

A Hybrid Technique for Credit Card Fraud Detection

Shipra Rathore
Computer science & Engineering
LNCT-E, Bhopal

Megha Jain
Computer science & Engineering
LNCT-E, Bhopal

ABSTRACT

Credit card fraud occurs when user provide their information to the unknown persons or stolen by the unknown persons, that information can be used for unauthorized online purchase and some other situation. A technique is required to detect such fraud events. Many techniques are exist to detect such frauds. But these existing techniques are not efficient to provide better performance to detect such credit card fraud events. In this paper a hybrid technique which uses the properties of PGNN and Cost based model is presented which provides enhanced functionality to detect credit card frauds. The analysis of hybrid technique shows that the proposed technique provides an accurate and efficient way to detect credit card frauds.

Keywords

PGNN(Parallel Granular Neural Network), CBM(Cost Based Model), HMM(Hidden Markov Model), Credit Card Fraud Detection.

1. INTRODUCTION

Credit-card-fraud may be termed as an unauthenticated use of the system or the criminal activity by the use of the physical-card or information of card without informing the holder of card .The credit card is a small plastic card, which has been issued to the user like a system of payment. With fast growth in its number of credit card transactions, all fraudulent activities have been increased. The credit card might be physical or virtual. In some physical-card [1], the cardholder shows his card physically to few merchant for generating payment. To proceed fraudulent transactions for such purchase, an attacker grab the credit card. Secondly purchase, only little crucial information regarding card like as card number, expiration date, secure code and etc. are needed for making payment. Such purchases are generally committed over the Internet or on phone. To commit fraud in such type of purchases, a fraudster requires being aware of card details. Mostly, the genuine cardholder isn't familiar that somebody else has stolen their card information. In actual life, fraudulent transaction have been scattered through genuine transactions and the simple pattern matching Techniques aren't mostly satisfactory to search those frauds exactly. Outlier detection refer as data mining technique generally detected for fraud detection [2]. Outliers are the data points which are inconsistent with its reminder the dataset or deviate so much from some other observations so as to the arouse suspicion as they were produced through various approaches. Outlier-detection may be obtained through techniques like neural network, SOM, HMM etc.

1.1 Credit Card Fraud Detection Techniques

Credit card is being taken to get the goods and services through online and offline transaction mode too. This divided into two types: 1) physical card and 2) virtual card [3]. In

physical card [4] based purchase, the card holder suppose to the card at any merchant counter and merchant will then sweep that card the EMV (Euro pay, MasterCard and Visa) machine. Fraud transaction takes place in such mode, only when the card been stolen. It became hard to search fraud in such transaction. When the card holder does not aware of loss of their card and don't reports to the police or that card issuing company, that person will faces thee economical loses to issuing the authorities. Another approach of the purchasing such as Online, these transactions basically take place on telephone or internet and for making such transaction the user requires some crucial information of that credit card (such as credit card number, validity, CVV number, name of card holder). To attempt fraud transaction to buy goods and services, fraudster must be loaded with all details of the card only after that he/she can make transactions. Mostly, the cardholder might or may not aware that when or where that person can be seen or hide card information. To search such of fraud transaction, they have introduced a Hidden Markov Model which observes the spending profile of that card holder. An HMM observes the spending profile of every card holder and detect any type of discrepancy in such spending patterns.

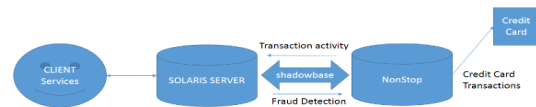


Figure 1.1: Over View of Credit Card Fraud Detection Process.

Fraud detection are been searched on the analyzing of any last transactions data which assist to make spending profile of the card holder. Every card holder possess unique pattern having information regarding level amount of the transactions, and information of the items purchased, merchant information, date of the transaction etc. It is the efficient method to counter fraud transaction by internet. When some deviation is observed from the available patterns of that card holder, then it can generate any alarm to that system for stopping the transaction.

Rest of the paper organizes as follows: II Literature Review, a brief over view over the techniques used for credit card fraud detection is presented in this section. III Problem Definition, brief description over the problems in credit card fraud detection techniques is presented in this section. IV Proposed Methodology, An overview over the proposed technique is presented in this section. V Experimental Setup, a description over the experimental scenario is presented in this section. VI



Result Analysis, a comparison of the results is presented in this section. VII Conclusion.

2. LITERATURE REVIEW

Salvatore J. Stolfo, Wei Fan, Wenke Lee [5] a distributed data mining system for credit card fraud detection is presented. In that system MADAM ID (Mining Audit Data for Automated Model for Intrusion Detection) is used to integrate cost based model with intrusion detection system to detect anomaly in credit card transactions a JAM project based model is used to provide better performance for fraud detection. In that technique cost model integrated with the data mining technique in distributed manner are used. Which provide an enhanced functionality to detect fraud in credit card transactions. But automated distribution of cost based trained data is not possible thus an automated distribution based technique is required to provide better performance to detect credit card frauds.

Mubeena Syeda, Yan-Qing Zbang and Yi Pan [6] a fast and efficient data mining technique for data mining and knowledge discovery of credit card fraud related data is presented. A parallel fuzzy neural network is used to train the dataset which contains data about credit card frauds in that technique multiple system works simultaneously to provide better performance to detect credit card frauds logs data of the various credit cards transactions are used to detect credit card frauds. But in that technique logs and updated logs are required to provide an enhanced credit card fraud detection mechanism which degrades the performance of the whole technique.

Philip K. Chan, Florida Institute of Technology Wei Fan, Andreas L. Prodromidis, and Salvatore J. Stolfo [7] a cost model based technique which uses data mining techniques in a distributed manner to provide an efficient mechanism to detect credit card frauds. In that technique dataset divided into various subsets and then data mining techniques are applied over these subsets to provide to generate classifiers for these subsets. In that way Meta classifiers are generated which provides an enhanced functionality to detect frauds in credit card transactions.

3. PROBLEM DEFINITION

Credit card frauds occurs when any intruder or hacker stolen your card or user provide their credit card details to the unknown person. That causes act of unauthorized charges over your credit card means unknown person purchasing things on your credit card without taking your permission. There are various type of attacks like identity theft, in that user's identity can be used by the intruders to get new credit card. Credit card skimming can be performed to get unauthorized access for the by getting user's credit card information by making fake copies of the credit cards and use these credit card details to perform attacks over these cards. To detect such credit card fraud events there are various techniques are presented by the researchers. HMM (Hidden Markov Model), in that technique uses system logs of the persons, if any person detected as a fraud then that person restricted for any further transactions. Parallel Granular Neural Network (PGNN), it provides an efficient technique to extract data from the database also increases the speed of data extraction process. A distributed cost based model is presented in that technique a parallel and data learning technique is presented which provides an efficient technique for fraud detection.

But these techniques suffers some defects like, cost based model training based on the defined cost is not automated which degrades the performance of the technique, in HMM, a person's information always treated as a fraud if it once detected as a fraud which reduces flexibility of the system. In PGNN a dependency on the log data is poses which degrades the performance of the technique.

4. PROPOSED METHODOLOGY

In existing technique PGNN (parallel granular neural network) and cost based model are generally used for the credit card fraud detection. In PGNN a Fuzzy neural network based technique is presented. In that technique a distributed mechanism is presented to provide an efficient mechanism for credit card fraud detection. In that technique log data of different credit card transactions is used, to detect credit card frauds. But in that technique updated logs are required to detect credit card frauds. In cost based model data mining techniques over the large scale dataset which contains data about various credit card fraud events is presented. In that large dataset in divided into small subsets and then meta-classifiers are generated by the use of data mining technique and a cost model is integrated with this technique to provide an enhanced functionality to provide better performance for credit card fraud detection. But there no automated distribution of the data is provided which degrades the performance of the whole technique.

A new hybrid technique which poses the properties of cost based model and parallel granular neural network to provide an enhanced credit card fraud detection mechanism is presented in this paper. Algorithm for the proposed technique presented below.

Proposed algorithm

In this algorithm, U represents user, C represents card, D represents details.

1. Start
2. U registers himself to the shopping portal SP with credentials CR
3. login into SP
 - a. if(first login)
 - i. Prompt user to set Security Questions SQ
 - ii. Prompt user to set card details D
 - iii. Prompt to login again
 - b. Else
 - i. Check if(IP used >5)
 1. Treat IP as Familiar
 2. Put question sets 1
 - ii. Else if(IP used <=5 && IP used >=3)
 1. Treat IP as Friendly
 2. Put question sets 2
 - iii. Else
 1. Treat IP as public

2. Put question sets 3
- iv. If(user gives correct answers to all sets)
 1. Allow to login and Shopping
- v. Else block the user for that IP as PGNN
4. Shopping starts and go for transaction
 - a. If(Transaction Amount TA>Limit L)

Block the transaction as CBM

Else if (Product quantities PQts >LQts)

Block the transaction as CBC

Else if (new TA > Average Limit AL)

Block the transaction

Else

Proceed to transaction

Prompt to enter card details

If (true)

Log Transaction Successful

Else

Log transaction as blocked
5. Ends here.

5. EXPERIMENTAL SETUP

To implement proposed technique a JSP (Java Server Page) a server side programming technology which used to provide functionality to develop dynamic and platform independent web applications. In that technique a system which contains 2GB RAM, Intel core processor, 80GB HDD disk.

For implementation purpose a NETBEANS IDE simulator is used. Which provides a development environment to develop various projects in languages like Java, PHP, JSP, C, C++ etc. existing techniques like CBS, PGNN and proposed hybrid technique which uses features of both the technique to provide enhanced functionality to detect fraud events in credit card transactions.

6. RESULT ANALYSIS

A comparison of the results generated by the techniques is presented in this section, which contains experimental results for the existing and proposed technique. A statistical and graphical analysis of the results, over the parameters called Precision, Recall, and F-measure is presented.

Evaluation parameters

Precision:-
$$\frac{\text{No.of relevant document retrieved}}{\text{Total document retrieved from the file}}$$

Recall:-
$$\frac{\text{No.of relevant document retrieved}}{\text{Total no of relevant document in the file}}$$

F-measure:-
$$2 \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

6.1 Statistical analysis of the Results

A statistical analysis of the results is presented in Table 6.1, which contains numerical data of the experimental results is presented. That statistical analysis shows that proposed technique provides an efficient mechanism to detect credit card frauds. To evaluate the performance of the technique Precision, Recall, F-measure are used as evaluation parameters. That analysis shows that proposed technique provides better precision to detect credit card frauds as compare to the existing technique.

Table 6.1: Statistical Comparison of Results

Technique	Precision (%)	Recall(%)	F-measure
Cost based Model	91.41	1.04	2.06
PGNN	56.09	43.90	49.25
CBC&PGNN	98.95	8.58	15.69

6.2 Graphical Analysis of the Results.

A graphical comparison of the result is presented in Figure 6.1, which shows a graphical analysis of the results. That analysis shows, proposed technique provides better performance as compare to the existing techniques.

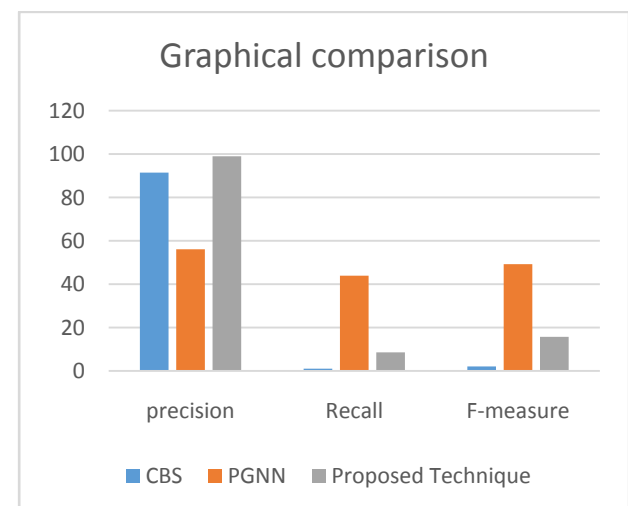


Figure 6.1: Graphical Comparison of the Results.

7. CONCLUSION

A hybrid technique to detect credit card frauds is presented in this paper. That technique uses the properties of PGNN and CBM to provide an efficient fraud detection technique. And overcome the limitations of the existing technique. A brief description over the proposed technique is presented in section



IV Proposed Methodology. And comparison analysis of the results is presented in VI, result and analysis section. That results analysis shows proposed technique provides an enhanced functionality to detect credit card frauds. To evaluate the performance of the proposed technique Precision, Recall and F-measures are used as evaluation parameters. That analysis shows proposed technique provides better precision, Recall, and F-measure.

For future work enhanced security mechanism can be used, in which password and password entering behavior of the user is used to teach the authentication for any transaction.

8. REFERENCES

- [1] Xu Wei, and Liu Yuan, "An Optimized SVM Model for Detection of Fraudulent Online Credit Card Transactions," International Conference on Management of e-Commerce and e-Government, IEEE, 2012.
- [2] Vaishali "Fraud Detection in Credit Card by Clustering Approach", International Journal of Computer Applications (0975 – 8887) Volume 98– No.3, July 2014.
- [3] K. Zakir Hussain, M. Durairaj, and G. Rabia lahani Farzana, "Criminal behaviour analysis by using data mining techniques," IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.
- [4] Chung-Hsien Yu, Max W. Ward, Melissa Morabito, and Wei Ding," Crime Forecasting Using Data Mining Techniques," 11th IEEE International Conference on Data Mining Workshops, 2011.
- [5] Salvatore J. Stolfo, Wei Fan, Wenke Lee "Cost-based Modeling for Fraud and Intrusion Detection: Results from the JAM Project" IEEE, 2000.
- [6] Mubeena Syeda, Yan-Qing Zbang and Yi Pan, Parallel Granular Neural Networks for Fast Credit Card Fraud Detection, IEEE, 2002.
- [7] Philip K. Chan, Florida Institute of Technology Wei Fan, Andreas L. Prodromidis, and Salvatore J. Stolfo, Columbia University "Distributed Data Mining in Credit Card Fraud Detection" November/December 1999.
- [8] C. Phua , V. Lee, K. Smith, and R. Gayler, "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," <http://www.bsys.monash.edu.au/people/cphua/>, Mar. 2007.
- [9] E. Aleskerov, B. Freisleben, and B. Rao, "CARDWATCH: A Neural Network Based Database Mining System for Credit Card Fraud Detection," Proc. IEEE/IAFE: Computational Intelligence for Financial Eng., 1997.
- [10] Ms. Pratiksha L. Meshram, Prof. TarunYenganti, "Credit and ATM Card Fraud Prevention Using Multiple Cryptographic Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013.
- [11] SahilHak, Suraj Singh, Varun Purohit "Credit Card Fraud Detection Using Advanced Combination Heuristic and Bayes' Theorem", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 4, April 2015.
- [12] Abhinav Srivastava , Amlan Kundu, Shamik Sural and Arun K. Majumdar, IEEE "Credit Card Fraud Detection Using Hidden Markov Model" Ieee Transactions On Dependable And Secure Computing, January-March 2008.
- [13] Rinky D. Patel, Dheeraj Kumar Singh, "Credit Card Fraud Detection & Prevention of Fraud Using Genetic Algorithm", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.