Volume 9, Special Issue No. 1, February 2018

ISBN: 978-93-5300-455-2

International Journal of Advanced Research in Computer Science
(ISSN: 0976-5697)

REVIEW ARTICLE

ICRACC 2018
(23rd–24th February 2018)

Available Online at www.ijarcs.info

CREDIT CARD FRAUD RECOGNITION USING DATA MINING TECHNIQUES

R.Akila, MCA, M.Phil.
Assistant Professor in Computer Science
Guru Nanak College
Velachery- Chennai, India
akila.akilarchp@gmail.com

M.Bhuvaneswari, ME.
Assistant Professor in Computer Science
Guru Nanak College
Velachery- Chennai, India
me.bhuvaneswari@gmail.com

ABSTRACT

In recent world most of the people, small and large scale originations are moving their daily business activity to online and providing customers services via internet. Credit Card (CC) payment is playing major role in the business activity but same time CC fraud is one of the major concern and issues in online transaction. In recent year CC fraud frauds are increased in day to day activity. The Main reason is most of the customers are using CC for all kind of payment. So the aim of this paper is to identify the different types of CC frauds and review the alternative techniques to detect the CC frauds. So satisfying the customers all originations are moving to secured transaction for customer to make payment for purchasing goods. This study will help to understand the CC fraud and type of methodology can be used to detect the CC fraud. This study will help to understand the CC fraud and type of methodology used to detect the CC fraud.

1. INTRODUCTION

The internet becomes most popular mode of payment for online transaction. Banking system provides e-cash, e commerce and e-services improving for online transaction. This payment facilitates the acceptance of electronic payment for online transactions also known as a sample of Electronic Data Interchange (EDI), e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping. Now a day tremendous volume and value increase in credit card transactions and same time credit card frauds also increasing day by day.

1.1CREDIT CARD FRAUD IN BANKING

The CC is one of the most conventional ways of online transaction. It allows cardholders to purchase goods and services from the shopping websites or from the market. In case of risk of fraud transaction using CC has also been increasing. CC fraud detection is one of the ethical issues in the credit card companies, banks and financial Institutes. CC fraud system to find the fraud and remove duplicate from CC fraud application. Fraud can be identified two ways in banking sector. First validate exact match between duplicate data with fraud data base and compare duplicate data with fraud data base approximately with slightly altered spellings. This paper discuss with each successful fraud pattern to find the fraud with short time period.

2. RECOMMENDED SYSTEM

Fraud detection is one of the main and important goalsof this paper. Generally security based layer is proposed system for fraud detection in data mining. In security based layers CD and SD techniques are mainly used to find the fraud detection in real time.

1) Communal Detection (CD)
2) Spike Detection (SD)

CD technique is fixed set of attribute to find the fraud. It will compare with default list and match attribute with exact value. SD technique is same as CD but it will not match with exact value and compare with variable attributes.

2.1.Calculate CD Score

This is the method most of the places are using to detect the fraud in basic level. If any new application submitted from users or customer first it is taken as ainput to CD layer. CD layer compared with white list data provide the suspicious score, based on score it is decided as fraud or not. Basically CD layer used to compare with common relationship between new application and default list. If five or more attributes are matched the CD assign less number of suspicious score. If CD gives fewer score then it is considered as legal transaction and new application details added to white list. Suppose it gives more suspicious score then this transaction may be fraud. Even though if give less score new application data can be passed as a input to SD layer.

2.2 Calculate SD Score

This is another approach to find the fraud detection. SD layer taken input from CD layer output. SD algorithm have different step to find the suspicious score. Single step to find the scaled count value when compare with new application data.If single value similarity and time difference exceed then it is considered as fraud. Another step calculates current value score based on calculated weighted score. For example match with any one of the unique id, if it is matched then it gives more suspicious score and declare as fraud and reject the new application else added in the white list.

3. ARCHITECTURE DESIGN AND OVERVIEW

The architecture diagram represents complete flow of fraud detection system. Here first collected all input data from user or customers and all input data passed to fraud detection section to find the fraud based on suspicious score. Then different type algorithms and techniques such as case base reasoning, retrieval data methods, and diagnose the data. Finally find the data as fraud or not based on above techniques. If input data detected as fraud then details are stored to blocked list else if data is legal relationship then it is stored in original database and it is considered as genuine transaction.

3.1 Fraud Detection

Fraud detection system has used two different algorithms such as CD and SD to find the fraud. CD algorithms is purely relationship oriented and applied attributes to find the suspicious score. CD techniques called as adaptive based approach. Before proceed the SD it is required to reinforce that CD and find real relationship to reduce the score. SD is not white list oriented approach it is attributed oriented process.

3.2 Fraud Verification

All new user details are taken to this section to identify the fraud, in the process applied two algorithms (CD & SD)and verified input data to make efficient credit card transaction. If the data is original it is proceed to further transaction else it is rejected the transaction and its added to black list. Next time easily find the fraud in first level without applied the CD & SD algorithm.

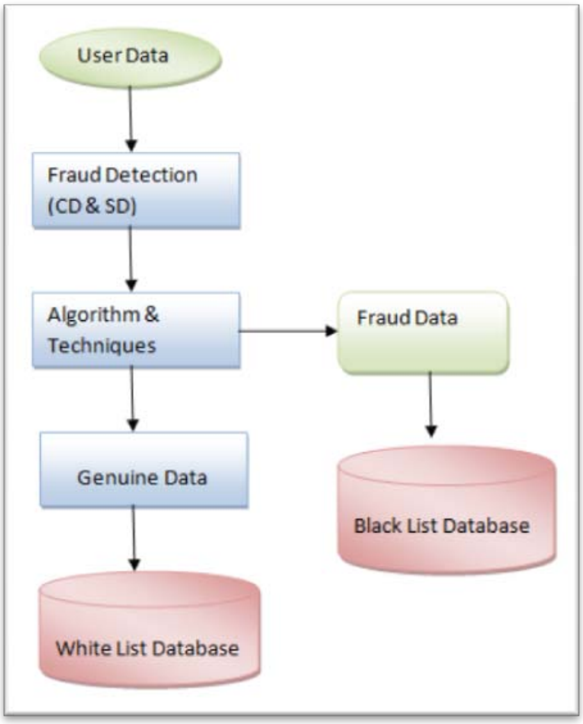

Fig1:System Architecture Diagram

4. BIOMETRICS PROCESS

Now a day’s biometrics techniques is playing major role in security system. Biometrics based security is really challenged to fraudster.In the biometrics finger print authentication is one the way to stop the fraud. In this process electronic finger print scanners are scanned the finger print and stored in digital format. Digital format pictures are then processed in to digital template with unique value. Using this system only authorizes users or customers can make transaction. All the scanned digital templates are stored in biometric database.

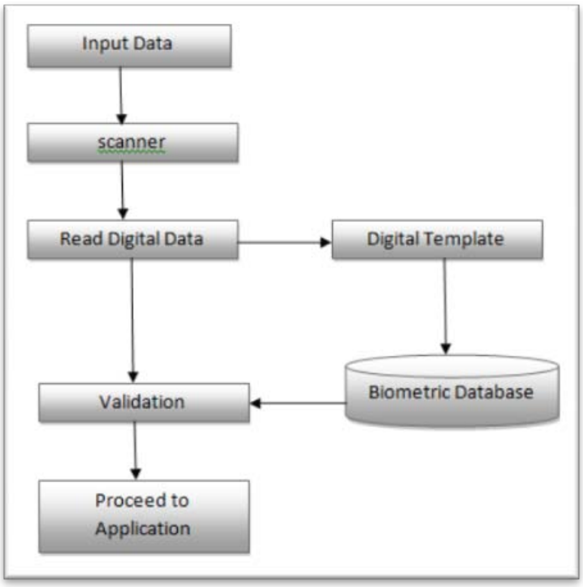

Fig. 2: Example for Biometrics Pattern Comparison and Retrieval

5. CONCLUSION AND FUTURE WORK

Data mining is a recognized platform fordefining rules, analyzing and predicting the data from large amount of data base.The aim of this paper is Identity the frauds in online transaction. This system detects the fraud detection in online system and it is used to avoid theduplicates application entry while applying new credit card.The CD and SD algorithm used to detect the fraud from multipleapplicants. In this proposed system combine with theexisting algorithm SD and CD and this system is well organized with more efficient and secure. Fraud verification layer is used to throw the fraudulent activity immediately because all black list data stored in the data base. Limited time period is required to identify the fraud using this proposed system. This technique can apply different industry to find the fraud activity.

6. REFERENCES

[1] ALKA HERENJ,SUSHMITA MISHRA, Secure Mechanism for credit card transaction fraud detection system issue 2,February 2013

[2] Richard J.Boltan and David J.Hand, “Statistical Fraud Detection”, pp.1-54, 2002.

[3] ID Analytics, “ID Score-Risk: Gain Greater Visibility

[4] V.Dhecpa and Dr. RDhanapal, Analysis of credit-card frauddetection methods', International Journal of Recent Trendsin Engineering (2009), vol, 2. No. 3, pp.126-128.

[5] ID Analytics,ID Score-Risk: Gain Greater Visibility into Individual Identity Risk,”Unpublished, 2008.