International Journal of Advanced Computer Technology (IJACT)
ISSN: 2319-7900 www.ijact.org Volume IX, Issue V, October 2020

An Assessment on Credit Card Fraud Detection: Survey

Abhishek Malviya[1], Himanshu Yadav[2]
Department of CSE, RITS, Bhopal
Abhishek.malviya27@gmail.com[1], himanshuyadav86@gmail.com[2]

ABSTRACT: Credit card fraud is a costly problem for many financial institutions, costing businesses billions of dollars a year. Many adversaries still escape fraud detection systems because these systems often do not include information about the adversary's knowledge of the fraud detection mechanism. This thesis aims to include information on the motivations of "crooks" and the knowledge base in an adaptive fraud detection system. In this thesis, we use a theoretical adversarial learning approach to classification to model the best fraudster strategy. We proactively adapt the fraud detection system to classify these future fraudulent transactions better. Therefore, this document aims to provide an over-supervised bird's-eye approach with a suitable feature extraction technique that improves fraud detection rather than mistakenly classifying an actual transaction as fraud.

Keywords: - Credit Card Fraud Detection, Classification, Ensemble Techniques, Random Forest, Decision Trees

I. INTRODUCTION

Nowadays, as internet speed has increased and the prices of mobile have decreased very much in the past few years. Also, the data prices too are very much affordable to most of the people. This has resulted in the digitization of most of the institutes as it is easy and convenient for people and also for the authority to maintain the records. So, it resulted in most of the banks and other institutes receiving and transferring money through credit cards.

But with the hackers and other cybercriminals around, there are always chances of the frauds in the transactions. The possibility of the fraud transaction is significantly less. Still, it is not negligible and even having one fraud transaction is unacceptable because it is a crime and we can't neglect it even if it is very less as it harms both the customer and credibility of the institute. So this paper aims at analyzing various classification techniques using multiple metrics for judging multiple classifiers.

The central challenge with Credit card fraud detection is to develop a system which can differentiate between the normal and an intrusion which represents potentially harmful activity. A promising solution is emerging in the form of machine learning technique, and in particular, supervised learning.

Credit card fraud detection relies on the analysis of recorded transactions. Transaction data are mainly composed of several attributes (e.g. credit card identifier, transaction date, recipient, amount of the transaction). Automatic systems are essential since it is not always possible or easy for a human analyst to detect fraudulent patterns in transaction datasets, often characterized by a large number of samples, many dimensions and online updates. Also, the cardholder is not reliable in reporting the theft, loss or fraudulent use of a card [10-17].

II. CREDIT CARD FRAUD

Credit card frauds may occur in various ways [9]: to mention some, we can have stolen card fraud, cardholder-not-present fraud and application fraud:

(a) Stolen card fraud is the most common type of fraud where the fraudster usually tries to spend as much as possible and as quickly as possible. The detection of such a fraud typically relies on the discovery of an unexpected usage pattern of the credit card (generally unexpectedly important) for the common practice.

(b) Cardholder-not-present fraud often observed in e-business. Here the fraudster needs the information about a credit card but not the card itself. This fraud demands prompt detection since, unlike the previous case, the official card owner is not aware that his data have been stolen.

(c) Application fraud corresponds to the application for a credit card with false personal information. This kind of fraud occurs more rarely since it could be detected during the application by checking the information of the applier, contrary to other frauds that cannot be anticipated.

In the following, we will now discuss the advantages and disadvantages of Expert Driven and Data-Driven approaches to fraud detection. The Expert Driven approach uses domain knowledge from fraud investigators to define rules that used to predict the probability of a new transaction to be fraudulent. Let us imagine that the investigators know from experience that a transaction done on a betting website with an amount greater than $10000 is almost certain to be fraudulent. Then we can automatize the detection by mean of a rule as "IF transaction amount > $10000 & Betting website THEN fraud probability = 0.99". In the same spirit, we can define a set of rules for different

scenarios. Typically, expert rules can be distinguished between scoring rules and blocking rules. The former assigns a score to a transaction based on the risk the investigators associate to a certain pattern; the latter can block the transaction because the risk of fraud is too high. The advantages of expert rules are: i) they are easy to develop and to understand, ii) they explain why an alert was generated and iii) they exploit domain expert knowledge. However, they have several drawbacks: i) they are subjective (if you ask seven experts you may get seven different opinions), ii) they detect only easy correlations between variables and frauds (it is hard for a human analyst to think in more the three-dimension and explore all possible pattern combinations), iii) they can detect only known fraudulent strategies, iv) they require human monitoring/supervision (update in case of performance drop) and v) they can become obsolete soon due to fraud evolution.

III. Challenges in Data-Driven Fraud Detection Systems

The design of FDSs employing DDMs based on Machine Learning algorithms is particularly challenging for the following reasons:

(a) Frauds represent a small fraction of all the daily transactions [18].

(b) Frauds distribution evolves because of seasonality and new attack strategies [19].

(c) The true nature (class) of the majority of transactions is typically known only several days after the transaction took place since only a few transactions are timely checked by investigators [20].

The first challenge is also known as the unbalanced problem [21] since the distribution of the transactions is skewed towards the genuine class. The distributions of genuine and fraud samples are not only unbalanced but also overlapping (see the plot over the first two principal components in Figure 1.2). Most Machine Learning algorithms are not designed to cope with both unbalanced and overlapped class distributions [22]. The change in fraudulent activities and customer behaviour is the main responsible for non-stationary in the stream of transactions. This situation is typically referred to as concept drift [23]. It is of extreme relevance for FDSs which have to be constantly updated either by exploiting the most recent supervised samples or by forgetting outdated information that might be no more useful whereas not misleading. FDS strategies that are not updated or revisited frequently are often losing their predictive accuracy in the long term [18]. The third challenge is related to the fact that, in a real-world setting, it is impossible to check all transactions. The cost of human labour seriously constrains the number of alerts, returned by the FDS, which can be validated by investigators. Investigators check FDS alerts by calling the cardholders and then provide the FDS with feedbacks indicating whether the alerts were related to fraudulent or genuine transactions. These feedbacks, which refer to a tiny fraction of the amount of the daily transactions, are the only real-time information that can be provided to train or update classifiers. The class (fraudulent / non-fraudulent) of the rest of the transactions is known only several days later. Classes can be automatically assigned when a certain period has passed, e.g. by assuming a certain reaction time for customers to discover and then report frauds. Standard FDSs ignoring feedbacks from investigators often provide less accurate alerts than FDSs able to use both feedbacks and the other supervised samples available [20] efficiently.

IV. Related Work

This section gives an extensive literature survey on the multiple relational classifications using genetic algorithms. We study various research paper and journal and know about data classification. All methodology and process are not described here. But some related work in the field of association classification discusses by the name of authors and their respective title.

M. F. Zeager [1] use a game theoretical adversarial learning approach to model the fraudster's best strategy, and pre-emptively adopt the fraud detection system to better classify these future fraudulent transactions. Using a logistic regression classifier as the fraud detection mechanism, we initially identify the best strategy for the adversary based on the number of fraudulent transactions that go undetected and assume that the adversary uses this strategy for future transactions to improve our classifier. Prior research has used game theoretic models for adversarial learning in the domains of credit card fraud and email spam. Still, this project adds to the literature by extending these frameworks to a practical, real-world data set. Test results show that our adversarial framework produces an increasing AUC score on validation sets over several iterations in comparison to the static model usually employed by credit card companies.

Alejandro Correa Bahnsen [2] expands the transaction aggregation strategy and proposes to create a new set of features based on analyzing the periodic behaviour of the time of a transaction using the von Mises distribution. Then, using a real credit card fraud dataset provided by a large European card processing company, we compare state-of-the-art credit card fraud detection models and evaluate how the different sets of features have an impact on the results. By including the proposed periodic features into the methods, the results show an average increase in savings of 13%.

Y. Saygin [3] used a game-theoretic framework to suggest the fair value for information extracted via data mining and shared between two retail-market competitors. For mutual benefit, the two players each owning a privileged information set (a collection of data or database) may want to share or pool all or part of the information contained within their respective databases. Assume that each player is equipped with a data mining technique which extracts information from the data. We first model the information sharing as a cooperative game. Then, we use results from the cost-sharing literature to provide information sharing methods when data can be quantified either as discrete or as continuous variables. In the latter case, we provide a means for obtaining decision rules for pricing shared information.

C. Jiang [4] proposes a novel fraud detection method that composes of four stages. To enrich a cardholder's behavioural patterns, we first utilize the cardholders' historical transaction data to divide all cardholders into different groups such that the transaction behaviours of the members in the same group are similar. We thus propose a window-sliding strategy to aggregate the transactions in each group. Next, we extract a collection of specific behavioural patterns for each cardholder based on the aggregated transactions and the cardholder's historical transactions. Then we train a set of classifiers for each group on the base of all behavioural patterns. Finally, we use the classifier set to detect fraud online. If a new transaction is fraudulent, a feedback mechanism took in the detection process to solve the problem of concept drift. The results of our experiments show that our approach is better than others.

K. Randhawa [5] machine learning algorithms used to detect credit card fraud as a Standard model first used. Then, hybrid methods which use AdaBoost and majority voting methods are applied. To evaluate the efficiency of a model, a publicly available credit card data set used. Then, a real-world credit card data set from a financial institution is analyzed. Besides, noise is added to the data samples to further assess the robustness of the algorithms. The experimental results positively indicate that the majority voting method achieves good accuracy rates in detecting fraud cases in credit cards.

S. M. S. Askari [6] proposed a fraud detection algorithm based on Fuzzy-ID3. Intermediate nodes we split using attribute having the highest information gain. The leaf nodes classify the transactions as fraud, doubtful or normal. The experimental result exhibits that the technique is an efficient one in detecting frauds.

Charleonnan [7] proposed method adopts three base classifiers which are MLP, NB and Naive Bayes algorithms. Besides, it can analyze the correctness to work with the unbalance datasets. Therefore, this research is focusing on the information of the credit card company of Taiwan for collecting data on customer behaviours in credit card payment. After that, it has brought the information to predict correctness whether it has the risks in payment. The result shows that the proposed method can achieve the best classification performance in terms of accuracy and sensitivity.

V. CONCLUSION

Nowadays, as internet speed has increased and the prices of mobile have decreased very much in the past few years. Also, the data prices too are very much affordable to most of the people. This has resulted in the digitization of most of the institutes as it is easy and convenient for people and also for the authority to maintain the records. So, it resulted in most of the banks and other institutes receiving and transferring money through credit cards. But with the hackers and other cybercriminals around, there are always chances of the frauds in the transactions. The possibility of the fraud transaction is very less. Still, it is not negligible and even having one fraud transaction is unacceptable because it is a crime and we can't neglect it even if it is very less as it harms both the customer and credibility of the institute. So this dissertation aims to suggest one supervised approach with proper feature extraction technique that improving fraud detection rather than misclassifying a genuine transaction as fraud.

REFERENCE

[1]. M. F. Zeager, A. Sridhar, N. Fogal, S. Adams, D. E. Brown and P. A. Beling, "Adversarial learning in credit card fraud detection," *2017 Systems and Information Engineering Design Symposium (SIEDS)*, Charlottesville, VA, 2017, pp. 112-116.

[2]. Alejandro Correa Bahnsen, Djamila Aouada, Aleksandar Stojanovic, Björn Ottersten, “Feature engineering strategies for credit card fraud detection”, Expert Systems with Applications, Volume 51, 2016, Pages 134-142,

[3]. Y. Saygin, A. Reisman and YunTong Wang, "Value of information gained from data mining in the context of information sharing," in *IEEE Transactions on Engineering Management*, vol. 51, no. 4, pp. 441-450, Nov. 2004.

[4]. C. Jiang, J. Song, G. Liu, L. Zheng and W. Luan, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," in *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1-1.

[5]. K. Randhawa, C. K. Loo, M. Seera, C. P. Lim and A. K. Nandi, "Credit card fraud detection using AdaBoost and majority voting," in *IEEE Access*, vol. PP, no. 99, pp. 1-1

[6]. S. M. S. Askari and M. A. Hussain, "Credit card fraud detection using fuzzy ID3," *2017 International Conference on Computing,*

Communication and Automation (ICCCA), Greater Noida, 2017, pp. 446-452.

[7]. Charleonnan, "Credit card fraud detection using RUS and MRN algorithms," *2016 Management and Innovation Technology International Conference (MITicon)*, Bang-San, 2016, pp.

[8]. DUDA, R. O. AND HART, P. E., 1973. "Pattern Classification and Scene Analysis". John Wiley and Sons, Inc., New York, NY.

[9]. MAO, J. AND JAIN, A. K., 1996. "A self-organizing network for hyperellipsoidal clustering (HEC)". IEEE Trans. Neural Netw. 7, 16–29.

[10]. Angiulli, F. (2009) "Outlier Detection Techniques for Data Mining" John Wang (Ed.), Encyclopedia of Data Warehousing and Mining, Second Edition, Pp. 1483-1488.

[11]. Dubes, R. (1993). "Cluster analysis and related issue". In Handbook of Pattern Recognition and Computer Vision, C. Chen, L. Pau, and P. Wang, Eds., River Edge, NJ: World Science Publishing Company, pp. 3 – 32.

[12]. Gordon, A. (1998). "Cluster validation". In Data Science, Classification, and Related Methods, C. Hayashi, N. Ohsumi, K. Yajima, Y. Tanaka, H. Bock, and Y. Bada, Eds., New York, NY: Springer - Verlag, pp. 22 – 39.

[13]. Halkidi, M., Batistakis, Y., and Vazirgiannis, M. (2002). "Cluster validity methods": Part I & II, SIGMOD Record, 31 (2 & 3).

[14]. Dubes, R. (1993). "Cluster analysis and related issue". In Handbook of Pattern Recognition and Computer Vision, C. Chen, L. Pau, and P. Wang, Eds., River Edge, NJ: World Science Publishing Company, pp. 3 – 32.

[15]. Rand, W. (1971). "Objective criteria for the evaluation of clustering methods". Journal of the American Statistical Association, 66: 846 – 850.

[16]. Peter J. Rousseeuw (1987). "Silhouettes: a Graphical Aid to the Interpretation and Validation of Cluster Analysis". Computational and Applied Mathematics 20: 53–65.

[17]. L. Hubert, J. Schultz. "Quadratic assignment as a general data-analysis strategy".1976. British Journal of Mathematical and Statistical Psychologie. 29. 190-241.

[18]. P. Jaccard. "The distribution of flora in the alpine zone". 1912. New Phytologist. 11, 37–50.

[19]. Fujikawa, Y. and Ho, T. (2002). "Cluster-based algorithms for dealing with missing values".In Cheng, M.-S., Yu, P. S., and Liu, B., editors, Advances in Knowledge Discovery and Data Mining, Proceedings of the 6th Pacific-Asia Conference, PAKDD 2002, Taipei, Taiwan, volume 2336 of Lecture Notes in Computer Science, pages 549–554. New York: Springer.

[20]. W.M. Rand. "Objective criteria for the evaluation of clustering methods". 1971. Journal of the American Statistical Association. 846-850.

[21]. Everitt, B., Landau, S., and Leese, M. (2001). "Cluster analysis", 4th edition. London: Arnold

[22]. Hartigan, J. (1975). "Clustering algorithms". New York, NY: John Wiley & Sons

[23]. ROSENFELD, A. AND KAK, A. C., 1982. "Digital Picture Processing". 2nd ed. Academic Press, Inc., New York, NY.