Credit Card Fraud Detection & Prevention – A Survey

Surbhi Gupta
PG Student
Department of Computer Science & Engineering
JSS Academy of Technical Education, Noida, Uttar Pradesh, India

Mrs. Nitima Malsa
Assistant Professor
Department of Computer Science & Engineering
JSS Academy of Technical Education, Noida, Uttar Pradesh, India

Mr. Vimal Gupta
Assistant Professor
Department of Computer Science & Engineering
JSS Academy of Technical Education, Noida, Uttar Pradesh, India

Abstract

A credit card is a convenient tool that allows you to buy items now and pay for them later. Banking Sector involves a lot of transactions for their day to day operation and they have now realized that their main disquietude is how to detect fraud as early as possible. The credit card has become the most popular mode of payment for both online as well as regular purchase. Credit card frauds are increasing day by day regardless of various techniques developed for its detection. Fraud detection systems have become essential for all credit card issuing banks to minimize their losses. The most commonly used fraud detection methods are Artificial Immune System (AIS), Hidden Markov Model (HMM), Neural Network, Genetic Algorithms, Decision Tree and Support Vector Machine (SVM). These techniques can be used alone or in collaboration using ensemble or meta-learning techniques to build classifiers. The main objective of this paper is to review methodology of different detection methods based on credit card in terms of Parameter like Speed of detection, Accuracy and cost the comparison of mentioned approaches based on survey. This paper presents a survey of various techniques used in credit card fraud detection and prevention.

Keywords: Credit Card, Credit Card Fraud, Fraud Detection Techniques, Fraud Prevention Techniques

I. Introduction

A credit card is an instrument which provides instantaneous credit facilities to its holder to avail a variety of goods and services at the merchant outlet. It is made of plastic and hence popularly called as "plastic money".

A. *Parties to a Credit Card:*

There are three parties to credit card

- The issuer
- The cardholder
- The member establishments[16]

While performing online transaction using a credit card issued by bank, the transaction may be either online purchase or transfer. The online purchase can be done using the credit or debit card issued by the bank or the card based purchase can be categorized into two types Physical Card and Virtual Card.

B. *Physical Card Based Purchase*

The card holder contains a card and in order to purchase a good or make any transaction the card holder should carry the card.

C. *Virtual Card Based Purchase*

The card holder need not carry the card; just a few details about the card are enough to carry out the transactions. It is generally done in online shopping. Only some important information about a card (card number, expiration date, secure code) is required to make the payment.

Credit card work flow diagram is illustrated in Figure 1.1 Cardholder provides credit card information to merchant for purchase. Merchant sends credit card information to payment processor for payment authorization. Credit card organization clearing and settlement merchant acquirer and issuer bank.

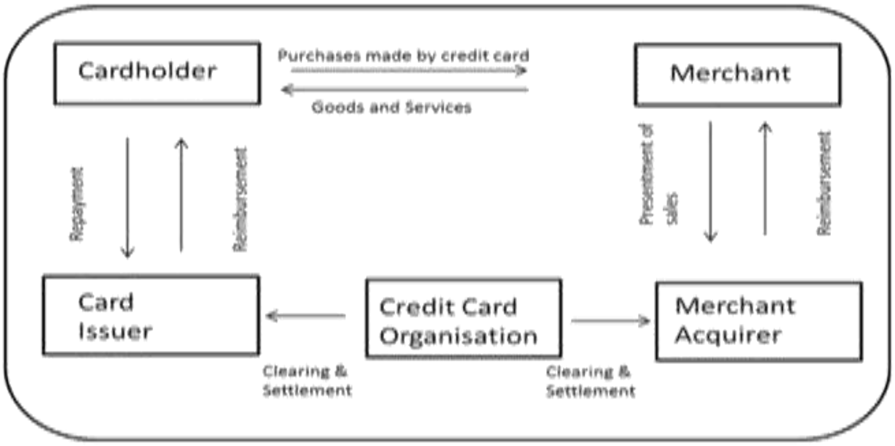

Fig. 1.1: Credit card work flow [21]

II. CYBERCRIME

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).The first recorded cybercrime took place in 1820. Cybercriminals may use computer technology to access personal information, business trade secrets, or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.

A. *Classification of Cybercrime*

There are two classes of cybercrimes

1) *Computer Assisted Cybercrimes:*

Computer is instrumental in committing the crime. Selling nonexistent, defective, substandard or counterfeit goods, theft of credit card, bank fraud, fake stock shares, intellectual property offences including unauthorized sharing of the copy righted content of movies, music, digitized books.

2) *Computer Oriented Cybercrimes:*

Computer is the target of the crime.

- Malicious Software: viruses, Trojans (which corrupt server)
- Cyber terrorism
- Hacking
- Child pornography
- Violent and extreme pornography
- Internet inspired homicides and suicides
- Worm: Self-replicating programmes spread autonomously without a carrier.
- Ex- Via mail, scanning remote systems.
- Trojan: installed during downloading some programme as a background activity causing irreparable damage.

3) *Credit card fraud*

Credit Card Fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a Credit card or debit card, as a fraudulent source of funds.

4) *Types of frauds-*

Credit card fraud has been divided into two types: Offline fraud and On-line fraud.

- Offline fraud is committed by using a stolen physical card at call center or any other place.
- Online-fraud is committed via internet, phone, shopping, web, or in absence of card holder.

Bankruptcy fraud
Theft fraud/ Counterfeit fraud
Application fraud
Behavioral fraud

Figure 1.2 shows types of fraud. Green are counterfeit and 39% fraud . Light green are card not present and 23 % fraud. Blue are 28% lost/ stolen fraud. Light blue are 6% Intercepted in mail fraud. Sky blue are 2% Fraudulent Application fraud. C-green are 2% others.

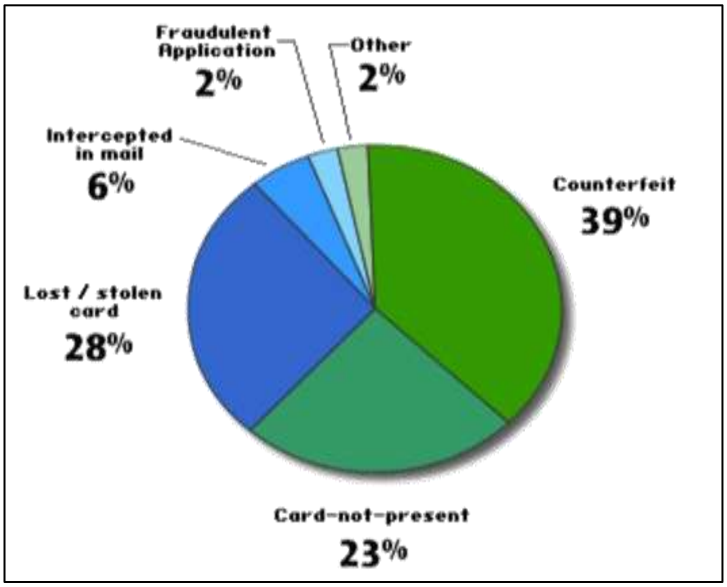

Fig. 1.2: Types of fraud[22]

B. *Credit Card Fraud Detection Method*

Fraud Detection is the process of identifying fraudulent transactions after the payments authorize. In Credit card fraud detection there are multiple approaches-

- Artificial Immune Systems
- Hidden Markov Model
- Neural Network
- Genetic Algorithm
- Decision Tree
- Support Vector Machine

C. *Credit Card Fraud Prevention*

There are many fraud prevention techniques:

D. *The Address Verification Service*

AVS is a security technique used to prevent the online credit card fraud. This technique used by the merchant to check if the customer's billing address is matching with customer's file in the credit card issuer bank. AVS technique takes the first five digits from the submitted street address and Zip code to be checked and matched with the customer's file in the issuer bank [4].

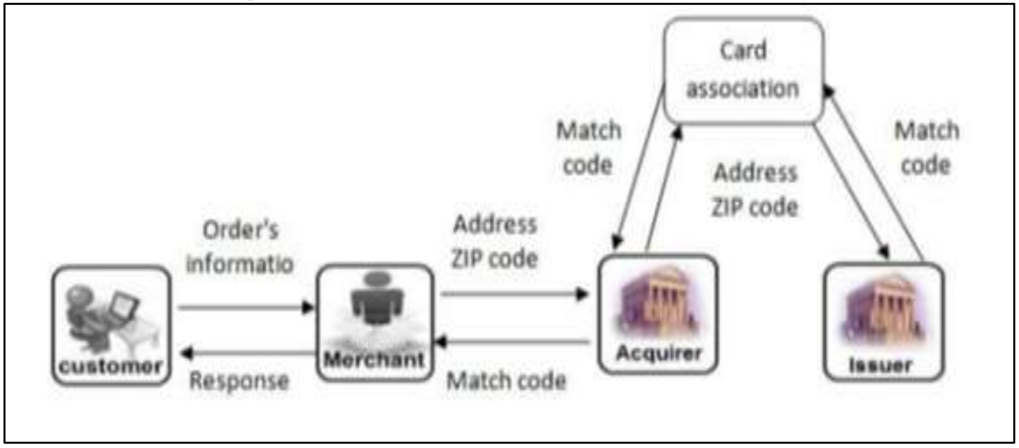

Fig. 1.3: Address Verification Service [4]

E. *Card Verification Value 2(CVV2)-*

CVV2 is stand for Card Verification Value 2. This value consists of three or four digit number printed on the front or back of the credit cards. CVV2 is a security feature used to prevent fraud especially when the fraudster obtains the credit card number in the internet.

F. *Positive and Negative List-*

It is used by the merchants to identify returning customers if they are trusted customers or fraudsters. This list would contain these customers' information i.e. address, zip code, phone number, email and credit card number. There are two types of lists: positive list and negative list.

G. *Customer Authentication-*

The customer authentication is a technique used to authenticate the authorized customers who want to make a purchase. Visa provides customer authentication services and it called "Verified by Visa". Also, MasterCard provides this service with name "MasterCard Secures Code" [4].

Table – 1
Advantages and disadvantages of fraud prevention techniques

Techniques	*Advantages*	*Disadvantages*
Address Verification Service (AVS)	*It is easy, fast and one of the most risk management techniques the merchant can take.* *Reduce the risk of fraud.*	*AVS is ineffective for the soft-product.*
Card Verification Value2(CVV2)	*It reduces the Cardholder-not-present fraud.* *It prevents the counterfeit cards.* *There are no extra costs.*	*CVV2 is not useful in the lost or stolen cards.* *The fraudster can hacked into the online system then get the CVV2.*
Positive and Negative list	*The using of lists is very easy.* *Negative list is a good for prevent repeat fraud.* *Positive list reduce the time which taken to check a valid order.*	*This list cannot use prevent identity theft fraud.* *The lists need a frequently updating.*
Customer Authentication	*The total cost is approximately low.* *The customer authentication technique is an excellent tool to prevent the fraud.*	*Only the Visa or Master card customer can use this Service. So, the merchant need to use additional fraud prevention techniques.*

III. LITERATURE SURVEY

This section, presents review of the selected literature in Credit card fraud detection.

Neda Sultana Halvaiees [2014] presented an Artificial Immune Systems, and introduce a new model called AIS-based Fraud Detection Model (AFDM). The immune system can distinguish between self and non-self. In the concept of credit card fraud detection, self represents all patterns in a finite space that is legitimate and non-self represents all patterns that are not in self.

The AIS consists of artificial lymphocytes (ALCs) that able to classify any pattern as self or non-self by detecting only non-self patterns. Lymphocytes are classified into two main types: B-cells and T-cells, both originated in the bone marrow. Those lymphocytes that develop within the bone marrow are named B-cells, and 8 those that migrate to and develop within the thymus (the organ which is located behind the breastbone) are named T-cells. The main developments within AIS have focused on three main immunological theories: clonal selection, immune networks and negative selection [1].

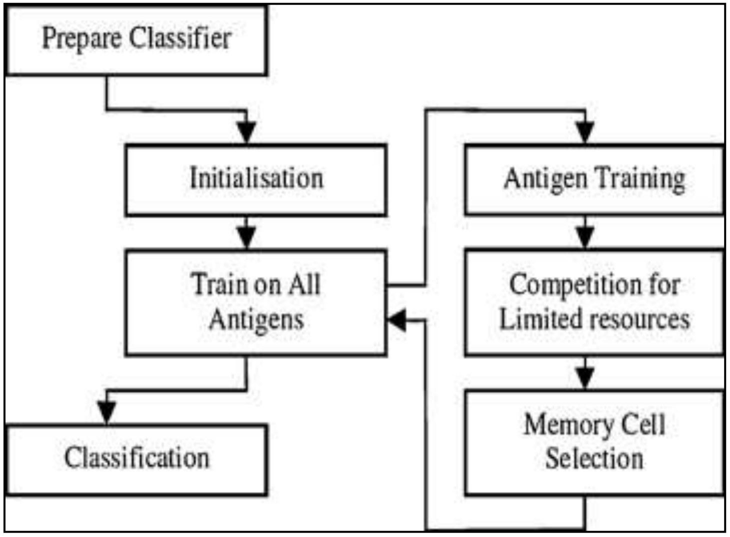

Fig. 1.4: Lifecycle overview of the AIRS algorithm [1]

Abhinav Srivastava [2008] et al describes the “Credit card fraud detection method by using Hidden Markov Model (HMM)”. In this method, they model the sequence of operations in credit card transaction processing using a Hidden Markov Model (HMM). An HMM is a double embedded stochastic process with two hierarchy levels. It can be used to model complicated stochastic processes as compared to a traditional Markov model. A Hidden Markov Model has a finite set of states governed by a set of transition probabilities. HMM uses cardholder's spending behavior to detect fraud. In Implementation, three behavior of cardholder are taken into consideration.

1) Low spending behavior
2) Medium spending behavior
3) High spending behavior

Different cardholders has their different spending behavior (low, medium, high).Low spending behavior of any cardholder means cardholder spend low amount (L), medium spending behavior of any cardholder means cardholder spend medium amount (M), high spending behavior of any cardholder means cardholder spend high amount (H). These profiles are observation symbols. The mechanism requires at least 10 transactions to determine accurately the transaction as fraud or not.

H. Algorithm Steps:

1) *Training Phase: Cluster creation*
   1) STEP 1: To identify the profile of cardholder from their purchasing
   2) STEP 2: The probability calculation depends on the amount of time that has elapsed since entry into the current state.
   3) STEP 3: To construct the training sequence for training model.
2) *Detection Phase: Fraud detection*
   1) STEP 1: To Generate the observation symbol.
   2) STEP 2: To form new sequence by adding in existing sequences.
   3) STEP 3: To calculate the probability difference and test the result with training phase [2].

Adrian Banarescu [2015] describes the "Detecting and Preventing Fraud with Data Analytics". Fraud involves inclusively significant financial risks which may threaten profitability, and the image of an economic entity. An overview, the technology can be implemented to improve fraud prevention and detection, inside of a public or private economic entity. In Economic and financial crisis, 2008 with the bankruptcy of Lehman Brothers in the USA, unlike previous crises, has had a very rapid nationally and internationally spread, It established its systemic nature in 2009. Anti-fraud activities, based on software and hardware solutions, are recommended to be carried out and coordinated by a group of specialists, with different experience, in order to cover various fields of activity. The processes of data analysis as a tool for preventing and detecting fraud can be used successfully in any field, mainly in those of the database and the data are or may be easily converted into electronic format.

- Create a special entity for this purpose.
- Creating a recovery system [3].

Aman Srivastava [2016] describes the credit card fraud detection at Merchant Side using Neural Networks. Fraud detection using neural network is totally based on the human brain working principal. Neural network technology has made a computer capable of think. As human brain learn through past experience and use its knowledge or experience in making the decision in daily life problem the same technique is applied with the credit card fraud detection technology. The neural network is used in the system to analyze the data about the card holder along with the purchase details and Transaction location to predict the genuine transactions. Neural network approach is automatic credit card fraud detection system and type of artificial intelligence programming which is based on variety of methods including machine learning approach, supervised and data mining for reasoning under uncertainty. The advantage of neural network is that it learns and does not need to be reprogrammed [6].

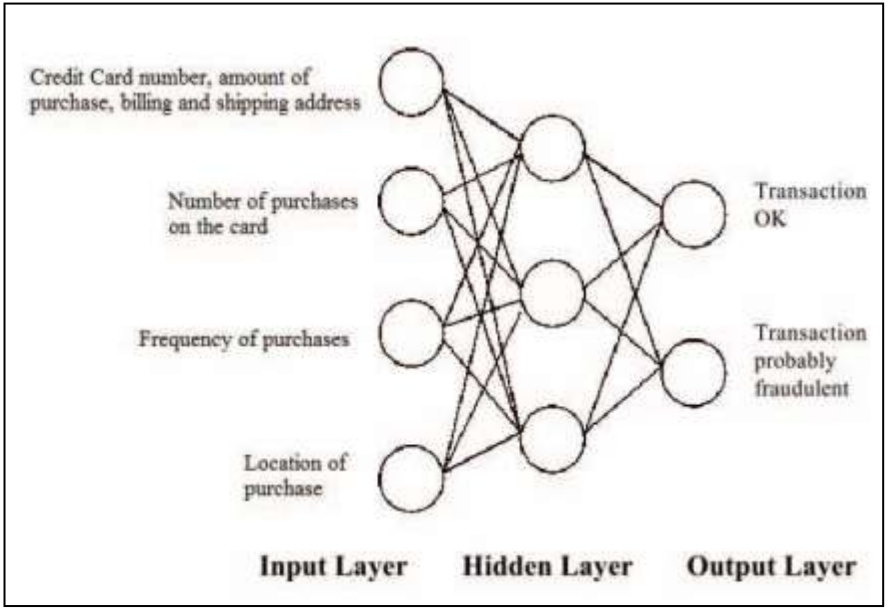
Credit Card number, amount of purchase, billing and shipping address
Number of purchases on the card
Frequency of purchases
Location of purchase
Transaction OK
Transaction probably fraudulent
Input Layer
Hidden Layer
Output Layer

Fig. 3: Layer of Neural Network in Credit Card [6]

Ekrem Duman [2011] proposed a Detecting credit card fraud by Genetic algorithm and scatter search. Genetic algorithms, inspired from natural evolution were first introduced by Holland (1975). Genetic Algorithm is an optimization technique that attempts to replicate natural evolution processes. Genetic algorithms are inspired from natural evolution. GA has been used in credit card fraud detection for minimizing the wrongly classified number of transactions. The fraud in Credit card both the physical security of credit card and privacy of credit card number should be maintained. Genetic algorithm has been applied in many areas, many financial organizations are seeking efficient framework. The operators of Genetic Algorithm are:

- Selection – It is the survival of the fittest and the preference is always given to better outcomes.
- Mutation – It is based on trying random combinations and evaluating the result (success or failure) of the outcome.
- Crossover- It is done by combining portions of good outcomes in the hope of creating an even better outcome.

In this techniques fraud detected and fraud transactions are generated with the given sample data set.
Processes are four steps-

- STEP 1: Input group of data credit card transactions, every transaction record with n attributes, and standardize the data.
- STEP 2: Calculate the critical values, C_Freq, C_Loc, C_OD, C_BB, and C_Ds.
- STEP 3: Generation find the critical values.
- STEP 4: Discover fraud transactions using this algorithm.

Dr R.Dhanapal [2012] describes a Credit card fraud detection using decision tree for tracing Email and Ip. Decision trees are statistical data mining technique that express independent attributes and a dependent attributes logically AND in a tree shaped structure. Decision Tree have become one of the most powerful and popular approaches in knowledge discovery. Decision Tree algorithm is a data mining induction Techniques that recursively partitions a data set of records using depth-first greedy approach (Hunts et al, 1966) or breadth-first approach (Shafer et al, 1996) until all the data items belongs to a special class. A decision tree structure is made of root, leaf and internal nodes. The tree Structure is used in classifying unknown data records. The tree leaves are made up of the class labels which the data items have been group [11].

Support Vector Machines (SVMs) have developed from Statistical Learning Theory. It has been widely applied to fields such as handwriting digit, character and text recognition, and more recently to satellite image classification. The basic idea of SVM classification algorithm is to construct a hyper plane as the decision plane which making the distance between the positive and negative mode maximum. The strength of SVMs comes from two main properties: - kernel representation and margin optimization. A kernel function represents the dot product of projections of the two data instance in a high dimensional feature space. SVM can have better prediction performance than BPN (Back propagation network) in predicting the future data. But in large data BPN has a good performance. SVM methods require large training dataset sizes in order to achieve maximum prediction accuracy [12].

Table – 2
Advantages and disadvantages of fraud detection method

Techniques	*Advantages*	*Disadvantages*
Artificial Immune System (AIS)	*Self-Organization/easy in integration with other systems/fault tolerance*	*Need high training time in NSA*
Hidden Markov Model (HMM)	*Fast in detection*	*Low accuracy/not scalable to large size data sets*
Neural Network	*High accuracy/ Portability/ high speed in detection*	*High expense/ Sensitivity to data format.*
Genetic Algorithm	*Inexpensive/fast in detection*	*Requires extensive tool knowledge to set up and operate and difficult to understand.*
Decision Tree	*High flexibility/easy to Implement*	*Requirements to check each condition one by one. In fraud detection condition is transaction.*
Support Vector Machines (SVM)	*SVMs can be robust, even when the training sample has some bias.*	*Expensive/Poor in process large dataset*

IV. CONCLUSION

In this paper, present a comparative study of six fraud detection methods based on credit card (Artificial Immune System, Hidden Markov Model, Neural Network, Genetic Algorithm, Decision Tree and Support Vector Machine). The main objective of this paper is to review methodology of different detection methods based on credit card. In terms of Parameter like Speed of detection, Accuracy and cost the comparison of mentioned approaches based on survey.

Table – 3
Comparison of different fraud detection methods

Methods	*Speed of detection*	*Accuracy*	*Cost*
AIS	*Very fast*	*Good*	*Inexpensive*
HMM	*Fast*	*Low*	*High expensive*
NN	*Fast*	*Medium*	*Expensive*
GA	*Good*	*Medium*	*Inexpensive*
DT	*Fast*	*Medium*	*Expensive*
SVM	*Low*	*Medium*	*Expensive*

REFERENCES

[1] Neda Soltani Halvaiee, Msohammad Kazem Akbari "A novel model for credit card fraud detection using Artificial Immune Systems", Elsevier, pp 40-39, 2014.

[2] Abhinav Srivastava, Amlan Kundu, Shamik Sural and Arun k. Majumdar, "Credit Card Fraud Detection Using Hidden Markov Model", IEEE Transaction on dependable and secure computing, VOL.5, NO.1, January-March 2008.

[3] Adrian Banarescu "Detecting and Preventing Fraud with Data Analytics", Elsevier, pp 1827-1836, 2015.

[4] Dr. Saleh Al-Furiah, Lamia AL-Braheem "Comprehensive study on methods of fraud prevention in credit card e-payment system", ACM 978-1-60558-660-1/09/0012, December2009.

[5] Ms.Pratiksha L.Meshram, Prof. Tarun Yenganti "Credit and ATM Card Fraud Prevention Using Multiple Cryptographic Algorithms", ISSN: 2277 128X, Volume 3, August 2013.

[6] Aman Srivastava, Mugdha Yadav, Sandipani Basu, Shubham Salunkhe, Muzaffar Shabad "Credit Card Fraud Detection at Merchant Side using Neural Networks", 978-9-3805-4421-2, IEEE 2016.

[7] Raghavendra Patidar, Lokesh Sharma "Credit Card Fraud Detection using Neural Network", ISSN: 2231-2307, Vol. 1, June 2011.

[8] Gabriel Preti Santiago, Adriano C.M. Pereira, Roberto Hirata "A modelling approach for credit card fraud detection in electronic payment services", ACM 978-1-4503-3196-8/15/04, April 2015.

[9] Ekrem Duman, M.Hamdi Ozcelik "Detecting credit card fraud detection by Genetic Algorithm and scatter search", Elsevier, pp- 13057-13063, 2011.

[10] Ishu Trivedi, Monika, Mrigya Mridushi "Credit card fraud detection", ISSN: 2278-1021, vol. 5, Januray 2016.

[11] Dr R.Dhanapal, Gayathiri.p "Credit card fraud detection using Decision tree for Tracing Email and ip", ISSN: 1694-0814, Vol.9, No 2, September 2012.

[12] Masoumeh Zareapoor, Pourya Shamsolmoali "Application of Credit card fraud detection: Based on bagging ensemble classifier", Elsevier, pp- 679-685, 2015.

[13] Vinit Kumar Gunjan, Amit Kumar, Sharda Avdhanam "A Survey of Cyber Crime in India", 978-1-4673-2818-0/13, IEEE 2013.

[14] Samaneh Sorournejad, Zahra Zozaji, Reza Ebrahimi Atani, Amir Hassan Monadjemi "A Survey of Credit card fraud detection techniques: Data and Techniques Oriented Perspective", IEEE 2016.

[15] Ayhan Demiriz, Betul Ekizoglu "Using Location Aware Business Rules for Preventing Retail Banking Frauds", 978-1-4799-7620-1/15, IEEE 2015.

[16] Mr.K.Kathirvel "Credit card frauds and measures to detect and prevent them", ISSN 2277- 3622 Vol.2, No. 3, March 2013.

[17] Neda Soltani, Mohammad Kazen Akbari, Mortaza Sargolzaei Javan "A New User-Based Model for Credit Card Fraud Detection Based on Artificial Immune System", 978-1-4673-1479-4/12, IEEE 2012.

[18] Mayuri Agrawal, Sonali Rangdale "Discovering Fraud in Credit Card by Genetic Programming", ISSN 2278-0211 Vol.3, November 2014.

[19] M.Gadi, X.Wang, A do Lago " Credit card fraud detection with artificial immune system, Artif. Immune System" 119-131, 2008.

[20] MohdAvesh Zubair Khan, Jabir Daud Pathan, Ali Haider Ekbal Ahmed " Credit card fraud detection system using Hidden Markov Model and K-Clustering", ISSN 2778-1021 Vol.3, February 2014.

[21] https://www.google.co.in/search?q=Credit+card+diagrams[fig 1.1]

[22] https://www.google.co.in/search?q=types+of+fraud+types[fig 1.2]