International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

A Research on Credit Card Fraudulent Detection System

Devika S P, Nisarga K S, Gagana P Rao, Chandini S B, Rajkumar N

Abstract: ***Nowadays credit card is more popular among the private and public employees. By using the credit card, the users purchase the consumable durable products in online, also transferring the amount from one account to other. The fraudster is detecting the details of the behavior user transaction and doing the illegal activities with the card by phishing, Trojan virus, etc. The fraudulent may threaten the users on their sensitive information. In this paper, we have discussed various methods of detecting and controlling the fraudulent activities. This will be helpful to improve the security for card transaction in future.***

I. INTRODUCTION

Fraud is the critical activity that affects the economy and the nations. A credit card is a major problem that has become the most popular in online transaction and as well as daily purchase. This can happen in so many ways by losing the credit card or stolen by someone. Fraud describes any products or system as unauthorized use. The fraud uses the credit card information without compensation to obtain the devices and products. First, there was no fraud-related offense, then there was a theft act implemented in 1978, which entered into force on 15 January 2007. The primary distinction between fraud prevention and fraud detection, when fraud prevention succeeded, is the identification of fraud used to identify fraud at first comfort. Fraud is described by the use of unlawful products and the credit card bribery system is carried out by the information of credits and is acquired deliberately without charging for products. A fraud is achieved based on telecommunications, computer intrusion, money laundering, credit cards, medical and scientific detection son on [1]. Past few years in India, the annual increase was more than 40% have filled with hacking, credit cards, publication of absence contents and banking fraud. There were two kinds of credit card fraud categorized as physical fraud and virtual fraud. Over 160 companies said it was 12 times more internet or digital fraud than offline or physical fraud. Therefore, the primary objective was to identify behavioral analysis of this type of fraud. To solve this issue, monetary organization discovered a remedy for multiple fraud avoidance activities such as email checking system, loan card approval, and rule-based monitoring. The knowing cases of criminal behavior was to detect the card and it also causes in business sector mainly it due to identified and measured the crime instance individual research performed on criminal behavior, mainly it was happening for other policies and legal for protect the financial records of customers for avoid the financial domains in real datasets of legal and privacy activities [2]. Internet atmosphere was open for shopping in online criminals used some of the bad techniques to steal the sensitive information about card holders. The HMM based credit card fraud detection analyzed the fraudulent by transaction patterns on each card. The HMM based credit card fraud detection analyzed the fraudulent by transaction patterns on each card [3]. The high transactions majority dose not verifying by the investigators time and cost constraints evident this transaction endures unlabeled until customer uncover and discover the fraud report or until enough time was elapsed that considered has transaction non disputed genuinely. A fraudulent is known immediately and blocked if any card is found as a victim of a fraud [4]. The fraudster had many ways to illegally acquire the user card information such that phishing, Trojan virus etc. A fraudulent requires only the information of a card for transaction for online shopping to make fraud [5]. A fraudulent performance is caused more by financial motivation [6]. The fraud is happened if a retailer like Walmart handle a lot of larger range of credit card [7]. In order to acquire the individual unauthorized funds by using credit card for whom intended fraudulent card transaction activity the unauthorized person used other credit card information for its personal benefits without knowing the knowledge of card issuers and card holder it causes the illegal activity [8]. If an illegal activity is done by a user to get unauthorized funds from account of a credit card user for whom it was not meant is defined as fraudulent [10]. A fraud happens when a unknown user uses somebody's credit card for personal usage and even the issuing banks are unaware of the card being used [11]. The fraudulent of transaction reveals the interactions between entities and anomaly detection on features that detect details of fraud activities [12].

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Devika S P*, Department of Information Science Engineering, Vidyavardhaka College of Engineering, Mysuru, India. (devikasp5@gmail.com)
Nisarga K S, Department of Information Science Engineering, Vidyavardhaka College of Engineering, Mysuru, India. (nisargaks451@gmail.com)
Gagana P Rao, (gaganarao1597@gmail.com)
Chandini S B, Department of Information Science Engineering, Vidyavardhaka College of Engineering, Mysuru, India.
Rajkumar N, Department of Information Science Engineering, Vidyavardhaka College of Engineering, Mysuru, India.

The fraudulent quickly identifies the thresholds and take advantages and exploit the tools which remain static [13].

II. LITERATURE SURVEY

A novel approach was proposed about a credit card fraud detection and they represented three phases. In first phase they checked about the verification of card and user authentication, if first is cleared successfully then they check second phase. In second phase fuzzy clustering algorithms was applied to identify the patterns of credit cards based on their activities, according to normal problems the transaction was classified as three types, they are legitimate, suspicious and fraudulent. If a transaction is suspicious a neural network mechanism to determine the fraudulent activity by genuine user. This was used to merge clustering methods in identifying fake stochastic model-based operations while minimizing false alarm production. The stochastic models were used to analyze suggested device efficiency. Based on these findings, they suggest that mixed use of fuzzy clustering and teaching distinct methods to address kinds of real-world issues. The other learning techniques was used to compare and experiment are done in the future results [1]. It aims at presenting the job of researchers interested in data access and presenting an attitude to studies on fraud detection. Here some of the fields include accounts for mobile money online banking system credit card transactions and retail shops. They also contain some of these field-based studies and figure out the impossibility of comparing the job of popular public data collection to evaluate distinct outcomes. Here they introduce a fresh strategy to financial-based fraud detection using authority and mobility to simulate synthetic data for tests in order to prevent the constraints, privacy policies and client security applicable to actual information. Future financial fraud detection job focuses on mutual information collections containing various evil behaviors that will match and evaluate fresh method efficiency with current techniques. To accomplish this, researchers and the public needed to construct a conventional synthetic financial data set [2]. Proposed a method called novel fraud detection method and it composed four stages. In first stage they utilize the cardholder's transaction data and they divided each cardholder's into different teams as the behavior members in the same team are similar. And they proposed a strategy of window-sliding in each teams to aggregate the transaction. In second stage they extract the collection of some special behavioral patterns based on transaction for each cardholder's. In third stage they train set of classifier for each team based on all their behavioral patterns. In the last stage, they used classifiers to identify online fraud, if any fresh transactions were fake, the procedure for detecting the drift idea and its issues will be adopted. Here they proposed a technique for solving an adaptive capacity to adjust its parameters to cardholder's timely actions. These writers ' potential objective is to develop an employee regular time frame to enhance cheating prevention performance [3].

The real-world fraud detection system (FDS) consists of two main aspects [4]:

a. The supervised information was provided in the way of timely manner.
b. It was used to assess the fraud detection performance measures.

They present the three major contributions:

i. First they proposed the Formalization the problem of fraud detection which describes the operating condition of fraud detection systems.
ii. They designed a strategy of novel learning and asses them, it is addressed to class imbalance, verification latency and concept drift.
iii. Here they demonstrate the method drift and class unbalance in real-world.

On study of fraud detection is significant and interesting as the popularization is growing seriously in the online shopping transaction fraud detection to extract behavior profiles (BP's) based on user's transaction records. The Markov chain models were also used to represent the BP's of users. They proposed the logical behaviour models to display customer element documents depending on the total order-based model. At the same moment, they described the probability matrix for the state transition that captures customer activity. Later they built a BP to check an incoming order for all customers whether it was fraud or not. This paper's potential research concentrated on some machine learning techniques and account attribute standards in which the model can exactly customize the activities of the user [5]. Increasing of fraudulent activity day by day, also the online transaction became rapidly popular in the fraudsters. There are different frauds detection that uses the current systems across the business sector. The author developed a fraud detection system that can be useful for organizations. These fraud detection techniques and methods are used for detection. These fraud detection techniques help for the organizations to build a profiling their applicants. In which the system helps them to detect fraud detection application. By the use of the application, the user's feedback has the majority of successful overall of system, agreeing that this application was effectively and meaningful of fraud detection [6]. They developed a technique for 'Credit card fraud detection'. Most of the companies' security weakness was credit card fraud. To detect this there are multiple approaches. The author's used method mixes where the first techniques are purchasing behaviour depending on the sort of products that clients buy. The second technique is expenditure behaviour, detecting the highest quantity invested in this behavioral fraud. And the following technique was Markov model concealed, accounts of a specific customer are protected in this model and distinct situations of fraud are categorized together. Another Technique-Genetic algorithm used by the author was used to calculate the limit and accurate fraud. The primary objective of this study article was to investigate distinct solutions to the same issue and to recognize the customer and the fraud [7]. In today's world there is a very huge use of mobiles phones. While travelling there was a problem for carrying credit or debit card and also a huge cash that can be mishandled or get stolen. Therefore, extra care of credit/debit and cash has to be taken.

To overcame this problem, the technology has been implemented for the solution. In this paper they designed and introduced a 'NoCash' mobile application, this application which initiated payment of bill/invoice. NoCash is benefited and used by the merchants for payment purpose for customers.

The NoCash application of payment transaction need only mobile phones and no need of other application like NFC-Enabled Point of Sales (PoS) machines. The main objective of this paper was development of system which makes the transaction of payment easier and that reduce mishandle of customer's card and bring the huge cash for shopping and while travelling also. By use of this application the merchant's profit is increased and reduced in the fraud detection activities. This application was related to their unwanted expenditure [8].

This paper represents a Hybrid approach, named qualitative case-based reasoning and learning (QCBRL) [9]. It combines three AI methods,

i. Case-based reasoning
ii. Reinforcement learning
iii. Qualitative spatial reasoning

This system was designed for an agent that to learn, retrieve and reuse of qualitative cases in the domain of robot soccer which is applied in Half-field offence and has obtained promising results. In the future work they proposed humanoid robot soccer to analyze in the real domain results. This paper compares different classification algorithms, i.e., Transaction of data in credit card is fraudulent or not. It has supervised algorithms like Decision tree, random forest and support vector machines (svm) which corrects data and modify the accuracy table. This paper also focuses on the machine learning based on data mining. This data mining consists of three techniques which holds huge data sets where each one has its own merits and demerits based on its application. Here the three main algorithms discussed above has its own limitations and features. As the data is highly imbalanced oversampling of data is done here [10].

This paper suggests detection model to capture anomalous transactions where a fallback causes fail in the technology. Some of the classifiers evaluated when model creation yielded higher accuracy for random tree and j48 of value 94.32% and 93.50%. These 2 classifiers analyzed that j48 is more understanding in the data log transaction. This suggests a model based on behavior of cardholders to detect anomalous transactions. The Non-disclosure agreement(NDA) model details was not elaborated here between the bank and the proponent. Benefits of this detection system was to lesser the cost of the phone and SMS extremely by the banks. The SMS was sent to customers with detected transactions instead of sending SMS notifications [11]. Money laundering is known to be very serious illegal activities in financial fraud. This involves financial and complex networks of trade, at this situation it's difficult for detecting the fraud activities and which makes it difficult to detect the possibilities of fraud. In network, the complex network builds the entities features and trading or transaction. CoDetect, that leverage of network and feature information in financial fraud detection and also this CoDetect can simultaneously have the feature of detecting the financial fraud activities and the possibilities that fraud can be associated. CoDetect was a new proposed framework, it is a similarity graph-based matrix that perform the fraud detection. The nature of the financial fraud activities can be revealed by the new way of CoDetect. To identify the fraud, the framework provides a way of sparse matrix. By the help of CoDetect framework, not only the financial fraud supervision can be detected and also by suspicions method it can be able to trace the original fraud [12]. In today's world the fraud detection activity for national economics have become an important task and also in the international economics. The banks and the financial institutions they carry out the security of financial transaction. in this paper, the authors explore the location data and finding the business rules it can be easily deployed in fraud detection rule-based on practically. The authors first complied set of machines like, automated teller machine (ATM). By the number of mobile card owners, it is easily to divided business rules for detecting the anomalies. The paper say that the identity of users does not leave their place in the significant bulk of ATM users. There was an implemented possibility of detect the financial transaction location [13].

III. DISCUSSION & RESULTS

In particular, prior study on fraud detection concentrated on using private data collections to create statistical methods and exploiting the authority of information mining to find concealed trends or anomalies in economic information. However, owing to the absence of usually accessible information, it is difficult to evaluate and contrast some of these techniques. Lundin et al. suggested a technique for generating synthetic data for monitoring fraud detection in general, with no specific concentrate on economic information. Generation measures always begin with information compilation, accompanied by a data analysis that helps distinguish between user accounts. Lastly, with the identities specified, the ultimate phase is user, attacker and system modeling. The methodology is not so distinct with respect to the job checked. We must contribute, however, that the method is iterative and the findings help assess and validate the value of the synthetic data produced.

IV. CONCLUSION

Credit card fraudulent activities which are faced by the people is one of the major issues. Due to these fraudulent activities, many credit card users are losing their money and their sensitive information. In this paper, we have discussed the different fraudulent detection and controlling techniques in credit card and also it will be helpful to improve the security from the fraudsters in future to avoid the illegal activities.

REFERENCES

1. T. K. Behera and S. Panigrahi, "Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering Neural Network," in *2015 Second International Conference on Advances in Computing and Communication Engineering*, 2015, pp. 494–499.

2. E. A. Lopez-Rojas and S. Axelsson, "A review of computer simulation for fraud detection research in financial datasets," in *2016 Future Technologies Conference (FTC)*, 2016, pp. 932–935.
3. C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan, "Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3637–3647, Oct. 2018.
4. Andrea Dal Pozzolo, Giacomo Boracchi, Olivier Caelen, Cesare Alippi, and Gianluca Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 29, no. 8, pp. 3784–3797, Aug. 2018.
5. L. Zheng, G. Liu, C. Yan, and C. Jiang, "Transaction Fraud Detection Based on Total Order Relation and Behavior Diversity," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 3, pp. 796–806, Sep. 2018.
6. D. Al-Jumeily, A. Hussain, A. MacDermott, G. Seeckts, and J. Lunn, "Methods and techniques to support the development of fraud detection system," in *2015 International Conference on Systems, Signals and Image Processing (IWSSIP)*, 2015, pp. 224–227.
7. Ayushi Agrawal, Shiv Kumar, and Amit Kumar Mishra, "Implementation of Novel Approach for Credit Card Fraud Detection," in *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2015, pp. 1–4.
8. D. Pojee, S. Zulphekari, F. Rarh, and V. Shah, "Secure and quick NFC payment with data mining and intelligent fraud detection," in *2017 2nd International Conference on Communication and Electronics Systems (ICCES)*, 2017, pp. 148–152.
9. T. P. D. Homem, D. H. Perico, P. E. Santos, A. H. R. Costa, R. A. C. Bianchi, and R. L. de Mantaras, "A hybrid approach to learn, retrieve and reuse qualitative cases," in *2017 Latin American Robotics Symposium (LARS) and 2017 Brazilian Symposium on Robotics (SBR)*, 2017, pp. 1–6.
10. J. Vimala Devi and K. . Kavitha, "Fraud Detection in Credit Card Transactions by using Classification Algorithms," in *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, 2017, pp. 125–131.
11. J. R. D. Kho and L. A. Vea, "Credit card fraud detection based on transaction behavior," in *TENCON 2017 - 2017 IEEE Region 10 Conference*, 2017, pp. 1880–1884.
12. D. Huang, D. Mu, L. Yang, and X. Cai, "CoDetect: Financial Fraud Detection with Anomaly Feature Detection," *IEEE Access*, vol. 6, pp. 19161–19174, 2018.
13. A. Demiriz and B. Ekizoglu, "Using location aware business rules for preventing retail banking frauds," in *2015 First International Conference on Anti-Cybercrime (ICACC)*, 2015, pp. 1–6.