ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 6, June 2017

Review on Computational Techniques for Credit Card Fraud Detection

S. Deepica

Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh, India

Email Id: deepica.dominic@Galgotiasuniversity.edu.in

ABSTRACT: The safety risks correlated with e-commerce are commonplace and the number of credit card transactions are becoming critical. The safety concerns arising from online use of credit cards are discussed in this paper. Literature has been studied over the past two and a half decades to examine evolving obfuscation techniques and responses to this issue. Online payments are also rising in India as a result of a growing number of online corporate fraud. Such frauds are aimed towards banking services such as credit, debit and ATM Cards, payment gateways, etc. Furthermore, due to the large credit limits presented by banks, a significant number of credit card frauds are decided to launch. The three parties-spending, issuing banks, and traders-are left in a jiffy by online credit-carry fraud which creates economic damage to them all. Many typical features and usable credit card transaction databases have been collected that provide new investigators with a point of reference. Efficiency in solving key issues of fraud detection such as real-time identification, definition drift, mismatch databases, and classification adaptation have been explored in current fraud detection approaches. New guidelines have also been recommended for credit card fraud identification.

KEYWORDS*:* Credit card fraud, Credit card fraud detection system, Machine learning, Computational models, Classifiers, Supervised and unsupervised learning

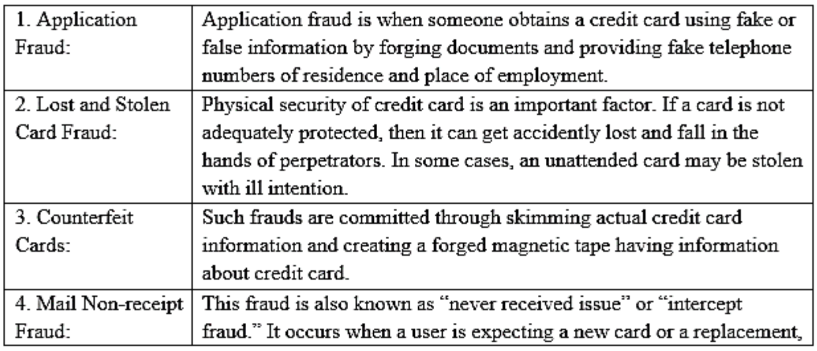
I. INTRODUCTION

For even more than two decades, credit cards have been the primary financial processing devices in all electronic commercial activity. This helps make payment services based on credit cards fraud susceptible. The first credit card was released in the U.S. in 1958, while in India the first credit card were released in 1981. The first debit card was released. Since that day, the loss of trillions of loans and daily credit card fraud have been continuing Credit card fraud is a growing and severe problem involving illegal / non-authorized card use, unanticipated purchase activity, or any form of the disabled card transaction. Large e-commerce players such as Amazon India, Flipkart, and Snap-deal have penetrated online trade in India substantially. Therefore, in an individual transaction, the entire ecosystem can witness a varied improvement in the use of credit cards. Such use is called "non-present card," since only credit card information is needed rather than physical cards. The growth in electronic payments also contributes to a significant spike in India's online banking fraud. Fraud targets banks such as cash, debit and ATM cards, payment gateways and other methods in net banking. Yet, due to huge banking credit limits, a big chapter in fraud is being opened on credit cards. Credit card frauds are being conducted because of strong banks ' credit limits. The three groups, spenders, issuers of banks and retailers, are all fooled by an on-line scam of credit card, and all-cause massive damage. The cardholder/wallet owner shall be liable for identifying theft with little or no particular preventive procedure in the credit card company. The cardholder shall report the authorizing bank with fraudulent charges. The bank also reviews the matter and the procedure for restoring the credit for the sale is activated where proof of wrongdoing is identified. The cardholder might not continue to be harmed by credit card fraud due to excessive multiple defaults in the fraud situations protected in the issuing bank. The chargeback is nevertheless reciprocal and does not extend to all frauds. There are also some potential drawbacks and considerations for follow-up. Merchants also have to take full responsibility for losses caused by fraud, especially on credit card payments. Even though the loss of fraud is incurred by the credit card company, the broker may lose a lot of money due to irretrievable costs such as shipping charges or card homestead exemptions. A lot of resources are also used by the credit card company to manage the case costs. In order to address the question, banks aim to provide their customers with appropriate guidance on the safe use of cards. But the evacuation orders aren't always against all the perpetrators ' social engineering processes. Therefore banks must use tools to identify and trace the origins of fraud throughout the case of a suspected scam. The processing time was a few days for this finding that does not serve as a deterrent to theft.

II. CREDIT CARD FRAUDS AND DETECTION

A credit card is a polymer small card issued from a financial firm that enables the account holder to buy goods and services. The charged balance is deposited into the wallet of the customer and the amount lent must be returned and any other costs agreed to as negotiated by the card company. Such cards will be used by physical implementation at the point of sale (PoS) and by disclosing information on cards through online purchases. Every fraudulent use would be considered a credit card scam in either of these two ways. Credit card fraud is primarily based on unauthorized exposure to possession at the time or credit card details. In different cases, the mode of operation will, however, vary. In the case of frauds addressed in publications of financial information, it is possible to classify them into two broad categories outlined in this section. Obtaining Physical Cards illegally comprise of following depicted types (Table 1), while types are depicted fig.1

Table.1: Obtaining Physical Cards Illegally



1. Application Fraud:	Application fraud is when someone obtains a credit card using fake or false information by forging documents and providing fake telephone numbers of residence and place of employment.
2. Lost and Stolen Card Fraud:	Physical security of credit card is an important factor. If a card is not adequately protected, then it can get accidently lost and fall in the hands of perpetrators. In some cases, an unattended card may be stolen with ill intention.
3. Counterfeit Cards:	Such frauds are committed through skimming actual credit card information and creating a forged magnetic tape having information about credit card.
4. Mail Non-receipt Fraud:	This fraud is also known as "never received issue" or "intercept fraud." It occurs when a user is expecting a new card or a replacement,

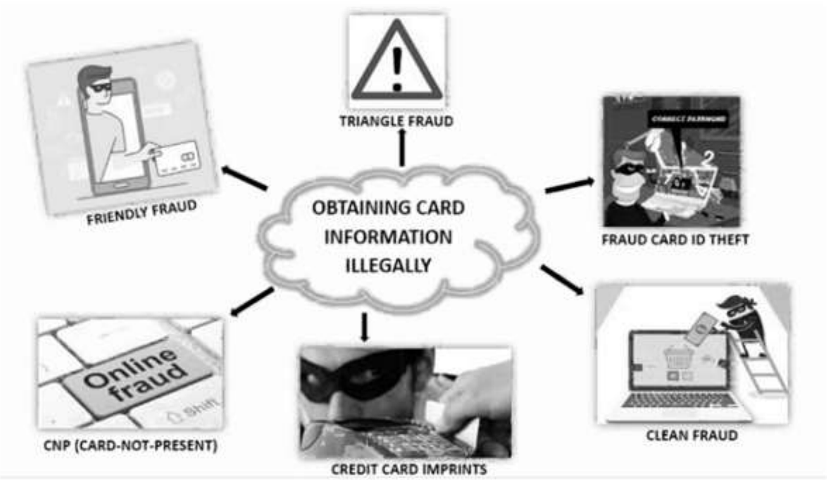
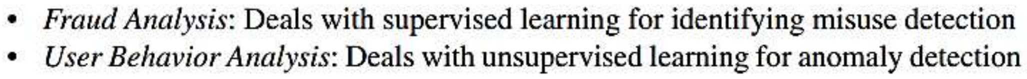


Fig.1: Types of Frauds by Obtaining Credit card Information Illegally

III. COMPUTATIONAL TECHNIQUES FOR FRAUD DETECTION

Computing methods suggested as much as the scams themselves are introduced for the analysis of fraudulent activity. To order to obtain automatic fraud detection mechanisms in the context of multiple data types, different methods were used for analytics, natural language processing and data mining. The methods commonly used for the analysis of fraudulent activity can be defined as follows:

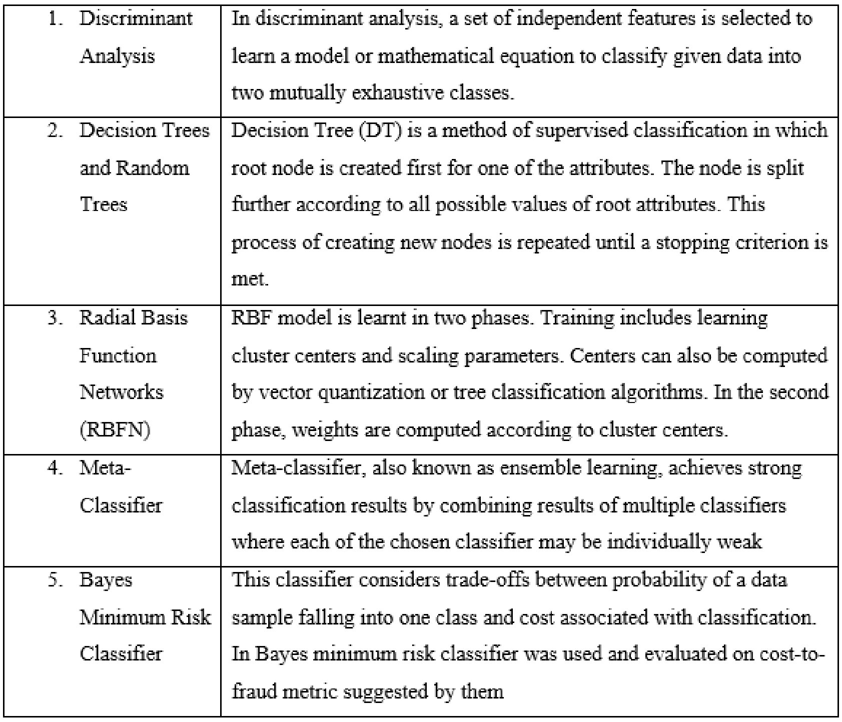


- *Fraud Analysis*: Deals with supervised learning for identifying misuse detection
- *User Behavior Analysis*: Deals with unsupervised learning for anomaly detection

If a proportion of label purchases are obtainable, machine-based classificatory can be trained to identify future trades that are politically motivated and regular. Such classificatory use mark data to model the transactions of both forms. Several supervised models of learning have been implemented for the identification, such as judgment tables, backpropagation neural networks, support vector machines (SVMs), random forests and Bayesian networks (BNs). Nevertheless, such approaches do not allow new forms in fraudulent transactions to be detected. When adapting to new crimes, the unattended class of approaches is versatile and can be implemented towards an innovative fraudster. Fewer unattended forms of identification of fraud include self-organization graphs, peer group analysis, breakpoint analysis and strategic thinking[1]–[8].

One type of techniques identify deception based on individual user behavior analyzes, which have been overlooked in machine learning approaches. These include a description of each user's daily activity behavior centered on his or her usual transactions. The real transaction is compared to this database and each transaction is given a degree of suspicion depending on the profile of the customer. The Transaction properties for preprocessing are of normative, ordinal, Boolean, integer and document mixed data form. Binning, combining, normalization, sorting, ordinal to numerical, group characteristics are few preprocessing processes used in the map entry variables for a collection of more concise characteristics. Until implementing other mathematical models focused on machine learning, pre-processing is a necessary step. Table 2 presents "Computational Models Based on Supervised Machine Learning".

Table.2: Computational Models Bases on Supervised Machine Learning



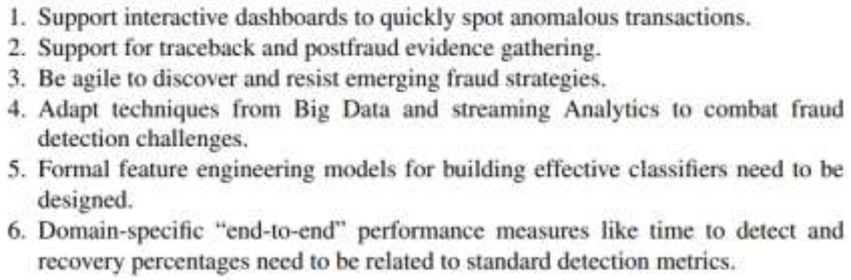
1. Discriminant Analysis	In discriminant analysis, a set of independent features is selected to learn a model or mathematical equation to classify given data into two mutually exhaustive classes.
2. Decision Trees and Random Trees	Decision Tree (DT) is a method of supervised classification in which root node is created first for one of the attributes. The node is split further according to all possible values of root attributes. This process of creating new nodes is repeated until a stopping criterion is met.
3. Radial Basis Function Networks (RBFN)	RBF model is learnt in two phases. Training includes learning cluster centers and scaling parameters. Centers can also be computed by vector quantization or tree classification algorithms. In the second phase, weights are computed according to cluster centers.
4. Meta-Classifier	Meta-classifier, also known as ensemble learning, achieves strong classification results by combining results of multiple classifiers where each of the chosen classifier may be individually weak
5. Bayes Minimum Risk Classifier	This classifier considers trade-offs between probability of a data sample falling into one class and cost associated with classification. In Bayes minimum risk classifier was used and evaluated on cost-to-fraud metric suggested by them

- Mathematical models based on different methods:

Many other means of addressing the issue have increasingly been explored. An algorithm for hybrid data extraction/complex networking was suggested. To describe common functions in transaction records, dynamic networks have been used. "Parenclitical nets" have specifically been used, a strategy of network restoration that seeks to distinguish between a particular data example in the case and a series of educational instances. The design of the network topology is focused on topological characteristics which have an irregular relationship between normal payments and unusual ones. The Area under the Curve (AUC) increased by approximately 5.9% when networks were taught to minimize negative results. A Conduct Certification (BC) fraud detection approach was suggested. BC classifies general and unique user behavior functionality (festival/weekends) that FDS will review. From the behavioral characteristic collection in data sets the dichotomous behavior characteristic vector of 13 values, specifically: (1) "week-day" (2) "week-end" (3) "festival" (4) "standard-day" (5–8) "interval" (i=1–4), is four-time-prevails (9). A risk factor is determined on the basis of BC cardholder on each cryptographic signature and a warning is produced if the danger is greater than the thresholds. The technique was conducted well on a synthetically constructed data set and provided up to 92 percent specificity values[8]–[14].

- Credit Card Fraud Detection Next-generation computer model

Much has been accomplished with improving fraud detection methods, but more also needs to be done. A relatively new area is the knowledge from the anti-stationary data stream, with biased class representation and a weak real-time, positive result and strong true negative ratio. With a critical analysis of the work carried out on modeling numerical FDS models, there is little need for more progress:



1. Support interactive dashboards to quickly spot anomalous transactions.
2. Support for traceback and postfraud evidence gathering.
3. Be agile to discover and resist emerging fraud strategies.
4. Adapt techniques from Big Data and streaming Analytics to combat fraud detection challenges.
5. Formal feature engineering models for building effective classifiers need to be designed.
6. Domain-specific "end-to-end" performance measures like time to detect and recovery percentages need to be related to standard detection metrics.

IV. CONCLUSION

Fraud in credit card purchases is a recent occurrence as credit card transactions have been rapidly increasing. Several computer-based learning devices are suggested for the creation of a powerful detection system of credit card fraud. The most common models in the last two and a half years were reviewed in this segment. Existing identity verification systems were found to suffer from issues such as minimal knowledge of credit card processing, lack of conventional algorithms, suitable criteria and high fallacious-positive alarm rates. Above all, the validity of earlier models cannot be measured by credit card comparison datasets. Downloading data technology and Big Data Analysis techniques have not yet been and can be discussed in this area.

REFERENCES

[1] S. Benson Edwin Raj and A. Annie Portia, "Analysis on credit card fraud detection methods," in *2011 International Conference on Computer, Communication and Electrical Technology, ICCCET 2011*, 2011.

[2] A. Correa Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature engineering strategies for credit card fraud detection," *Expert Syst. Appl.*, 2016.

[3] A. Dal Pozzolo, O. Caelen, Y. A. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," *Expert Syst. Appl.*, 2014.

[4] M. Zareapoor and P. Shamsolmoali, "Application of credit card fraud detection: Based on bagging ensemble classifier," in *Procedia Computer Science*, 2015.

[5] F. Carcillo, A. Dal Pozzolo, Y. A. Le Borgne, O. Caelen, Y. Mazzer, and G. Bontempi, “SCARFF: A scalable framework for streaming credit card fraud detection with spark,” *Inf. Fusion*, 2018.

[6] I. Trivedi, M. M, and M. Mridushi, “Credit Card Fraud Detection,” *IJARCCE*, vol. 5, no. 1, pp. 39–42, 2016.

[7] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, “Credit card fraud detection: A realistic modeling and a novel learning strategy,” *IEEE Trans. Neural Networks Learn. Syst.*, 2018.

[8] J. Akhilomen, “Data mining application for cyber credit-card fraud detection system,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013.

[9] F. Carcillo, Y. A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, “Combining unsupervised and supervised learning in credit card fraud detection,” *Inf. Sci. (Ny).*, 2019.

[10] N. Wong, P. Ray, G. Stephens, and L. Lewis, “Artificial immune systems for the detection of credit card fraud: An architecture, prototype and preliminary results,” *Inf. Syst. J.*, 2012.

[11] S. Patil, V. Nemade, and P. K. Soni, “Predictive Modelling for Credit Card Fraud Detection Using Data Analytics,” in *Procedia Computer Science*, 2018.

[12] U. Azeem, K. Shan, A. Nadeem, and N. Q. Mohammad, “Real-Time Credit-Card Fraud Detection using Artificial Neural Network Tuned by Simulated Annealing Algorithm,” *Int. Conf. Recent Trends Information, Telecommun. Comput. ITC*, 2014.

[13] A. Dal Pozzolo, “Adaptive Machine Learning for Credit Card Fraud Detection Declaration of Authorship,” *PhD Thesis*, 2015.

[14] K. K. Sherly and R. Nedunchezhian, “Boat adaptive credit card fraud detection system,” in *2010 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2010*, 2010.

- V.M. Prabhakaran, Prof S.Balamurgan ,A.Brindha ,S.Gayathri ,Dr.Gokul Kruba Shanker,Duruvak kumar V.S, “NGCC: Certain Investigations on Next Generation 2020 Cloud Computing-Issues, Challenges and Open Problems,” Australian Journal of Basic and Applied Sciences (2015)
- V.M.Prabhakaran, Prof.S.Balamurugan , S.Charanyaa, “Data Flow Modelling for Effective Protection of Electronic Health Records (EHRs) in Cloud”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 2015
- R. Santhya, S. Latha, S. Balamurugan and S. Charanyaa, "Further investigations on strategies developed for efficient discovery of matching dependencies" International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 1, January 2015
- Ishleen Kaur, Gagandeep Singh Narula and Vishal Jain, “Identification and Analysis of Software Quality Estimators for Prediction of Fault Prone Modules”, INDIACom-2017, 4th 2017 International Conference on “Computing for Sustainable Global Development”.
- Ishleen Kaur, Gagandeep Singh Narula, Ritika Wason, Vishal Jain and Anupam Baliyan, “Neuro Fuzzy—COCOMO II Model for Software Cost Estimation”, International Journal of Information Technology (BJIT), Volume 10, Issue 2, June 2018, page no. 181 to 187 having ISSN No. 2511-2104.
- Ishleen Kaur, Gagandeep Singh Narula, Vishal Jain, “Differential Analysis of Token Metric and Object Oriented Metrics for Fault Prediction”, International Journal of Information Technology (BJIT), Vol. 9, No. 1, Issue 17, March, 2017, page no. 93-100 having ISSN No. 2511-2104.