**International Journal of Management, IT & Engineering**
Vol. 8 Issue 11, November 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

# DATA MINING APPLICATION FOR CREDIT CARD FRAUD DETECTION SYSTEM

**S.PADMA PRIYA** [*]

**Dr.D.USHA** [**]

**Abstract**

In recent days most of the small and large originations have moved their daily businesses to online and provide the services to customers using internet. Credit Card (CC) fraud is one of the major issues in online transaction. In recent year CC fraud or no card frauds are increased in day to day activity. The main reason is most of the customers are using CC for their all kind of payment. So the aim of this paper is to identify the different types of CC fraud and to review the alternative techniques to detect the CC frauds. Therefore secured transaction is required for CC holders when consuming their CC to make electronic payment for purchasing goods. This study different types of fraudsters that commit CC fraud and the type of techniques used by these cyber fraudsters to commit fraud on the internet is discussed

[*] **Assistant professor & Head, Department of Information Technology, Cumbum**

[**] **Assistant professor & Head, Department of Computer Science, Mother Teresa Women's University, Kodaikanal**

## 1. Introduction

CC fraud can be defined as the fraudulent use of a credit card account through the theft of the account holder's card number, card details and personal information, through a wide variety of methods in order to perform illegal transactions from the compromised account. Fraud can also define as criminal activity or adjunct to identity theft. Due to the expansion of modern technology, the payment mode of individual has been changed significantly. The use of online payment mode like Online Banking, Debit Card, Credit Card etc. Now a day tremendous volume and value increase in credit card transactions. CC fraud begins with the theft of the physical card or with the compromise of data linked with the account, including the card account number or other details that would regularly and essentially be available to a merchant during a genuine transaction. Fraud detection and software that analyzes the patterns or blue print and unusual behaviour as well as individual transactions in order to flag likely fraud. Profiles include such information as IP address.

## 2. DATA MINING: AN OVERVIEW

### 2.1 Definition

Data mining is defined as the extraction of hidden prognostic info from giant databases. In general, data mining (sometimes called data or knowledge discovery) is that the method of analysing knowledge from completely different views and summarizing it into helpful info. This info will be accustomed to increase profits, scores prices, or both. Data mining code is one amongst variety of analytical tools for analysing knowledge. It permits users to investigate knowledge from different dimensions or angles or categorize it, and summarize the relationships identified. Technically, data mining is the method of finding correlations or patterns among dozens of fields in giant relative databases

### 2.2. The evolution of data mining

Data mining is a comparatively different term, the technology is not. Data mining is product or application improvement process and the result of a long research. Data mining is the computational process of exploring and uncovering patterns in large data sets. It is a subfield of applied science which mixes several techniques from statistics, knowledge science, information theory and machine learning.

## 3. CYBER CREDIT- CARD FRAUDSTERS

### 3.1 CNP (Card Not Present) Fraud

They are fraudsters with very little or no this may be done through phone, mail or web. It means someone uses your card while not really being in physical management of it.Additional and additional and sometimes, merchants wouldforce the cardboard verification code, creating CNP fraud slightly harder, however if a fraudster will get your account variety, they in all probability recognize that variety too.

### 3.2 Electronic or Manual Credit Card Imprints

A second style of master card fraud is intimate through mastercard imprints this suggeststhat someone

skims info that's placed on the magnetic strip of the cardboard. This is often then wont to encipher a faux card or to complete dishonorable transactions.

### 3.3 Mail Non-Receipt Card Fraud

This type of fraud is additionally referred to as ne'er received issue or intercepts fraud. during this case, you were expecting a brand new card or replacement one and a criminal is ready to intercept these. The criminal can then register the cardboard and that they can use it to create purchases and additional.

## 4. TECHNIQUES FOR CREDIT-CARD INFORMATION STEALING BY CYBER CREDIT-CARD FRAUDSTERS

### 4.1 Credit-card fraud generator software

Credit card generators don't seem to be machines in their title. They’re merely code programs that use totally different mastercard company’s variety generating rules to form numerically valid mastercard numbers. Their primary use is in mastercard fraud, though there are some legitimate uses, like testing e-commerce sites to make sure that the numbers method through properly mastercard numbers carries with it a prefix distinguishing the precise style of card, like american categorical, MasterCard or Visa, followed by the quantity sequences of the provision monetary establishments, reports CPAFinder.com. mastercard generators use differing types of specialised code to form numbers matching this pattern. Ironically, the method of generating the required variety sequences involves the utilization of associate formula that developers originally designed to stay store clerks from inputting inaccurate numbers into mastercard machines.

### 4.2 Spyware, Site-cloning and False Merchant sites

Site cloning is where fraudsters clone a complete website or simply the pages from that you place your order'. Customers don't have any reason to believe square measure they're not coping with the corporate

that they needed to get merchandise or services from as a result of the pages that they're viewing are similar to those of the $64000 website. The individual can fill in associate form, along with his or her details. These can embrace name, address and full card details. The cloned or spoofed website can receive these details and send the client a receipt of the dealings via email even as the $64000 Company would. The patron suspects nothing, while the fraudsters have all the main points they have to commit mastercard fraud. These sites usually provide the client an especially low cost service, like the supply of hard core porno at a considerably
cheaper price than rival sites

### 4.3 CC/CVV2 shopping websites

Credit-card fraudsters with no professional computer skills can buy hacked credit-card information on these websites to use for fake/illegal (because of lying and stealing) electronic payment for some products that are bought and sold) and services on the internet.

### 4.4 Physical stolen credit-card information

Card are going to be taken from your possession, either through stealing or as a result of you lost it. The criminals WHO get their hands on that can then use it to create payments. It’s tough to try and do this through machines, as they'll need a PIN. However, it's simple enough to use a found or purloined card to create on-line purchases.

## 5. METHODOLOGY

### 5.1 Credit Card Fraud detection model

There is a fixed pattern to how credit-card owners consume their credit-card on the internet. This fixed pattern can be drawn from legal/real and true regular activities of the credit-card owner for the past one or two years on its credit-card; the regular (person who sells things) websites the credit-card owner regularly makes electronic payment for products (that are bought and sold) and services, the (related to where mountains, rivers, cities, etc., are located) location where past legal/real and true transactions have been made, the (related to where mountains, rivers, cities, etc., are located) location where products (that are bought and sold) have been shipped to by the credit-card owner, the email address and phone number regularly used by the credit card owner for notice/communication. Using the Nerve-related/brain-related Network technology, the computer-program or software can be trained with this fixed pattern to use it as knowledge in classifying a (happening or viewable immediately, without any delay) transaction as fake/illegal (because of lying and stealing) or legal/real and true transaction. The behavioural pattern in the current transaction differs with the learned pattern of the original credit-card owner, the system will continue to match the pattern of the current transaction if it's almost the same with past computer credit-card illegal dishonesty/stealing (by lying) transactions. If the system returns false (of (existence of two things that aren't equal in size, power, color, etc.) patterns between the current transaction and past illegal dishonesty /stealing (by lying) transactions) then the system classifies the transaction as suspicious illegal dishonesty/stealing (by lying) but if true, then the system will classify the transaction as illegal illegal dishonesty /stealing (by lying) transaction.

### 5.2 Geolocation of real-time transaction

The geolocation technology provides the complete and total (related to where mountains, rivers, cities, etc., are located) location of an internet-connected computer by its IP address. An IP address is a (like nothing else in the world) network identifier issued by an Internet Service Provider to a computer-user every time they are logged on to the Internet. This Data mining computer program is trained with IP-addresses (City and Country location being formatted from the IP-addresses) of internet-connected-computers the credit-card owner has used in the past one or two years legal/real and true transaction on its credit-card. This is a good (machine /method

/way) to train Nerve-related/brain-related Networks for computer credit-card illegal dishonesty/stealing (by lying) detection because in training Nerve-related/brain-related Networks with the City and Country locations formatted from IP-addresses where the credit-card owner has regularly made legal/real and true transactions from for the past one or two years, Nerve-related/brain-related Networks can know if the internet-connected-computer of the current transaction behaves in pattern like the internet-connected computers the credit-card owner has regularly made his past one or two years legal/real and true credit-card transactions. While this is a very good anti-illegal dishonesty/stealing (by lying) (machine/method/way) and useful for watching and following criminals who cheat people, the IP addresses can also be changed using (related to being a substitute for someone or something) servers. Unnamed substitute servers allow Internet users to hide their actual IP address and run their computers behind a fake IP address of their desired area. The main purpose using a (related to being a substitute for someone or something) server is to remain unnamed or to avoid being detected. Fraudsters hide themselves behind unnamed substitute servers to do/perform credit-card illegal dishonesty /stealing (by lying) on the internet. This Data mining application automatically flags for suspicious illegal dishonesty/stealing (by lying) if a proxy-server is detected in a transaction.

### 5.3 Email address and Phone number

When a credit-card is issued to an individual by a credit-card issuer or company, an email address

or phone number from the person is registered with the credit card so that the individual can receive notice /communication via telephone or email of any transaction that's been made on their credit -card. For this reason, fraudsters do use different email-addresses and phone numbers when doing/performing computer illegal dishonesty/stealing (by lying) on credit cards. Although, It is important to take note that the computer fraudsters do not only use email-addresses registered with free domains (like Yahoo, Google or Hotmail), but also they do pay to get registered email-addresses with non-free domains. Therefore, in this data mining computer program, Nerve-related/brain-related Networks will be trained with the email addresses and phone number the credit-card owner has used in past one or two years internet credit-card transactions.

### 5.4 Shipping address

Although it is not unusual/amazing for people sending gifts to others to request different shipping address. It is very hard to retrieve products (that are bought and sold) or understand /capture fraudsters once the products (that are bought and sold) have left the country of residence of the original credit-card owner. Fraudsters will possibly not send products (that are bought and sold) to the legal/real and true cardholder's billing-address. But it is possible that credit-card owners will send products (that are bought and sold) to legal/real and true shipping address different to their billing address. Therefore, in this data mining application, Nerve-related/brain-related Networks will be trained with Shipping addresses and oversee orders used by the credit-card owner in past one or two year’s transactions

### 5.5 Merchants’ websites, regular good and services purchased in past credit cardholder’s transactions

Nerve-related/brain-related Networks will be trained with the (person who sells things) websites the credit-card owner has regularly visited and the type of products (that are bought and sold) and services they have regularly (bought something for money) on its credit-card for the past 1 or two years. Nerve-related/brain-related Networks will be trained with the cost range of products (that are bought and sold) and services (bought something for money) in the past one or two years transactions of the credit cardholder's credit card.

## 6. CONCLUSIONS

In this paper, a data mining computer program has been modeled as a subsystem which can be used with software systems and applications in banks to detect credit-illegal dishonesty/stealing (by lying) in a transaction on the internet. This Data mining (online or paper form that asks for a job, money, admission, etc.) accepts input formatted on a pattern on which a transaction is being did/done/completed and matches it with the credit-card holder's patterns of its credit-card online consumptions it's been trained with to classify a (happening or viewable immediately, without any delay) transaction as real and true, suspicious illegal dishonesty /stealing (by lying) or illegal transaction. The data mining application modeled in this paper uses the (weird, unexpected thing) detection set of computer instructions of the Nerve-related/brain-related Networks to detect illegal dishonesty/stealing (by lying) in a (happening or viewable immediately, without any delay) transactions and it not likely to experience/likely to get errors because of its classification of Transactions (legal/real and true, Suspicious Illegal dishonesty/stealing (by lying) and illegal). In the case of the suspicious illegal dishonesty /stealing (by lying) classification, the bank using the system can (ask lots of questions about/try to find the truth about) further by calling the credit-card owner (related to /looking at/thinking about) the suspicious fake/illegal (because of lying and stealing) transaction.

## REFERENCES

[1] T. F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, P. G. Neumann, H. S. Javitz, A. Valdes, and T. D. Garvey. AReal-Time Intrusion Detection Expert System (IDES) - Final Technical Report. Technical report, SRI Computer Science Laboratory, SRI International, Menlo Park, CA, Feb. 1992.

[2] Dr. Yashpal Singh and Singh Chauhan, Neural networks in data mining. Journal of Theoretical and Applied Information Technology (2005-2009), vol, 5, no. 6. pp. 37-42.

[3] Khyati Chaudhary, Jyoti Yadav and Bhawna Mallick, A review of fraud detection techniques: credit-card, International Journal of Computer Applications (2012), vol. 45, no. I, pp.39-44

[4] Cybercrime: protecting against the growing threat Global Economic Crime Survey – PWC Global Economic. [ONLINE]. Available at: http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf. [Accessed 12 December 2012].

[5] S. Rosset, U. Murad., E. Neumann, Y. Idan, and G. Pinkas. Discovery of fraud rules for telecommunicationslchallenges and solutions. In *Proceedings of the fifth ACM SlGKDDinternational conference on Knowledge discovery and data mining*, pages 409-413. ACM Press, 1999