International Journal of Engineering Technology and Management Sciences[IJETMS]

Website: ijetms.in Issue:1, Volume No.2, January 2018

Credit card fraud detection: A hybrid approach

Mbuu Mutua
Department of Computer Science and Engineering
University College of Engineering, Osmania University
Hyderabad, India
Email ID: benmbuu@gmail.com

L. K. Suresh Kumar
Department of Computer Science and Engineering
University College of Engineering, Osmania University
Hyderabad, India
Email ID: suresh.lokhande@gmail.com

Abstract – There is no doubt that credit cards make life easier and enjoyable. Being able to pay for a service or good remotely is one of the good fruits of science and innovation. However, on the other side of the coin is a scary trend that is picking up at a fast rate; fraud. Even though it is true that fraud detection and prevention is a topic that has well been researched on for quite a while, it is clear that we are still not off the hook. More needs to be done. Fraudsters are still a big trouble to their victims and financial institutions. Most of the proposed techniques of dealing with credit card fraud detection and prevention have not been able to provide a total solution to this problem, for they display a lot of false positives and true negatives. This paper proposes a hybrid approach that combines several techniques to improve on the detection of fraud. The first part of the paper briefly introduces the whole issue of credit card and fraud, and the various tricks fraudsters are using to gain anonymity in their crimes. We next discuss the related work in this topic. The third section talks about the proposed approach, and then the last part is the conclusion.

Keywords – Fraud; Credit Card; Neural Network; Anomaly Detection; Hidden Markov Model

I. INTRODUCTION

In a world where e – commerce is garnering speed every day, credit cards are becoming more and more useful, and many people are embracing them as a convenient and flexible way of doing business transactions. Whether paying for goods and services ordered through the internet or telephone, purchasing in the local supermarket, fuel filling stations, and hotels, credit cards are becoming the new cash. However, when our cards or information about us fall on the hands of a fraudster, the damages that can occur are alarming. Fraudsters gather enough details about their victim to impersonate them and apply for a credit card on the account of their victims. After getting the credit card, the fraudsters will spent on the account of the victim, and if no one detects anything abnormal going on, the damage will be unbearable. At other times, the fraudster has enough information about the card that he can key in the details of the card without much struggle when making orders (example, where the only information required is the card number, cvv number, year and month of card expiry and name of the customer). Criminals have devised many variants of credit card fraud, and if any financial institution is to protect itself and its customers from credit card fraud, then it has to come up with very creative ways of dealing with the menace. This is mainly because the criminals have perfected the art of acting and behaving like the legitimate card owners, and it has therefore become hard to draw the line between suspicious behavior of a fraudster and the behavior of a genuine card holder. In such unclear scenarios, it is very likely that a fraudulent transaction will be classified genuine (true negative), while a legitimate transaction by the credit card holder will be classified as fraudulent (false positive).

The real test for the credit card issuers and other financial institutions has been, and will continue being, how to accurately classify transactions into fraudulent and legitimate categories, in an environment where the line between the two classes is blurred. Mahmud et al. [1] observes that generally, in real case, 99% of the transactions are legitimate while 1% only is fraudulent, so fraud datasets are extremely skewed and scattered. It is for this reason why statistical fraud detection techniques are inefficient in credit card fraud detection. Rajeshwari U and Sathish babu [2] highlight several variants of credit card fraud, among the most rampant being identity theft, fake cards, stolen/lost cards, and card not present fraud (where the fraudster enters all the information of their victim's credit card, while in reality they don't physically have the card). These variants are just few of the many ways criminals use to do fraud.

II. RELATED WORK

Detection of credit card fraud is a topic that has enjoyed substantial research in the recent past. Even though the existing detection techniques still have some loopholes, it is worthwhile to acknowledge several works here which we

think have helped us come up with this paper. Agrawal et al. [3] proposes a credit card fraud detection model which takes the customer entered details during a transaction and analyses them, taking each transaction at a time and classifying it as either fraudulent or legitimate. The model combines the hidden markov model, behavior based technique, and genetic algorithm. The authors of [4] proposes the use of hybrid support vector machine (HSVM) to perform prediction and classification on the credit card dataset and classify a transaction into two classes; fraud and genuine. The authors also present the results of the comparison between their proposed system and two other existing systems (PSO and GSA), and show that the proposed system offers better performance. [5] presents an overview of the data mining frameworks used in credit card fraud detection which includes among others Stepwise logistic regression, classification regression tree (CART), chi – squared automatic interaction detector, and neural network. The authors also identify four activities that comprise the credit card process, namely, fraud detection activity, new customer selection, customer relationship management, and repayment. They go further to tabulate the research done on each of these four activities, and for each activity, the data mining techniques employed.

Bhusari and Patil [6] introduces hidden markov model and proposes a model that comprises of two main modules (online shopping and fraud detection system). The proposed model here uses the details of the last ten transactions done by the user to analyze the new transaction and decide whether it is a fraud or a legitimate one. If a fraud is suspected, the model activates a security module which requires the person doing the transaction to enter more information about them for verification. Srivastava et al. [7] studies credit card fraud detection in merchant side, and proposes the use of neural network based model that links the merchant to the payment gateway and the proposed fraud detection system. The payment gateway, which acts as a link between the merchant and the fraud detection system keeps credit card details (e.g. the card number, expiry date etc), while the merchant supplies to the gateway details such as shipping address, amount, transaction date and time. The payment gateway passes these two sets of details to the fraud detection system for analysis and detection of any fraud using a self trained neural network.

[8] Proposes a hybrid framework with big data technologies for use in credit card fraud detection. The authors here expound on several fraud detection algorithms, model fusion methods, and big data technologies. In the model proposed here, a new transaction will be processed through five components of the system; quick filter, dempster Shafer adder (DSA), explicit filter, manual verification, and historical transaction database. Fahimeh Ghobadi and Mohsen Rohani [9] present a cost sensitive modeling of credit card fraud using neural network strategy. The authors briefly discuss the basic concepts of neural networks, and how they can be applied in credit card fraud. They then propose an approach whose major goals are achieving high detection rate, and saving costs by reducing reputational risk and risk of loss. Many more works on this topic of credit card fraud detection exist outside there, but due to space and time constraints we will not be able to highlight more. It is clear from the above that numerous techniques have been proposed and put in place to curb this menace. However, we still have not had a system or model that has sufficiently solved all the issues to do with credit card fraud. All the existing strategies still suffer from one weakness or another, and fraudsters have been capitalizing on these weaknesses to carry out fraudulent activities undetected.

III. THE PROPOSED APPROACH

In this paper we propose an efficient and simple approach that, if implemented, is going to improve the situation as it is, and drastically reduce the cases of credit card fraud. The approach combines several techniques to draw from their strengths, therefore making it more resilient and efficient in detecting a credit card fraud. Our approach combines artificial neural network, hidden markov model and anomaly detection data mining technique. The main reason behind our choice of artificial neural network is its quick and efficient ability to detect fraudulent activity at the time of transaction. Hidden markov model is not only equally able in detecting a fraud during a transaction as the artificial neural network, but also the model reduces false positive transactions, that is, genuine transactions classified as fraudulent. Our choice of anomaly detection is to compliment the hidden markov model which cannot detect fraud in initial few transactions, and its ability to handle non – linear data [10].

Our proposed approach uses a self training multi layer feed forward perceptron neural network as the final module of classifying the transaction as either genuine or a fraud. The model has three main modules. The first module takes the stored details of the previous transactions and the details of the new transaction and analyses them for any anomaly or suspicious signs. This module depends on the anomaly detection data mining technique for its operation. The next module that works alongside the first one takes the details of the new transaction (purchase amount, entered credit card information, etc), together with the already stored credit card information, analyses them, and assigns the new transaction a

probability value that denotes its likelihood to being a fraud. This module uses the hidden markov model technique and its outcome is a probability value. The lesser the outcome value of this module, the more legitimate the transaction is. Both the above modules pass their outcome to an intermediate feature whose main purpose is to convert the outcome values into variables, and to feed them into the multi layer perceptron neural network. The neural network is self trained, and its work is to classify the new transaction as either a fraud or legitimate, using the variables fed into it from the format converter. The figure below shows the structure of our proposed model for credit card fraud detection.

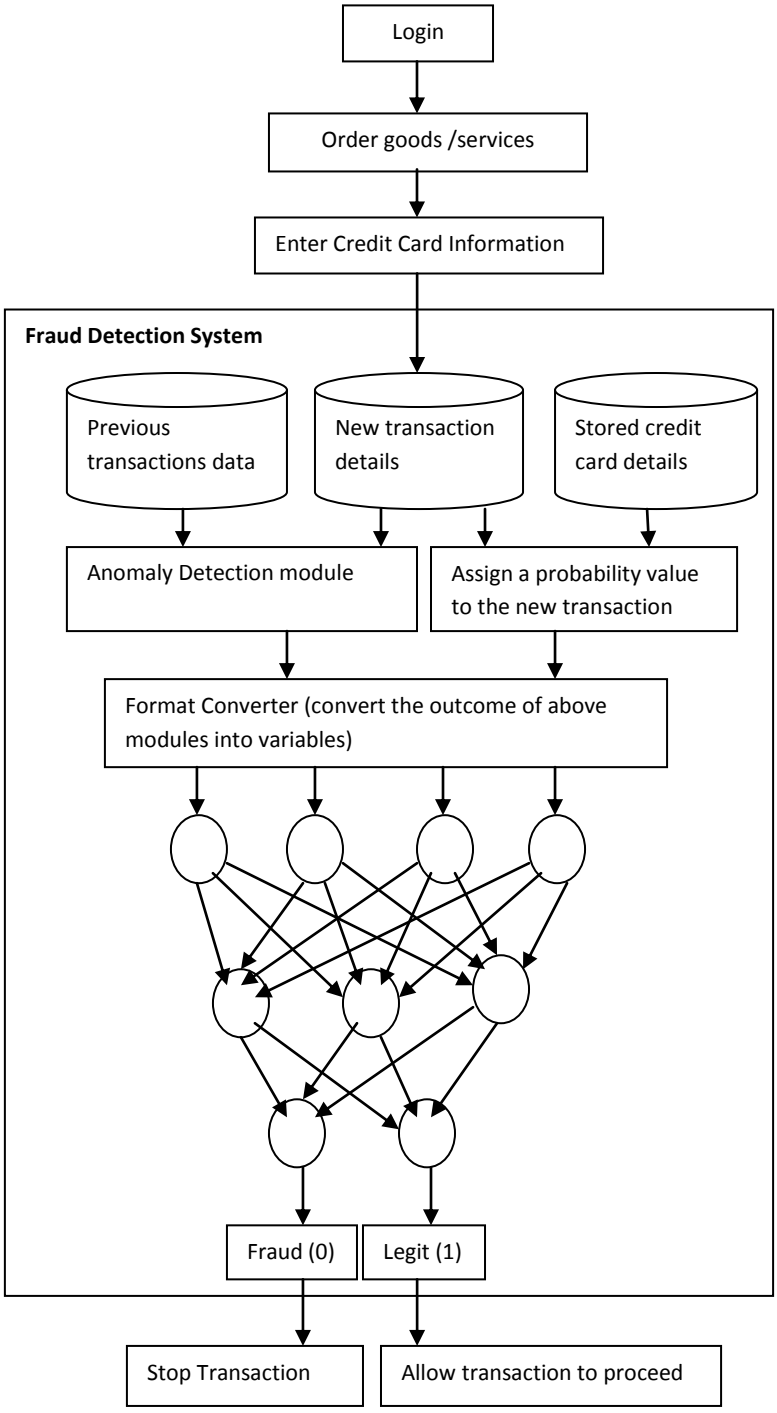

Fig. 1: Block diagram of the proposed model

IV. CONCLUSION

Credit card fraud detection is a very critical research area today. A lot of money has gone missing in the hands of fraudsters, wrecking our economy. For this reason we have come up with the approach above, which, if implemented, will cover a lot of loopholes fraudsters use to commit crimes. There are many proposed approaches which depend on a single technique in detecting fraud; but the approaches still have loopholes which fraudsters are capitalizing on. This is why we think that any approach that will be of benefit will have to combine several techniques, to make the approach more resilient. In this paper we have proposed a hybrid approach to credit card fraud detection that consists of the anomaly detection data mining technique, hidden markov model, and a multilayer neural network.

REFERENCES

[1]. Mohammad Sultan Mahmud, Phayung Meesad and Sunantha Sodsee, "An evaluation of computational intelligence in credit card fraud detection", IEEE communications journal, 2016

[2]. Rajeshwari U and Sathish babu, "Real-time credit card fraud detection using streaming analytics", 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) pp. 439 – 444

[3]. Ayushi Agrawal, Shiv Kumar and Amit Mishra, "A novel approach for credit card fraud detection", 2nd International Conference on Computing for Sustainable Global Development (INDIACom) 2015 pp.8 – 11

[4]. V. Mareeswari and G. Gunasekaran, "Prevention of credit card fraud detection based on HSVM", Proceedings of the International Conference On Information Communication And Embedded System(ICICES 2016)

[5]. Pornwatthana Wongchinsri and Werasak Kuratach, "A survey – data mining frameworks in credit card processing", IEEE communications journal 2016

[6]. V. Bhusari and S. Patil, "Study of hidden markov model in credit card fraudulent detection", proceedings of the World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR'16) pp. 33 – 37

[7]. Aman Srivastava, Mugdha Yadav and Sandipani Basu, "Credit card fraud detection at merchant side using neural networks", 2016 International Conference on Computing for Sustainable Global Development (INDIACom) pp. 667 – 670

[8]. You Dai, Jin Yan, Xiaoxin Tang, Han Zhao and Minyi Guo, "Online credit card fraud detection: A Hybrid framework with big

data technologies", 2016 IEEE Trustcom-BigDataSE-ISPA pp. 1644 – 1651

[9]. Fahimeh Ghobadi and Mohsen Rohani, "Cost sensitive modeling of credit card fraud using neural nnetwork strategy", proceedings of the 2nd Iranian Conference on Signal Processing and Intelligent Systems, 14 – 15 Dec 2016, Tehran, Iran

[10]. N. Malini and M. Pushpa, "Analysis on credit card fraud identification techniques based on KNN and outlier detection", proceedings of the 3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEEICB17)