A Comprehensive Study of Mechanisms Dealing Credit Cards to Defy Social Engineering Crimes

G. Kalyani*1, K. Krishna Jyothi*2, Prof.T.Venkat Narayana Rao*3, D.Rambabu*4

Abstract: Nowadays credit cards have become a prerequisite in our daily activities. The misuse of credit card is increasing day by day. There are several ways in which a offender performs a credit card fraud. It is always been advised to exercise and provide additional security to the credit cards in order to elude the frauds. This paper focuses on credit card frauds. It addresses the cyber security challenges faced by the businesses today and it also recommends some mechanisms to allocate number to the credit card so as to avoid and identify possible hacking and spoofing. This paper also reviews of diverse algorithms that can be used to overcome the frauds in plastic digital and virtual currencies.

Keywords: Cyber security, Neural network, hacking, offender, Identifiers.

I. INTRODUCTION

Nowadays, providing security to the cyber-space has turn out to be a big question that can only be handled through mutual approaches. Cyber Security Strategy states that the cyber-security is one of the prevalent challenges. The Internet has become a key factors related to financial competitiveness and a necessary tool of the business atmosphere.

The new approach of action in cyber defense is securing and responding to intimidation by frequent efforts and assistance of all parties that might be pretentious in case of a cyber-security confrontation. Providing security is not just by installing an antivirus or firewall software systems. Security should be addressed worldwide, beyond the limits of the physical network or the local area network [2]. Figure 1 depicts types of credit cards frauds prevailing.

A. Major Cyber security challenges

Cyber security principles deal with the top four cyber security challenges faced businesses in the present scenario.

1. Thwart downtime

The only major expenditure stemming from cyber attacks is loss of confidentiality, integrity and system downtime, which prevents people from functioning or customers from trade. In the oil and gas division, the cost of a foremost cyber assails that causes 24 hours of downtime that can exceed $8 million. Nevertheless the costliest cyber crimes engross DDoS attacks.

2. Preserves coronet jewels

The goal of several APT attackers is to snatch an organization’s most expensive intellectual property. Victorious APT attacks are capable of overwhelming. Attacks attributed to China against U.S. defense contractors, for example, resulted in information theft that calls into question the combat-readiness of some new military weapons systems [1][5].

3. Maintain reputation

Security breaches such as placing sensitive institutional and customers details on public domain. For example, exposing of hacking into businesses like Sony are releasing purchaser report,
credit card numbers and sensitive emails. Breaches of LinkedIn, Last.fm and eHarmony, in the meantime, came to light after customer records surfaced on subversive hacker forums, calling into inquiry those businesses cyber security attentiveness.

4. Protect significant infrastructure

Majority of infrastructure systems include power, oil, water, telecom, funding and shipping industries that are privately owned. The network control systems that maintain these industries are aging, mostly unreliable, and vulnerable. Attacks aligned with these systems are not speculative. The British Bankers’ Association (BBA) has specially made BAE Systems Applied Intelligence to generate a system that gives banks pre-alert of cyber intimidation. The Financial Crime Alerts Service (FCAS) system permit government and law enforcement agencies, including the National Crime Agency (NCA), to build banks foil the potential threats[6].

B. Complaints concerning banking Services

The below table summarizes the customers complaints against their banks with regard to the services provided. Five categories of complaints are taken into considerations which are very often, often, sometimes, rarely and never [4].

Table - I: Complaints Regarding Services

<table>
<thead>
<tr>
<th>Complaints</th>
<th>ATMs</th>
<th>Internet Banking</th>
<th>Mobile Banking</th>
<th>Credit Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) Very often</td>
<td>30(07)</td>
<td>12(03)</td>
<td>-</td>
<td>48(12)</td>
</tr>
<tr>
<td>b) Often</td>
<td>24(05)</td>
<td>18(05)</td>
<td>27(11)</td>
<td>66(16)</td>
</tr>
<tr>
<td>c) Sometimes</td>
<td>78(17)</td>
<td>42(11)</td>
<td>27(11)</td>
<td>72(18)</td>
</tr>
<tr>
<td>d) Rarely</td>
<td>198(44)</td>
<td>204(56)</td>
<td>126(53)</td>
<td>132(33)</td>
</tr>
<tr>
<td>e) Never</td>
<td>120(27)</td>
<td>90(25)</td>
<td>60(25)</td>
<td>84(21)</td>
</tr>
<tr>
<td>Total</td>
<td>450(100)</td>
<td>366(100)</td>
<td>240(100)</td>
<td>402(100)</td>
</tr>
</tbody>
</table>

Chi-Square = 5.880

Source: Compiled from the responses obtained from respondents

Table I and figure 2. Illustrates that there are utmost 27 % respondents who never faced troubles with ATMs. In case of credit cards, this per cent is lowest, that is 21 %. The table in addition shows the positions of Internet and Mobile banking in this perspective where this percentage is 25% in every situation. Hence, the frauds occurrences on credit cards are much in number [3][12].

II. ALLOCATING NUMBER TO CREDIT CARDS

Credit card is a miniature synthetic card provided to the customers as a system for transactions. They can buy products by credit card particulars online. Luhn’s formula is used for creating a valid credit card number. In addition several programs and scripts are available online intended for generating legal credit card numbers as listed in table II.

The first digit specifies the Major Industry Identifier (MII) that is category of entity who issued the credit card. The following issuer category gives the list of Different MII digits used:
The below table [table III] lists the better known issuer identifiers:

Table -III: Issuer-Idetifier

<table>
<thead>
<tr>
<th>Issuer</th>
<th>Identifier</th>
<th>Card Number Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diner’s Club/ Carte Blanche</td>
<td>300xxx-305xxx, 36xxxx, 38xxxx</td>
<td>14</td>
</tr>
<tr>
<td>American Express</td>
<td>34xxxx, 37xxxx</td>
<td>15</td>
</tr>
<tr>
<td>VISA</td>
<td>4xxxxxx</td>
<td>13,16</td>
</tr>
<tr>
<td>MasterCard</td>
<td>51xxxxx-55xxxx</td>
<td>16</td>
</tr>
<tr>
<td>Discover</td>
<td>6011xx</td>
<td>16</td>
</tr>
</tbody>
</table>

Example: The number 4408 0412 4356 7980 is taken as an example to illustrate the description of the number. The first digit represents Major Industry Identifier (MII) i.e., 4 (banking and financial), the next digits specify issuer identifier 40804 (a VISA associate), next is account number 12 4356 798, and finally the check digit is 0.

III. CREDIT CARD FRAUDS

There are several ways in which fraudsters perform a credit card deception. As technology changes, consequently the technology of fraudsters, and therefore the technique in which they carry out fraudulent actions also improvise [10][7][4].

A. Mercantile associated Frauds

1. Merchant Collusion

This kind of deception occurs when business owners or their staffs conspire to transfer the cardholder accounts or by means of the private data. They give the information regarding cardholders to fraudsters.

2. Triangulation

Triangulation is a kind of scam that is made and operates from a web site. The goods or commodities are presented at a great deal and are shipped prior to reimbursement. When the shopper browses the site and he likes the artifacts he places the online data such as valid credit card details, name and address to the web site. When the offender receives the particulars, they order goods as if a genuine site by means of stolen credit card particulars and acquire the products.

B. Internet associated Frauds

The internet is the main source for fraudster to make the deception in a simple and easiest technique. In recent times the Fraudsters begun to function on a truly global level. Through the growth of economic, transponder, and supporting places, the internet has become an innovative worlds market, capturing customers from nearly all countries across the globe. The following are the most frequently used techniques in Internet deceit.

1. Site cloning

Site cloning is a technique where fraudsters seal a complete site or few pages where the client ended a purchase. Customers have no idea that they are not dealing with the company they wish to acquire commodities or services from, as the pages they are screening are identical to those of the genuine site. The cloned site will obtain the card details and a receipt of the transaction and a email is sent to the real company would perform. Finally, the consumer would not know about the fraudster’s action in
acquiring all the particulars they require to commit credit card fraud.

2. **False mercantile sites**

Few sites frequently offer an economical service for the clients. These site wishes the customer to fill the complete particulars such as name and address to get admittance of the webpage where the customer gets the necessary products. Many of the sites claim to be free, but obliges a valid credit card figure to confirm an entity’s like name, place, age etc. In this way, these sites collect as many credit card particulars as possible. These sites never charge individuals for the services they offer. The sites are typically a part of larger illegal network and use these details either to increase revenues or sell these credit card details to diminutive fraudsters.

3. **Credit card generators**

The computer programs are used to produce valid credit card numbers and expiry dates. These generators work by producing lists of credit card account numbers from a sole account number. It uses the mathematical Luhn algorithm to generate valid card number combinations as the normal process. This makes the user to unlawfully generating several numbers in the form of any credit card formats [8].

**IV. METHODS TO OVERCOME CREDIT CARDS FRAUDS**

The following are different types of methods and ways to overcome credit card frauds.

A. **Hidden Markov Model**

B. **A Fusion Approach Using Dempster-Shafer Theory and Bayesian Learning**

C. **Genetic Algorithm**

D. **Artificial Immune System**

E. **-Support Vector Machine**

F. **-K- nearest neighbor algorithm**

G. **-Fuzzy Logic Based System**

H. **-Decision Tree**

A. **Hidden Markov Model**

Hidden Markov Model is a double embedded stochastic process which is used to model complicated stochastic processes compared to a traditional Markov model. If a received credit card transaction is not acknowledged by the skilled Hidden Markov Model with adequately high probability, then it is considered to be deceptive transactions. HMM, K-means algorithm for clustering and Baum Welch algorithm is used for training function. Depending on the price value ranges Low, Medium, and High, HMM stores information in the form of clusters. FDS checks whether transaction is genuine or fraudulent, based on the probabilities of initial set of transaction. As HMM maintains a record of transactions it reduces tiresome work of employee but produces high false alarm in addition to high false positive [3][11][9].

The figure 2 depicts the state diagram of HMM, which shows different stages and iterations.

![State Diagram of HMM](image)

**B. A Fusion Approach Using Dempster-Shafer Theory And Bayesian Learning**

Dempster–Shafer theory and Bayesian learning is a hybrid approach for credit card fraud discovery which combines evidences from existing to past performance. Each cardholder will have a definite type of shopping activities that establishes an activity summary for them. Information fusion and Bayesian learning is proposed for fraud detection system to combat credit card fraud.

The FDS method consists of four aspects i.e. rule-based filter, Dempster–Shafer adder, transaction record database and Bayesian learner. In rule-based component, the extent of its deviation from good pattern the mistrust level of every inward transaction is determined. Dempster–Shafer’s theory is use merging of multiple evidences and an early belief is calculated. The overall belief is obtained by using initial conviction values by applying Dempster–Shafer theory. The operation is identified as suspicious or suspicion depending on original conviction. Once a deal is found to be mistrustful, then the addition conviction is strengthened or destabilized according to its resemblance with falsified or authentic transaction.
C. Genetic Algorithm

Genetic algorithms, motivated from natural advancement were first introduced in Holland. As time progresses Genetic algorithms provide better solutions. Data mining algorithms have been proposed to solve fraud detection problem as it is a classification problem. Among them decision trees are most accepted. Fraud detection is used in the areas of data mining and E-commerce. In data mining domain Genetic algorithm is used for variable assortment and is mostly coupled with other Data Mining algorithms. In credit card fraud detection for minimizing the wrongly classified number of transactions Genetic algorithms has been used very often. It is handy for computer programming language application, thus it is found to be efficient in credit card fraud exposure [3].

D. Neural Network

Fraud detection methods based on neural network are the most popular ones. Neural network is a combination of input/output units and each link has a weight associated with it. At the time of early phase, to predict the correct class labels the network learns by adjusting weights. An artificial neural network consists of an interrelated cluster of artificial neurons. The theory of neural network is provoked by the functions of the brain especially by pattern recognition and associative memory. The neural network recognizes related patterns, based upon the associative memory of the patterns it learns to predict future principles or events. It is extensively applied in categorization and grouping. As time elapses the neural networks are able to learn from the past and thus, improve results over other techniques. Based on the current situation it obtains rules and predict future activity. Many of the credit card deception studies have focused on using neural networks. Neural networks are used to represent diverse relationships between inputs and outputs or to locate patterns in data[4].

The two important phases of neural network are training and recognition. It comprise of two methods supervised and unsupervised. Samples of both fraudulent and non fraudulent records are used to create models in supervised training. In contrast, unsupervised training simply seeks those transactions, which are most unlike from the standard. Unsupervised techniques use previous knowledge of fraudulent and non fraudulent transactions in the database. Neural network system is best suited for large transaction dataset. Figure 3 shows single layer feed forward model, which shows input and output layer.

![Image](http://www.ijcttjournal.org)

Fig-3: Single Layer Feed Forward Model

E. Artificial Immune System

Artificial immune system (AIS) embodies a significant approach motivated by biological systems. AIS have mainly focus on three major immunological theories: immune networks, clonal selection, and negative selection. The immune system can differentiate among self and non-self. In the perception of credit card fraud detection, self (S) represents all patterns in a restricted space that is genuine and non-self (S) represents all patterns that are not in self. The Artificial immune system consists of artificial lymphocytes (ALCs) that can classify any pattern as self or non-self by detecting simply non-self patterns. Classifying input data as normal or fraudulent is done by AIS detection engines which implements AIS based algorithms [5].

F. Support Vector Machine

The basic idea of SVM classification algorithm is to construct a hyper plane as the decision plane which makes the distance between the positive and negative mode maximum. The power of SVMs comes from two significant properties kernel depiction and margin optimization. To learn complex regions radial basis function (RBF) kernel is used. A kernel function represents the dot product of projections of two data points in a high dimensional feature space. In support vector machine, the classification function is a hyper-plane sorting out the different classes of information. The fundamental technique finds the smallest hyper sphere in the kernel space that contains all training instances, and then determines on which side of hyper sphere a test instance lies. If a test instance lies outside the hyper sphere, it is incorrigible to be disbelief [4][6]. For large data Back propagation
network has a good performance but SVM can have better prediction performance than BPN in predicting the future data.

G. K- Nearest Neighbor Algorithm

Data stream outlier detection algorithm which is based on reverse k-nearest neighbors (SODRNN) is used for credit card fraud detection. The divergent eminence of SODRNN algorithm needs only one pass of scan. Whereas conventional methods require scanning of database lot of times, it is not appropriate for data stream situation.

The performance of K- nearest neighbor algorithm is prejudiced by three major factors:
- The distance metric used to situate the next neighbors.
- The distance rule is used to obtain a categorization from k- nearest neighbor.
- The number of neighbors used to categorize the innovative model

H. Fuzzy Logic Based System

The aspire of fuzzy logic based system is to process the huge quantity of unsure data, which is common applied in our life. To speed up protocols for customer-specific credit card fraud detection fuzzy neural networks will be working on parallel machines.

Fuzzy Darwinian System

To develop fuzzy logic laws Fuzzy Darwinian Detection uses genetic programming. It categories the transactions into suspicious and unsuspicous. It consists of a fuzzy expert system and Genetic Programming (GP) search algorithm. This approach has extreme accuracy and produces a appropriate false alarm. Except for online transactions applicable. Also it is vastly expensive and possess low processing speed [8].

I. Decision Tree

Decision trees are arithmetical data mining method that represents free attributes and a reliant attributes logically AND in a tree shaped construction. Classification rules, derived from decision trees, are IF-THEN expressions and all the tests have to be successful for each imperative is to be generated. In Decision tree, the complex problem is divided into many simple ones and each sub problems is resolved through repetition. Decision trees are analytical decision support tools that create mapping from clariﬁcation to probable consequences. There are number of accepted classiﬁers construct decision trees to generate class models. The advantage of applying the data mining techniques includes decision trees is the rational of applying logic to ﬁnd frauds in the banking domain. The projected classiﬁers of C&RT and other decision tree techniques are better than SVM approaches in solving the difﬁculty under examination. However, as the range of the training data sets turn into larger, the correct performance of SVM based models attain the performance of the decision tree based models, but the number of frauds trapped by SVM models are less than the number of frauds caught by decision tree methods, particularly C&RT model.

V. CONCLUSION

This paper describes the challenges and needs for cyber security in the vast banking domain dealing credit and debit cards. It also discusses different types of credit card frauds that are surfacing online and offline. The paper includes different types of methods that have been proposed for fraud detection in credit cards. Indisputably, there are issues still to be dealt relating to passwords, identification and operational transparency with regard to cardholders. It is deemed that this paper would offer good scope of concern about privacy in current credit card systems.

REFERENCES

[1] Dr. Komal, Dr. Vandna Rani “ progress of banking in india: customers’ perspectives” Business Intelligence Journal - January, 2012 Vol.5 No.1

Biographies:

Assistant Professor G.Kalyani, received B.Tech in Computer science and Engineering from JNTU, Hyderabad, India, holds a M.Tech in Computer Science from IETE, Hyderabad, A.P., India. She has 9 years of experience in Computer Science and Engineering areas pertaining to academics. She is presently working as Assistant Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Ghatkesar, R.R.Dist., T.S, INDIA. She is currently working in the areas of advanced Programming languages, Compiler Design, Network Security and Discrete structures.

Assistant Professor K.Krishna Jyothi, received B.Tech in Computer science and Engineering from JNTU, Hyderabad, India, holds a M.Tech in Computer Science from JNTUH, Hyderabad, India. She has 5 years of experience in Computer Science and Engineering areas pertaining to academics. She is presently working as Assistant Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Ghatkesar, R.R.Dist., T.S, INDIA. She is currently working in the areas of advanced Programming languages, Database paradigms and Network Security.

Professor T.Venkat Narayana Rao, received B.E in Computer Technology and Engineering from Nagpur University, Nagpur, India, M.B.A (Systems), holds a M.Tech in Computer Science from Jawaharlal Nehru Technological University, Hyderabad, A.P., India and a Research Scholar in JNTUK. He has 23 years of vast experience in Computer Science and Engineering areas pertaining to academics and industry related IT issues. He is presently working as Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Ghatkesar, R.R.Dist., T.S, INDIA. He is nominated as an Editor and Reviewer to 45 International journals relating to Computer Science and Information Technology and has published 74 papers in international journals. He is currently working on research areas, which include Digital Image Processing, Digital Watermarking, Data Mining, Network Security and other emerging areas of Information Technology.

Dugyani Rambabu born in Karimnagar, Telagana state, India. Received B.Tech. Degree in Computer science and Engineering from JNTUH, Hyderabad, India and M.Tech. Degree in Computer science and Engineering form JNTUH, Hyderabad. He possesses 10 years of experience teaching Engineering Programme for reputed and AICTE approved colleges. Presently working as Asst. Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Ghatkesar, R.R.Dist., T.S, INDIA. He has been actively involved in organizing and coordinating / participating in seminar, workshops, conferences and other professional activities. His current research interests include Data mining, big data and emerging-technologies