Int. Conf. on Signal, Image Processing Communication & Automation, ICSIPCA

Benefits of SVM and Deep Learning in credit card fraud detection – A Survey

Ms. Sangeetha K N[1], Dr. Veenadevi[2], Dr. Usha B A[3]
[1]Research Scholar, Asst. Prof, Dept of E&C, JSS Academy of Technical Education
[2]Assc Prof, Dept of E&C, RV College of Engineering
[3]Asst. Prof, Dept of CSE, RV College of Engineering
knsangu12@gmail.com, veenadevi@rvce.edu.in, ushaba@rvce.edu.in

***Abstract*—Credit card frauds in the USA have grown at double rates in the recent years. Banks have been extra careful in increasing the credit of the customers, but in spite of the extra care taken by the banks, fraudsters have managed to run away with billions of dollars of cash in recent times. Banks have recently looked into deploying technology, in order to combat the menace. One of the hot topics in the recent times has been machine learning and data mining. Machine learning and data analytics is been deployed in various fields because of its convenience and extra-ordinary accuracy. In this paper, comparison of SVM and deep learning in dealing with the credit card fraud detection problem faced has been proposed.**

***Index Terms*— Credit card, Fraud detection, SVM.**

I. Introduction

In this paper, we are dealing with a very specific problem of fraud namely the credit card fraud. In countries like USA, the credit cash amount which can be drawn by the customer is decided once the customer loyally pays back his previous dues. The fraudsters have exploited the above system. The fraudsters initially draw minimum amount of credit cash available to them. They return the dues promptly. After such a few healthy transactions, the banks increase the credit cash limit available to the fraudsters. The fraudsters taking advantage of this draw the entire cash amount and run away with the huge amount of cash with them.

Such fraudulent activities by the fraudsters have increased steadily in the past few years. Because of such activity, in the US alone banks have lost close to 20 billion dollars in a year. One more area of concern is the growth of such fraudulent activity, such activity have grown in double digits in the last decade. Banks are now turning towards technology to stop this menace.

II. Previous Study

A lot of study and research has gone into the topic of ‘fraud detection and avoidance’. With the rise of machine learning and artificial intelligence, Researchers in tandem have developed a number of predictive and classification models to predict the fraudulent activity. Right from the supervised learning conventional machine learning models to deep learning, a number of models have been developed. There are many review papers describing types of frauds and different fraud techniques.

The earliest paper to explore the data mining based approach towards fraud detection was by Lu Q, Ju C [1].

Grenze ID: 02.ICSIPCA.2017.1.37

In their paper, the duo have done a deep research on the field of fraud detection using data mining based approaches. The duo have mentioned their finding by applying conventional machine learning algorithms to get a pattern, to prevent the future fraudsters from committing the fraud. Their research was limited to credit card fraud. But the results in the study gave way for further deep analysis on the topic.

Bolton RJ, Hands DJ [2] has explored how unsupervised machine learning algorithms can mitigate the problem of credit card fraud. Unsupervised machine learning which has garnered great attention of late because of surprisingly great results, have been suggested by the duo to get the patterns to nab the fraudsters.

Bhattacharya S, Jha S, Tharakunnel K [3] has done a comparative study on data mining approaches to determine the efficiency of the available techniques to combat the fraudsters. The study involved the comparison of various machine learning techniques available for predicting credit card fraud. The study which was a comparison between various different techniques like SVM, logistic regression, neural networks found out that neural networks performed the best in combating the fraud.

Y. Sahin & E. Duman, in [4], demonstrates the advantages of applying the data mining techniques including Decision Trees & Support Vector Machine (SVM) to the credit card fraud detection problem for reducing the banks risk. The results show that the classifiers & other Decision Tree approaches outperform SVM approaches in solving the problem under investigation.

R. Patidar & L. Sharma, in [5], presented fraud detection using Neural Network is totally based on the human brain working principal. Neural Network method has made a computer capable to think. As human brain learns through past experience & use that knowledge or experience to take the decision in daily life problem. The same technique is applied with the credit card fraud detection technology.

G. Singh et al., in [6], presented Support Vector Machines have developed from Statistical Learning Theory of AI domain. It has been widely applied to fields such as character & text recognition, handwriting digit, & more recently to satellite image classification. SVMs & other nonparametric classifiers have a reputation for being effective & reliable. SVMs function by nonlinearly projecting the training transaction dataset in the input space to a feature space of higher dimension by use of a kernel function is used. The results are stored in a separable dataset that can be separated with linear classifier. The process enables the classification of transaction datasets which are usually non- linearly separable in the input set. The functions used to project the data from input set to feature sets are called kernels (kernel machines), examples of which include Gaussian, polynomial & quadratic functions. Each function has alone parameters which have to be checked prior to classification & it also usually calculate through a cross validation process.

Deep learning models which are always data hungry perform the best when it is fed with more and more data. Since deep learning models which learn through experience and data, and a lot of unstructured and structured data is available with the banks, which the deep learning models can harness on. Hence, lately deep learning has been used extensively in data based mining research for fraud detection.

In this paper, comparison of two different techniques used in determining the fraudulent activity of the fraudsters, namely SVM and deep learning are discussed.

III. Support Vector Machine (SVM)

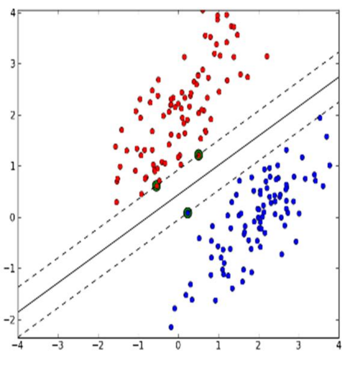

Figure 1: Concept of Support Vector Machine

In machine learning, support vector machines (SVMs, also support vector networks) supervised learning models with associated learning algorithms that analyze data used for classification and regression analysis. Given a set of training examples, each marked as belonging to one or the other of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall as shown in Fig1.

Since, SVM is very good in bi-classification, in the detection of fraudulent activity. It is quite accurate in prediction.

The advantages of SVM are highlighted below:

A. Regularization parameter

The SVM's have a regularization parameter. Regularization parameter is defined asin mathematics and statistics and particularly in the fields of machine learning and inverse problems, is a process of introducing additional information in order to solve an ill-posed problem or to prevent over fitting. Hence while training the models to detect a fraudulent activity; the data scientists need not worry about the phenomena of over fitting which is a major cause of concern for the data scientists.

B. Uses the kernel trick

Because of the use of kernel trick by the SVM, This operation is often computationally cheaper than the explicit computation of the coordinates.

Since the dataset used to train the model make use of huge datasets, the use of kernel trick by the SVM helps us in reducing huge computations, thus saving time.

C. Convex Optimization

Since SVM is defined by convex optimizations, there are efficient techniques to solve the problem. A convex optimization problem is a problem where all of the constraints are convex functions, and the objective is a convex function if minimizing, or a concave function if maximizing.

To solve such problems, efficient techniques like SMO are already available

IV. DEEP LEARNING

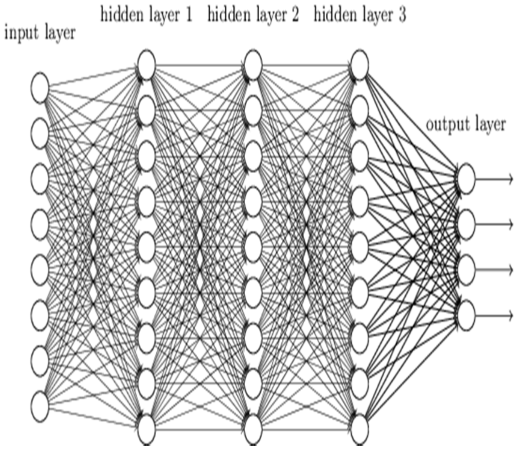

Figure2: Deep learning model (Deep Neural Network)

Deep learning (also known as deep structured learning, hierarchical learning or deep machine learning) is a class of machine learning algorithms that:

- Use a cascade of many layers of non linear processing units for feature extraction and transformation. Each successive layer uses the output from the previous layer as input. The algorithms may be supervised or unsupervised and applications include pattern analysis (unsupervised) and classification (supervised).
- Are based on the (unsupervised) learning of multiple levels of features or representations of the data. Higher level features are derived from lower level features to form a hierarchical representation.
- Are parts of the broader machine learning field of learning representations of data.
- Learn multiple levels of representations that correspond to different levels of abstraction; the levels form a hierarchy of concepts.

The advantages of deep learning in combating the fraudulent activity in the credit cash is given as:

A. Makes use of available infrastructure

With the rise of big data infrastructure such as Hadoop and Apache Spark, huge amounts of data can be easily processed and analyzed in recent times. Deep learning being data hungry feed on such huge amounts of data which can be handled by the available big data infrastructure. Hence deep learning harness the available infrastructure and feed on the huge data available.

B. Learn with examples

The biggest advantage, deep learning models have over the conventional machine learning algorithms is the ability to learn with examples. Hence, the data hungry deep learning models do not repeat the mistakes it did previously. Hence in our case, a bad prediction before in the fraudulent activity is not repeated in the future as, the deep learning models learn with experience and data.

C. Non dependency on statistical equations

Deep learning models unlike other classifiers like logistic regression, SVM do not depend on mathematical statistical equations to classify the data entrants. They learn with data and experience, hence the accuracy in prediction is higher in deep learning models compared to the traditional classifiers.

D. Comparison between SVM and Deep Learning in determining fraudulent activity

For a small data-set, SVM performs relatively compared to deep learning models. This is because; the SVM model depends on mathematical equation for the classification. Hence, the classification does not depend on the data-set when the classification of the data entrants in the test set is being classified.

The SVM also uses the kernel trick in good effect in reducing the huge computations that has to be performed in order to classify the data in the test set. Kernel trick as mentioned earlier in the paper is the trick employed in place of calculation of computationally expensive co-ordinates.

But one of the major disadvantages of using SVM for classification is that this model is a bi-classifier. Hence, the SVM can be used to predict fraud or not. But a middle ground is missing. The classifier gives a benefit of doubt in such a situation which might result in wrong classifications.

Deep learning on the other hand, does not depend on any mathematical statistical equations for the classification. Since the deep learning models learn by data and experience, the deep learning models tend to classify better in presence of huge data sets.

Deep learning data hungry models, is stark in contrast of the SVM which take more time in classification. This is because, the deep learning models unlike the SVM models do not employ kernel trick. But, in the underlying problem, wherein the banks are facing billions of dollars theft due to fraudsters, the efficiency of classification is more critical than the time for classification.

Hence, the deep learning models which learn by data and experience and more time consuming for classification is more suited for the problem of prediction of fraudulent activity by the fraudsters.

E. Conclusion and Future Work

The paper explores different fraud detection data mining techniques according to different areas. Data mining is a well known zone of analyzing, predicting and defining rules from the large amount of data and finding true, previously unknown patterns. This research focuses on data mining techniques as impressive approach for fraud patterns detection to curb the fraudulent activities of the fraudster.

But with the advent of neural networks and deep learning, wherein the model learn through data and get better in classification through experience, data mining based fraud detection has grown a lot. Deep learning, which is a process wherein there is more than one layer of neural networks, and each layer is associated with a task, has been in the news for its surprisingly excellent results in classification.

Recently a new model of deep learning called GAN has come into the scene. Generative adversarial networks are a type of artificial intelligence algorithms used in unsupervised machine learning, implemented by a system of two neural networks competing against each other in a zero-sum game framework GAN which consists of two deep learning models fighting with each other in order to get the maximum results is one of the proposed measure to combat the issue. By applying the GAN to the proposed problem, we can combat two issues. One is that, since there are two neural networks fighting with each other to get maximum efficiency in classification, there is no need to re-train the model again and again as in earlier case. Second the efficiency also increases due to the presence of two neural networks.

Only downside of the use of such a model would be the time consumption. The time taken by the model is higher than the conventional neural network model. But since, here more than the time, the efficiency of the classification is of utmost importance. Future work is to implement the model suggested above and record the analysis of the classifications with respect to the SVM model and the deep learning models discussed and compared in the paper.

REFERENCES

[1] Lu Q, Ju C. Research on "credit card fraud detection model based on class weighted support vector machine" in Journal of Convergence Information Technology, 2014, 6(1):62–68.

[2] R.J. Bolton and D.J. Hand "Statistical Fraud Detection: A Review", Statistical Science, 17(3), 235-255,2002.

[3] Bhattacharya.S, Jha.S, Tharakunnel. k, and Westland J.C, "Data mining for credit card fraud: A comparative study." Decision Support systems, Vol.50, no. 7, 2011, pp.602-613.

[4] Y. Sahin & E. Duman, "Detecting credit card fraud by decision trees & support vector machines," Proceeding of the International MultiConfrence of Engineers & Computer Scientist, vol. I, 2011.

[5] R. Patidar & L. Sharma, "Credit card fraud detection using neural network," International Journal of Soft Computing & Engineering (IJSCE), vol. 1, 2011.

[6] G. Singh, R. Gupta, A. Rastogi, M. Ch&el, & A. Riyaz, "A machine learning approach for detection of fraud based on SVM," International Journal of Scientific Engineering & Technology, vol. 1, no. 3, 2012.

[7] Gajendra Singh, Ravindra Gupta, Ashish Rastogi, Mahiraj D. S. Chandel, A. Riyaz "A Machine Learning Approach for Detection of Fraud based on SVM", International Journal of Scientific Engineering and Technology (ISSN : 2277-1581), Volume No.1, Issue No.3, pg : 194-198 01 July 2012.

[8] Lanford, J., Ledell, E., Parmar, V., Arora, A., & View, M. (2015). Deep Learning with H2O.

[9] G. Singh, R. Gupta, A. Rastogi, M. Ch&el, & A. Riyaz, "A machine learning approach for detection of fraud based on SVM," International Journal of Scientific Engineering & Technology, vol. 1, no. 3, 2012.

[10] Vijayshree B. Nipane, Poonam S. Kalinge, Dipali Vidhate, Kunal War, Bhagyashree P. Deshpande "Fraudulent Detection in Credit Card System Using SVM & Decision Tree", International Journal of Scientific Development and Research (IJSDR), Volume 1, Issue 5, May 2016.