, Integer
Associated Task	Classification
Number of instances	284807
Number of Attributes	30
Missing Values	N/A

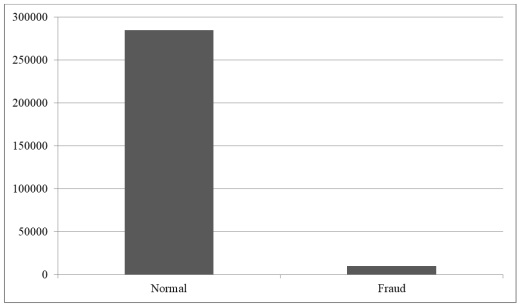


Figure 5: Data set distribution Over-Sampled, the fraud class counts for 3,1% of all transactions

Time and Amount have not been transformed and all the other features are represented by V0, V1, … V26 values. See Tab. 2.

4.2 Performance metrics

This Data-set classifies transactions by being fraudulent or not. We have 492 frauds out of 284807, which is highly unbalanced 0.173%. To solve this class unbalance, Random over-Sampling is used. Fig. reffig:datasetOverSampling shows the distribution of the Data-set After Over-Sampling .

The Dataset is spliced into training and test sets. For a Pre-trained model performance check, we split the data into two separate training sets and one independent test set for final model comparison. See Tab. 4.

4.3 Paradigms

In order to measure the efficiency of deep learning in this case of study, three learning classification methods were chosen for

Table 2: Dataset attributes

Variable name	Description	Type
V0, V1, ..., V26	Transaction features after PCA transformation	Integer
Time	Seconds elapsed between each and the first transaction	Integer
Amount	Amount of transaction	Integer
Class	Non fraudulent or fraudulent	0 or 1

Table 3: Comparison Algorithms

Support Vector Machine	Linear SVM Regression	SVM has been proven to surpasses traditional neural network models for solving complex non-linear problem, whch makes SVM a good choice for solving the complex changeable data structure problems such as fraud detection [32] [33].
Regression	Logistic Regression	As mentioned in section 2, in [15] the author used logistic regression to perform various credit card fraud experiments, the latter is found to have promising results in comparison of the traditional methods
Classical ANN	Non Linear Auto regression NN	Using non linear regression ANN has given good results in comparison with other linear models [18]
Deep Learning	Deep Neural network (DNN) with auto encoders	Beside being data-specific, Auto-encoders don't need explicit labels to train on, the labels are self generated withing the model. Due to the diversity of the fraudulent transaction, we believe that auto-encoders could be the most fitted for this task.

Table 4: Instances distribution

Number of Instances	284807
Split ratio for Pre-training	0.2
Split ratio for Training	0.4
Independent test set	0.4

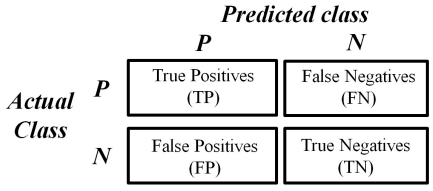


Figure 6: confusion matrix illustration

comparison, totaling 4 typical algorithms. The methods used for comparison were chosen by their redundancy in various binary classification research papers and their known good results. See Tab. 3 for more details.

For the metrics we used a combination of the confusion matrix and a column chart, as well as the precision and recall. A confusion matrix of a binary classifier is a table that shows the number of instances classified correctly/incorrectly in each class. Fig. 6 illustrates the confusion matrix of a binary classifier.

In our case, positive represents the fraudulent transactions and negative represents the legitimate ones. True positive (TP) represents the fraudulent transactions classified as fraud. True negative (TN) represents legitimate transactions classified as legitimate. False positive (FP) represents the misclassified legitimate transactions as fraud. False negative (FN) represents the misclassified fraudulent transactions as legitimate.

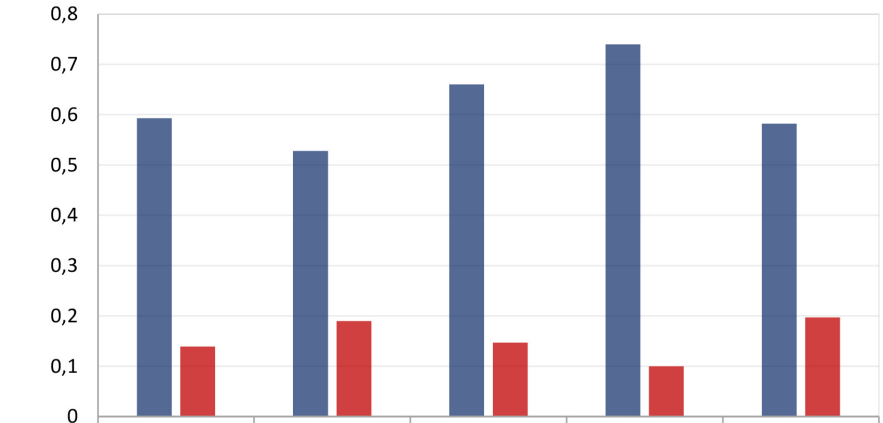
The precision is the measure of the exactness of the model, it is the accuracy on transaction predicted as fraud defined as the number of positive predictions divided by the total number of positive class predicted by the model, as follow:

$$Precision = TP/TP + FP. \tag{3}$$

The recall is the measure of the completeness of the model, it is the accuracy on fraud transactions defined as the number of positive predictions divided by the number of positive class values of the test data, as follow:

$$Recall = TP/TP + FN. \tag{4}$$

We use F1 score to convey the balance between precision and the recall defined as follow:



	Linear SVM Regression	Logistic Regression	NN Based Classification	Non Linear Auto Regression	Deep NN Auto-Encoder
Recall	0,593	0,528	0,660	0,740	0,582
Precison	0,139	0,190	0,147	0,100	0,197

Figure 7: Results metrics comparison

$$F1Score = 2((precision * recall)/(precision + recall)). \quad (5)$$

4.4 Results analysis

In card fraud detection systems, when a transaction raise a fraud flag, the transaction is refused, and the user must go through a verification process to verify if it's the case of a false flag or a real fraud. This verification processes vary from a phone call to a series of verification forms. The cost of a false flag is then equivalent to the cost of these processes, which is significantly lower than the cost of a fraud case. However, when the number of false flags is important, purchases get blocked more frequently by error, making one's use of a credit card tedious and time consuming, moreover it can generate big loses for either sides of the transaction. thus, our model should have a balanced mount of fraudulent transactions caught and false flags raised.

Tab. 5 shows the experimental results of our implemented algorithms. Each algorithm was tested four times and for each algorithm we created a confusion matrix, and represented the TP FN FP TN in the table. The non linear auto regression has caught the most amount of the fraudulent transactions, but at cost of the false flags. Logistic regression raised the least amount of false flags but is not the best at catching the fraudulent transactions. Deep Learning based on the auto encoder has balanced results, with a good amount of frauds caught and a fair amount of false flags. First results seems promising for the Deep neural network model. Let's see the accuracy of our models. Fig. 8 shows the accuracy of each algorithm.

The accuracy is defined as correct predictions made divided by the total number of predictions made. The data shows that Logistic regression followed by the Auto-encoder have the best accuracy and the typical neural network classification method has the worst. Because our data is not well balanced, we shouldn't draw conclusions from accuracy only. Accuracy can be misleading due to its dependencies (accuracy paradox[35]). Therefor, Recall and precision are shown in Fig. 7.

Table 5: Confusion Matrix results

	TP	FP	TN	FN
Linear SVM Regression	341	2111	115173	234
Logistic Regression	302	1290	116002	270
NN Based Classification	384	2229	115049	198
Non Linear Auto Regression	430	3871	113408	151
Deep NN Auto encoders	358	1457	115793	257

The results, in Fig. 7, show that in our model Non linear auto regression has the best Recall, but at the cost of precision. Deep NN auto encoder, in the other hand, has the best precision, with results close to logistic regression. We can't draw conclusion from recall an precision only, our model should have a well balanced values between the two metrics. Let's see the F1 scores Tab. 6. In this case of study, Deep NN Auto encoder has the overall best F1 score followed by logistic Regression, which confirms that Deep NN auto-encoder is the best fitted algorithm amongst the tested ones. Moreover, the deep learning algorithm used in this study is very simple; with more tuning of the parameter (Hyper-parameter Tuning with Grid Search) we may have better results. This provides good insight in which algorithm should be chosen in building our prediction model, and we choose Deep Neural network with auto-encoder.

5 CONCLUSION

In this paper we proposed a Real-time model for credit card fraud detection, for a real-life data set of Credit Card transactions, using Deep Learning. After the tests and the comparison study, on the performance of some typical real-time binary classifiers versus

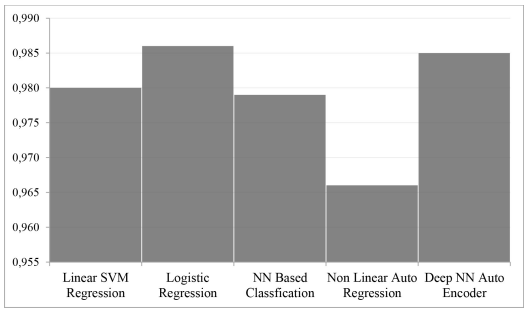


Figure 8: Accuracy of each algorithm

Table 6: F1 scores results

Classifier	F1 score
Linear SVM Regression	0,225
Logistic Regression	0,279
NN Based Classification	0,240
Non Linear Auto Regression	0,176
Deep NN Auto encoders	0,294

Deep Neural Network with Auto-encoder, the benchmark experiments show that Deep NN Auto encoder has very promising results, with the best F1 score. The experiment confirms that although the well known performance of logistic regression Deep learning out performs it. Therefore, future studies will focus mainly on state of the art deep learning paradigms for this type of Real-time Data Classification problems. The proposed Framework can be used by Credit Card Providers To monitor any unusual behavior and to detect possible fraud attempts.

REFERENCES

[1] J.P.Morgan. "Payments Fraud and Control Survey", PNC Financial Services Group, 2018.
[2] Boston Consulting Group. (2017). Global Payments 2017 – Deepening The Customer Relationship.
[3] Bose, Indranil, and Radha K. Mahapatra. "Business data mining—a machine learning perspective." Information and management 39.3 (2001): 211-225.
[4] TUNG, Hui-Hsuan, CHENG, Chiao-Chun, CHEN, Yu-Ying, et al. Binary Classification and Data Analysis for Modeling Calendar Anomalies in Financial Markets. In : Cloud Computing and Big Data (CCBD), 2016 7th International Conference on. IEEE, (2016). p. 116-121.
[5] Jacomo Corbo, Carlo Giovine, and Chris Wigley(2017, April). Applying analytics in financial institutions fight against fraud. McKinsey Analytics. Retrieved from https://www.mckinsey.com.
[6] Vapnik, V.: Statistical learning theory. Wiley, New York.(1998)
[7] I. Goodfellow, Y. Bengio, A. Courville.: Deep learning, Cambridge, Massachusetts, The MIT Press, (2016)
[8] Phyu, Thair Nu. "Survey of classification techniques in data mining." Proceedings of the International MultiConference of Engineers and Computer Scientists. Vol. 1. (2009).
[9] Bolton, Richard J., and David J. Hand. "Statistical fraud detection: A review." Statistical science (2002): 235-249.
[10] Zhou, Xun, et al. "A state of the art survey of data mining-based fraud detection and credit scoring." MATEC Web of Conferences. Vol. 189. EDP Sciences, 2018.
[11] John A. Stankovic. :Misconceptions about real-time computing. IEEE Computer, 21(10), 10-19 (1988).
[12] S. Benson Edwin Raj, A. Annie Portia.: Analysis on Credit Card Fraud Detection Methods. In: International Conference on Computer, Communication and Electrical Technology – ICCCET2011, 18th & 19th March, (2011)
[13] Martin, James.: Programming Real-time Computer Systems. Englewood Cliffs, NJ: Prentice-Hall Inc. p. 4. ISBN 0-13-730507-9.)(1965)
[14] Masoumeh Zareapoor, Seeja.K.R, and M.Afshar.Alam.: Analysis of Credit Card Fraud Detection Techniques: based on Certain Design Criteria. In: International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, August (2012)
[15] Bhattacharyya, Siddhartha, et al. "Data mining for credit card fraud: A comparative study." Decision Support Systems 50.3 (2011).
[16] Ghosh, Sushmito, and Douglas L. Reilly. "Credit card fraud detection with a neural-network." System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on. Vol. 3. IEEE, (1994).
[17] Bakar, Nor Mazlina Abu, and Izah Mohd Tahir. "Applying multiple linear regression and neural network to predict bank performance." International Business Research 2.4 (2009): 176.
[18] Landi, Alberto, et al. "Artificial neural networks for nonlinear regression and classification." Intelligent Systems Design and Applications (ISDA), 2010 10th International Conference on. IEEE, (2010).
[19] Aleskerov, Emin, Bernd Freisleben, and Bharat Rao : Cardwatch: A neural network based database mining system for credit card fraud detection. Computational Intelligence for Financial Engineering (CIFEr), 1997., Proceedings of the IEEE/IAFE 1997. IEEE, 1997.
[20] Dorronsoro, Jose R., et al. : Neural fraud detection in credit card operations. IEEE transactions on neural networks 8.4 (1997)
[21] 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).
[22] Hassibi, Khosrow. "Detecting payment card fraud with neural networks." World Scientific Book Chapters (2000): 141-157.
[23] ALTMAN, Edward I., MARCO, Giancarlo, et VARETTO, Franco.: Corporate distress diagnosis: Comparisons using linear discriminant analysis and neural networks (the Italian experience). Journal of banking & finance, vol. 18, no 3, p. 505-529.(1994)
[24] D.W. Hosmer, S. Lemeshow : Applied Logistic Regression, 2nd Ed, Wiley-Interscience, (2000)
[25] GOH, King-Shy, CHANG, Edward, et CHENG, Kwang-Ting.: SVM binary classifier ensembles for image classification. In : Proceedings of the tenth international conference on Information and knowledge management. ACM. p. 395-402.(2001)
[26] Shin, K.-S., Lee, T. S., & Kim, H.-J.: An application of support vector machines in bankruptcy prediction model. Expert Systems With Applications, 28(1), 127–135.(2005)
[27] Whitrow, Christopher, et al. "Transaction aggregation as a strategy for credit card fraud detection." Data Mining and Knowledge Discovery 18.1 (2009): 30-55.
[28] Y. Bengio.: Learning deep architectures for ai, Found. Trends Mach. Learn., vol. 2, no. 1, pp. 1–127, Jan. (2009)
[29] FU, Kang, CHENG, Dawei, TU, Yi, et al.: Credit Card Fraud Detection Using Convolutional Neural Networks. In : International Conference on Neural Information Processing. Springer International Publishing. p. 483-490. (2016)
[30] Srivastava, Abhinav, et al. "Credit card fraud detection using hidden Markov model." IEEE Transactions on dependable and secure computing 5.1 (2008): 37-48.
[31] Rushin, Gabriel, et al. "Horse race analysis in credit card fraud—deep learning, logistic regression, and Gradient Boosted Tree." Systems and Information Engineering Design Symposium (SIEDS), 2017. IEEE, (2017)
[32] Patel, S., and S. Gond. "Supervised Machine (SVM) learning for credit card fraud detection." International Journal of Engineering Trends and Technology (2014).
[33] Mareeswari, V., and G. Gunasekaran. "Prevention of credit card fraud detection based on HSVM." Information Communication and Embedded Systems (ICICES), 2016 International Conference on. IEEE, (2016).
[34] Abadi, Martín, et al. "Tensorflow: a system for large-scale machine learning." OSDI. Vol. 16. (2016).
[35] A. Ng.: CS 229 machine learning course materials, Stanford University, (2016)
[36] F. Chollet.: Keras: deep Learning library for Theano and TensorFlow, Github, https://github.com/fchollet/keras (2015)
[37] Jason Brownlee, Machine Learning Mastery with python (2016)
[38] John, S. N., et al. : Realtime Fraud Detection in the Banking Sector Using Data Mining Techniques/Algorithm. Computational Science and Computational Intelligence (CSCI), (2016)