Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 3): pp. 4149-4155
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.03.428

Deep Learning-Based Real-Time Credit Card Fraud Warning System

Vijay Singh Department of Computer Science & Engineering, Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002 vijaysingh.cse@geu.ac.in

Poonam Verma Department of Computer Application Graphic Era Hill University, Dehradun, Uttarakhand India, 248002 pverma@gehu.ac.in

ABSTRACT

There have been significant advancements in machine learning over the past couple decades, paving the way for the creation of the use and intelligent systems with enhanced data processing and categorization capabilities. Data validity (both logically and temporally) and timely feedback generation are essential to the systems' accuracy and precision. This study will focus on one such system a fraud detection system to better understand its inner workings. Investment in the study and creation of algorithmic and data analysis tools for use in detecting and preventing financial institution fraud is increasing. To solve this issue, numerous machine learning-based methods and algorithms have been presented. However, studies comparing Deep learning paradigms are scarce, and to the aimed to contribute, the works presented here fail to recognise the importance of a Real-time approach to problems of this kind. As a solution, we propose utilising deep neural network system to enhance a real-time fraud detection for credit cards approach. Our suggested model's auto-encoder base permits rapid verification or denial of credit card payments. We tested our model by contrasting it to four similar common forms of binary classifier models. Our proposed model outperforms the state-of-the-art solutions on the Benchmark dataset

I. INTRODUCTION

Credit card use for banking transactions and the associated risk of fraud and theft have both increased dramatically in recent years. J.P. Morgan funded the 2018 Association for Finance Professionals Payments Fraud Survey, which found an uptick in payments fraud. 78% of businesses, or almost 700 treasury and financial experts, reported experiencing payments fraud in 2016, an all-time high. Financial organizations have lost billions owing to fraud involving credit cards as digital payment methods have become more popular. Financial institutions therefore need to implement strategies for rapid and accurate fraud detection. Machine learning is a promising solution to this problem since it can use both previous client data and real-time transaction details.

Machine learning is now widely used in the banking and financial industry for tasks. Bots, artificial intelligence programmes used in the financial industry to engage with and answer inquiries from customers, are the product of machine learning. Algorithmic trading, also known as a decision trading support system, enables traders to make instantaneous choices. Additionally, machine learning is mostly utilized in the banking business for the purpose of fraud prevention. It was previously difficult to spot suspicious behaviour, but with the aid of Ml techniques, this work became much simpler. Machine learning demonstrated useful new techniques for analysing user behaviour and determining the presence or absence of fraudulent activity in past transactions. The latter is what we'll be focusing on here, specifically the detection of credit fraud.

Some academics have proposed using Deep Learning to optimise the use of banks' vast data in order to reduce financial transaction fraud. Deep learning is a catchall term for machine learning techniques that employ deep multilayered artificial neural networks. (ANN). It's a representation of human neurons based on biological principles, with the ability of each neuron to share information with other connected neurons in a hidden layer. Deep neural networks received a lot of interest in the field of machine learning. It is currently the standard for handling a wide variety of problems and has proven effective in a number of domains, including binary classification.

From the perspective of data analysis, determining whether or not a transaction is fraudulent boils down to two possible outcomes: either it is valid or it is fraudulent. The simplest form of classification is binary classification, in which a set of data is divided into two categories according to the features that have been assigned to them. Predicting outcomes that can only take one of two possible forms is where it shines. Examples include conventional medical diagnosis, spam filtering, and the identification of fraud in this context. Binary classification is a fundamental issue, despite its seeming simplicity. Binary classifiers can be learned using a wide variety of approaches.

Meanwhile, studies of real-time data processing have become increasingly important. That which "tries to regulate an atmosphere by gathering data, analysing it, and delivering it back the findings appropriately quick to impact the surrounds at that time" is what is meant by "real-time data," and it is delivered almost instantly when it has been gathered. Our ground-breaking contribution is a state-of-the-art machine learning-based approach to real-time credit card fraud detection. To identify whether a particular stream of customer transactions represents legitimate activity or fraud, our model employs a deep neural network built on auto-encoder data.

Two fundamental arguments are made in this study. To start, we apply an auto-encoder-based deep learning method to the detection of credit card fraud issue in real time. Second, a look at how several binary classification approaches to this monetary issue stack up against one another. Our deep machine learning with auto-encoder-based model performs well on this binary classification task, as we observe.

II. LITERATURE SUIRVEY

Credit card fraud has been an issue for many years, and several solutions have been presented to deal with it. The two most common methods are statistical (see Boltan and Hand's 2002 survey [1]) and AI-based. Many other approaches have been taken, including Linear regression, Support Vector Machines, Boltzman Machines, Artificial Neural Networks etc.

Regression analysis, regression analysis, discriminant function analysis, the Probit technique, and many more are just some of the statistical models that are being used in financial data mining at an increasing rate [2]. As stated in [3], logistic regression is commonly employed in the literature when dealing with difficulties of binary classification. In [4], the author evaluates several classic models for spotting fraud and concludes that logistic regression provides the best results. Thanks to their outstanding effectiveness as a classifier, SVMs have garnered a great deal of interest from recent research. SVMs are founded on the principle of structural risk minimization, as opposed to the empirical risk minimization that ANNs use. Data is mapped non-linearly to a set of features for analysis. This past few years

SVMs have been the subject of extensive study for their application in binary classification issues, especially in the realm of image classification [5] and in the realm of finance [6]. In [27], the authors contrasted SVM with alternative paradigms for combating credit card fraud, with a primary emphasis on developing novel inputs by fusing together variables that are utilised repeatedly in financial transactions.

In order to mimic the method in which human neurons process data, scientists have developed a sort of networked computer system known as an artificial neural networks (ANN). One of the neural network-based detection mechanisms developed by Ghosh and Reilly [7] used dataset supplied by a credit card provider to train on a representative cohort of labelled credit card transactions and then test on all financial accounts from the subsequent two months. The technique was successful, leading to a 20-fold decrease in false positives and a noticeable increase in the identification of fraudulent accounts.

Data mining utilising artificial neural networks pre-trained using customer records was pioneered in 1997 with the creation of [8]. To achieve this, it examines the customer's recent transactions in search of anomalies. Dorrronso et al. [9] introduced a neural classifier for identifying instances of online credit card theft. The network relies on an operation's data and logs, and it was built as a centralised centre for business dealings. Nonlinear modification of Fisher's discriminant analysis was used to account for the imbalance in the number of legitimate vs fraudulent transactions.

In [10], the authors suggested a frequent item set mining-based model for detecting credit card fraud. The authors of [11] successfully implemented the use of a feed forward ANN to identify fraudulent financial transactions.

Recent studies have shown the promise of certain kinds of deep learning models, such as recurrent neural networks, amid all the buzz around deep learning. Due to deep learning's infancy within the field of machine learning, it is still difficult to fully grasp the breadth of its potential applications and conduct in-depth assessments of its various paradigms. In [12], recurrent neural networks called convolutional neural networks were used to identify if a set of card purchases were fraudulent. These networks were inspired by the visual cortex of animals.

Using a Hidden Markov Model, a model was developed for identifying online fraud, and it was found that this method could correctly identify 80percent of fraud cases [13]. An auto-encoder-based deep learning strategy outperforms gradient boosted trees for fraud detection, as shown in [14]. However, the recommended works overlook the importance of a Real-time strategy for these problems, and to the greatest of our knowledge, comparison research addressing Machine learning paradigms are scarce. We present a supervised neural auto-encoder-based method for real-time binary classification to solve this problem. Second, we provide a complete contrast to other popular binary classification methods.

III. PROPOSED METHODOLOGY

✓ PREDICTED METHOD

We first propose a two-stage classification method, in which we periodically offline-train our machine learning models using historical data. To begin, we do feature engineering on the transaction data to create characteristics and labels for our machine learning categorization. Separate test and training sets are then created from the data. After that, we use the training features and labels to construct our models. First, predictions are made by the models based on the characteristics of the tests, and then these predictions are compared to the test results. This process is iterated multiple times until the desired level of accuracy is achieved in the model. Second, we use these models to make predictions based on an ongoing stream of new data.

✓ DEEP AUTO ENCODER

In order to achieve deep learning, we employ an Auto-Encoder. Input and output are balanced in Auto-Encoders, a special kind of neural network. As can be seen in Fig. 1, the basic building blocks consist of two parallel, stacked Restricted Boltzmann Machines. The two components that make up an automatic encoder are the transmitter and the decoder.

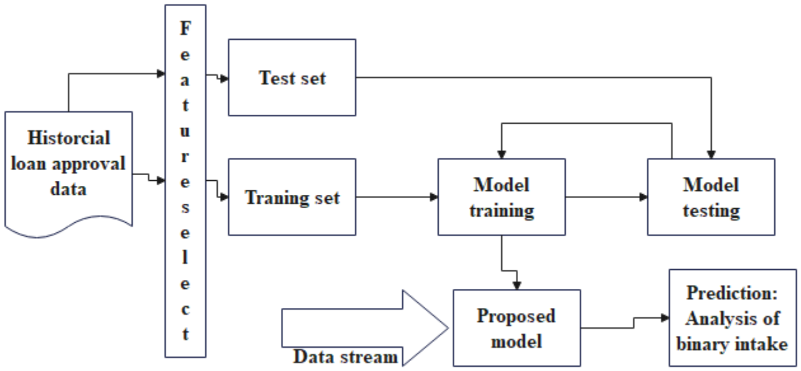

Fig 1: Block diagram of proposed model

Encoders reduce the amount of bits in an input signal. The bottleneck, also known as the peak level of compression or "compression threshold," is the point in the network when the input is reduced to its minimum size. What we have here is a "encoding" of the input, which is just a fancy word for compressed bits representing the original input.

Here, we decode the input to rebuild the original signal. In order for an encoding to be considered successful, the decoder must be able to recreate the input with 100% accuracy.

In this study, we encode and decode data using the hyperbolic tangent function tanh as shown in below equation

$$\text{Encoder} = g(z) = \tanh(W_z)$$

$$\text{Decoder} = \alpha = \tanh\,(W * g(z))$$

By computing the error signal and then sending it backward over the network, back-propagation allows for error reconstruction. The discrepancies between the planned and realised output levels serve as the condition. In order to do backpropagation, parameter gradients are used.We built an Auto encoder deep neural network with 6 hidden layers, consisting of 3 encoders, 3 decoders, and 2 pools. How the neural network is put together. The "Tanh" activation function has been used throughout the Auto-encoder neural network's hidden layers due to its excellent performance metrics.

IV. RESULTS AND ANALYSIS

A card fraud prevention system will automatically cancel a transaction if it suspects fraud. The user next goes through authentication, which verifies their identity and establishes whether or not this is a fake case. These verification procedures can include anything from one phone call to several paper-based forms. As a result, the cost of a fake flag is equivalent to the cost of these processes, which is much less than the cost of a fraud case. However, when the error flag count is high, genuine purchases are more likely to be refused by mistake, which makes using a credit card a tedious, inconvenient, and perhaps dangerous operation. As a result, it is crucial that our model not incorrectly flag too many legal transactions as false positives.

Table 1 displays the results of our deployed algorithms' experimental evaluations as well as their F1 scores. The TP, FN, and FP data are presented in a cnn model and a tabular format after being tested four times and analysed. Most false positives have been found using non linear auto regression, but this has come at the cost of fraudulent purchases. Regression analysis was not the most efficient method for detecting fraudulent money dealings, but it did not produce many false positives either. With Deeper Algorithm related on the auto encoder, a large number of fraudulent accounts are uncovered, but there are also a large number of false alarms. The early outcomes of the model's deep neural network are promising. See how accurate our forecasts really are.

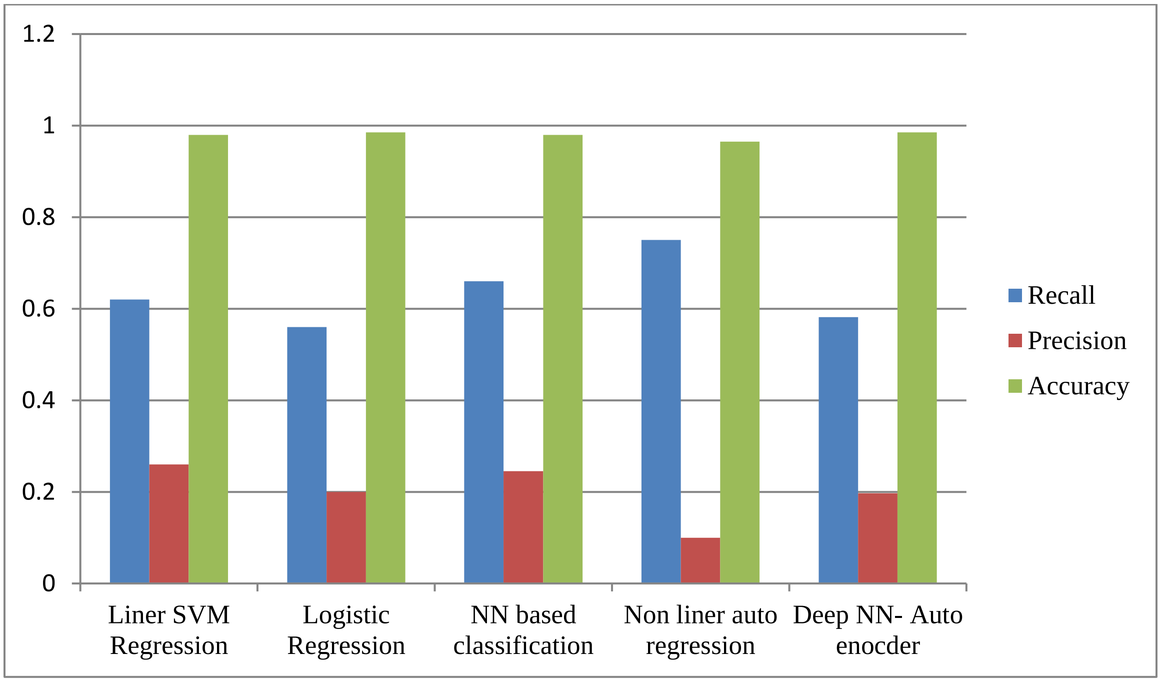

Fig 2: Proposed model vs Existing methods

The percentage of right predictions compared to the overall amount number of forecasts is an accuracy measure. From what we can see, Logistic regression and then Auto-encoder are the most effective methods for classification, while the traditional neural network technique comes in last. The data we have is too skewed for precision to be our sole criterion for drawing conclusions. Accuracy is often misleading because of the many variables that affect it (accuracy paradox). For this reason, Fig. 2 displays a contrast between recall and precision.

Various Classifier	F1 value of models
Deep NN auto encoder	0.226
Linear SVM Regression	0.589
Non linear auto regression	0.238
Logistic regression	0.752
NN Based Classification	0.645

Table 1:F1 score of proposed and existing methods

The results are shown in Figure 2; it turns out that non-linear automatic regression has the found That the top in our models, but at the sacrifice of precision. In comparison, the shallow NN auto encoder's precision is quite close to that of the regression approach. In order to draw any solid inferences from our model's results, we need to ensure that it has respectable values for both precision and recall. Our Deep NN auto-encoder achieved the highest F1 score in this study, following by the regression Models, demonstrating that it was the most appropriately fitted algorithm. Even though basic deep learning techniques were used in this study, more parameter tuning (through Hyper-parameter Tuning using Grid Search) might have yielded better results. In light of this, we decided that a Dnn coupled with an auto-encoder would be the most effective method for creating our prediction model.

V. CONCLUSION

In this study, we provide a real-time model for identifying credit card fraud using deep learning on a dataset comprised of actual credit card transactions. Comparing the results of various conventional real-time binary classifiers, the benchmark studies show that Deep NN Auto encoder achieves superior results, with the highest F1 score. It is commonly known how well logistic regression performs, but this experiment demonstrates that learning can do much better. Accordingly, subsequent studies will centre mostly on state-of-the-art machine learning models for Real-time Data Interpretation difficulties. The proposed Framework can be used by credit card issuers to monitor for and perhaps identify fraudulent operations.