REAL TIME FRAUD PREDICTION USING ADVANCED NEURAL NETWORK

Analyses based model to predict Fraud in Credit Card Transactions

Ayush Saraf, Aditya Mule, Sakshi Bhosale, Sargam Pandey

Department of Computer Science, AISSMS Institute Of Information Technology, SPPU, Pune, India

Abstract— Credit card transactions occurs in a tremendous rate so keep track on these transactions manually to categorize fraudulent transactions and non-fraudulent transactions is practically very hard, so there must be a mechanism that will do it automatically. Many information mining techniques had been proposed for fraud detection. In this paper, a new idea of core structured collection gaining knowledge of structures has been proposed by staking a group of version, a deep sequential learning version and another top layered group classifier in right order. Models in this structure have been cleared to be very efficient in scenarios like fraud detection, where the information sequence is made up of vectors with complex interconnected features. Fraud detection has become the vital activity to reduce fraud impact on service quality, costs and reputation of a company or institute. Traditional anti-fraud method relying on manual audit is unable to deal with explosively growing information data. Meanwhile, criminals are keeping on finding new tricks by avoiding known rules to commit fraud actions. Financial institutions are struggling to find more intelligent methods for detecting fraud events, with the goal of reducing fraud losses as much as possible.

***Keywords*—** Recurrent Neural Network, Classification, LSTM.

I. INTRODUCTION

Corporations are frequently first alerted to troubles from clients themselves, and the statistics can then be used to recognise other instances of fraud. As clients recognize fraud on their owned money, they name in, and [card providers and networks] highlight that in their system, after which they'll build a sort of warmth map of all the areas where they are seeing clients report fraud. Nowadays, due to rapid growth of technology, it has become easy for the hackers to hack the personal information of the user and access the account details which is leading to massive loss. Credit card fraud costs hundreds of millions of dollars every year. Credit card fraud can occur on many factors, ranging from ignorant company (or people involved in wholesale trade) to using certain types of technologies that make it cheap and easy to help criminals hide their true identities. This problem can be solved with the help of Deep Learning techniques that consists of various parameters that are used to construct the model to find the optimal combinations of parameters to detect fraudulent activity. The three main approach which we will be analyzing for our system are RNN, RNN with LSTM and clustering for the front end. The purpose of analyzing such algorithms is to detect credit card fraud transactions by applying deep neural networks. The network is trained to reach stability and be optimal so that an appropriate model can be found to detect whether the transaction made is normal or fraud. This problem of detecting fraud transactions can be regarded as a classification problem.

This paper is organized in the following fashion- Section I contains the introduction of Deep learning, Section II contain the related work of previous technologies implemented on this project, Section III contain the some measures of methodologies and statistic studies, Section IV contain the system architecture and Section V concludes research work with future directions.

II. RELATED WORK

Earlier, some of the clustering techniques were used such as k-means, Fuzzy C-means, hierarchical based clustering and no clustering to categorize transactions. Different model-based methods are introduced that explicitly isolates anomalies instead of profiles normal points. The concept of isolation has not been explored but tried to implement for detecting anomalies. Neural-network was also used for detection accuracy and earliness of fraud detection.

Linear regression, decision tree induction, nonlinear regression, as well as "stepwise neural networks" were used for feature selection and model comparison. The background of the development of the DNN, and then introduce several typical DNN model, including deep belief networks (DBN), stacked auto-encoder (SAE) and deep convolution neural networks (DCNN), finally research its applications from three aspects and prospects the development direction of DNN. The success stories of ANN, deep architectures, and reinforcement learning in making machines more intelligent are well known. Computational costs have dropped, computing power has surged, and quasi-unlimited solid-state storage is available at a reasonable price.

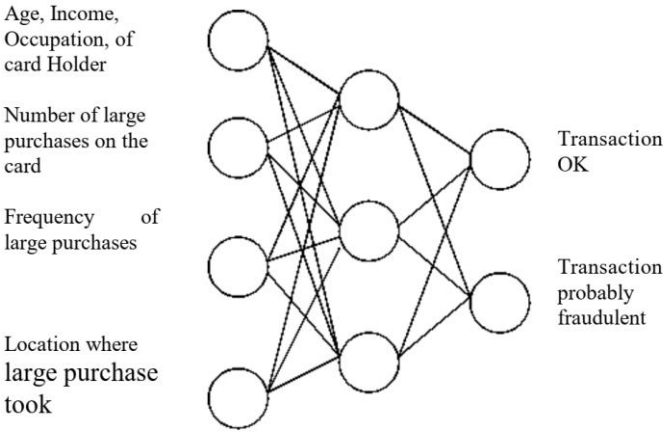
III. IMPLEMENTATION

Although there are several fraud detection technology, exist based on Data mining, Knowledge Discovery and Expert System etc. but all these are not capable enough to detect the fraud at the time when fraudulent transaction are in progress due to very less chance of a transaction being fraudulent. It has been seen that Credit card fraud detection has two highly peculiar characteristics. The first one is obviously the very limited time span in which the acceptance or rejection decision has to be made. The second one is the huge amount

of credit card operations that have to be processed at a given time. To just give a medium size example, millions of Visa card operations take place in a given day, 98% of them being handled on line. Of course, just very few will be fraudulent (otherwise, the entire industry would have soon ended up being out of businesses), but this just means that the haystack where these needles are to be found is simply enormous.

Neural network based fraud detection is based totally on the human brain working principal. Neural network technology has made a computer capable of think. As human brain learn through past experience and use its knowledge or experience in making the decision in daily life problem the same technique is applied with the credit card fraud detection technology. When a particular consumer uses its credit card , there is a fix pattern of credit card use, made by the way consumer uses its credit card. Using the last one or two year data neural network is train about the particular pattern of using a credit card by a particular consumer. As shown in the figure the neural network are train on information regarding to various categories about the card holder such as occupation of the card holder, income, occupation may fall in one category, while in another category information about the large amount of purchased are placed, these information include the number of large purchase, frequencies of large purchase, location where these kind of purchase are take place etc. within a fixed time period. In spite of pattern of credit card use neural network are also trained about the various credit card fraud face by a particular bank previously. Based on the pattern of uses of credit card, neural network make use of prediction algorithm on these pattern data to

Fig. 1



classify that weather a particular transaction is fraudulent or genuine. When credit card is being used by unauthorized user the neural network based fraud detection system check for the pattern used by the fraudster and matches with the pattern of the original card holder on which the neural network has been trained, if the pattern matches the neural network declare the transaction ok.

Matching the pattern does not mean that the transaction should exactly match with the pattern rather the neural network see to what extent there exist difference if the transaction is near by the pattern then the transaction is OK otherwise if there is a big difference then the chance of being a transaction illegal increase and the neural network declare the transaction a fault transaction. There are some occasion when the transaction made by a legal user is of a quite different and there are also possibilities that the illegal person made use of card that fit into the pattern for what the neural network is trained. Although it is rare, yet If the legal user can't complete a transaction due to these limitation then it is not much about to worry But what about the illegal person who is making use of card , hare also work human tendency to some extent when an illegal person gets a credit card he is not going to make use of this card again and again by making number of small transaction rather he will try to made as large purchase as possible and as quickly that may totally mismatch with the pattern for what the neural network is trained.

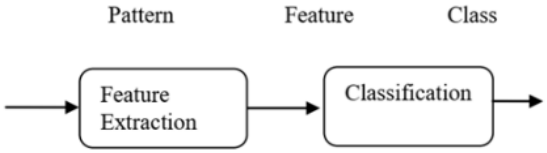


Fig.2

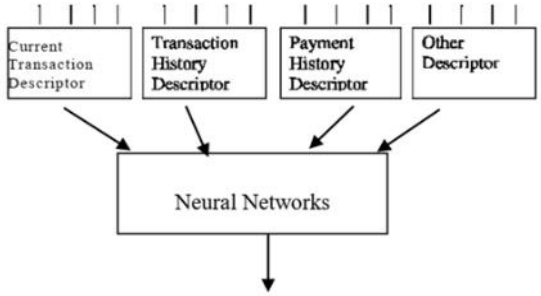


Fig. 3

In the design of neural network-based pattern recognition systems, there is always a process of business (e.g., jewellery store, consumer electronics, restaurant, hotel, etc.) History descriptors contain features characterizing the use of the card for transact-ions and the payments made to the account over some immediately prior time interval. Other descriptors can include such factors as the date of issue (or most recent reissue) of the card.

IV. CONCLUSION & FUTURE WORK

In this paper we saw different technique that is being used to execute credit card fraud how credit card fraud impact on financial institution as well as merchant and customer, fraud detection technique used by VISA and MasterCard. Neural network is a latest technique that is being used in different areas due to its powerful capabilities of learning and predicting. In this thesis we try to use this capability of neural network in the area of credit card fraud detection.

As we saw in this credit card fraud detection system there is need of large amount of previous data related to the pattern the consumer made during credit card use in purchase. Neural Network is train on this data but the problem arises at the initial stages when very few or not at all initial transaction has been made, how will we train NN when only few or no data is available to train the network

because in order to make a Neural Network to predict we must have some pattern through which NN can get train and make prediction. So we must have to design some system that may control credit card fraud before any real transaction is made.

REFERENCES

[1] Abhimanyu Roy, Jingyi Sun, Robert Mahoney, Loreto Alonzi, Stephen Adams, Peter Beling, Deep learning Detecting credit fraud in credit card transactions. IEEE Xplore(2018)

[2] Jain R., GourB., Dubey S., A hybrid approach for credit card fraud detection using rough set and decision tree technique, International Journal of Computer Applications139(10) (2016).

[3] DermalaN.,Agrawal A.N., Credit card fraud detection using SVM and Reduction of false alarms, International Journal of Innovations in Engineering and Technology (IJIET) 7(2)(2016).

[4] CarneiroE.M., Dias L.A.V., DaCunha A.M., Mialaret L.F.S., Cluster analysis and artificial neural networks: A case study in credit card fraud detection, 12th International Conference on Information Technology-New Generations (2015), 122-126.

[5] K. He, X. Zhang, S. Ren, J. Sun, "Deep residual learning for image recognition", *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 770-778, 2016.

[6] J. Corbo, C. Giovine, C. Wigley, "Applying analytics in financial institutions' fight against fraud", *McKinsey Analytics*, February 2018.

[7] G. Rushin, C. Stancil, M. Sun, S. Adams, P. Beling, "Horse race analysis in credit card fraud-deep learning logistic regression and Gradient Boosted Tree", *Systems and Information Engineering Design Symposium (SIEDS)*, pp. 117-121, 2017, April.

[8] M. Mohanraj, S. Jayaraj, C. Muraleedharan, "Applications of artificial neural networks for thermal analysis of heat exchangers-a review", *International Journal of Thermal Sciences*, vol. 90, pp. 150-172, 2015.

[9] I. Goodfellow et al., Deep learning, MIT Press, 2016.