ISSN No. 0976-5697

Volume 4, No. 6, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

Fraud Detection with the Help of Hidden Markov Model and Neural Network

Sagar P. Jumde
B.E (Final Year) Information Technology
Jawaharlal Darda Institute of Engineering and Technology
Yavatmal, India
Sagarjumde21@gmail.com

Radha W.Nalamwar
B.E (Final Year) Information Technology
Jawaharlal Darda Institute of Engineering and Technology
Yavatmal, India
radhanalamwar21@gmail.com

Prof. Sunita P.Aware
Assistant prof.IT Dept
Jawaharlal Darda Institute of Engineering and Technology
Yavatmal, India
sunita_aware@yahoo.co.in

Abstract: This paper discusses the status of research on detection of fraud. Now a day's Many Peoples are using internet banking for online Transaction we call it as E-commerce. As online transaction interest is increased associated with there are many frauds increasing such as using key logger, virus and worms to reveal internet banking account information such as password and ID. In this paper we explained about how Fraud is detected using Hidden Markov Model also care has been taken to prevent genuine Transaction should not be rejected by making use of one time password which is generated by server and sent to Personal Mobile of Customer. the project is exploring the detection of fraudulent behaviour based on a combination of absolute and differential usage. Three approaches are being investigated: a rule-based approach and two approaches based on neural networks, where both supervised and unsupervised learning are considered. Special attention is being paid to the feasibility of the implementations.

Keywords: Internet Banking, Hidden Markov Model, Neural network, fraud detection, Transaction.

I. INTRODUCTION

Fraud is impacts on organizations in several areas including financial, operational, and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be staggering. The losses to reputation, goodwill, and customer relations can be devastating. As fraud can be perpetrated by any employee within an organization or by those from the outside, it is important to have an effective fraud management program in place to safeguard your organization's assets and reputation. Fraud detection in banking is a critical activity that can span a series of fraud schemes and fraudulent activity from bank employees and customers alike. Since banking is a relatively highly regulated industry, there are also a number of external compliance requirements that banks must adhere to in the combat against fraudulent and criminal activity.

A. Online Banking:

Below Some Online banking feature are mentioned those features are application specific. The Common features fall broadly into several categories.

a. Transactional:

It includes following features

a) Funds transfer between a two customer's account.
b) Paying Third Parties.
c) Investment purchase or sale.
d) Loan applications

b. Non-transactional:

a) Viewing Account Balance.
b) Viewing Recent Transaction.
c) Ordering cheque books.

Support of multiple users having varying levels of authorityTransaction approval process Wire transfer

To access internet banking, the customer would go to the financial institution's website, and enter the internet banking facility using the customer number and password. Some Financial institutions have set up additional security steps for access, but there is no consistency to the approach adopted.

B. Hidden Markov Model:

A hidden Markov model (HMM) is a statistical model in which the system being modeled is assumed to be a Markov process with unobserved state. In our case type of purchase is modeled to different state. A HMM can be considered as the simplest dynamic Bayesian network. Difference between regular Markov model and Hidden Markov Model is the state is directly visible to the observer in case of Regular Markov Model while it is absent in case of HMM. Therefore the state transition probabilities are the only parameters in Regular Markov Model. Each state has a probability distribution over the possible output tokens. In our case possible output tokens are Low, Medium, High. Therefore the sequence of tokens generated by an HMM gives some information about the sequence of states. Even if the model parameters are known exactly, the model is still 'hidden'. Hidden Markov models are used for their application pattern recognition such as speech,

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

handwriting, gesture recognition, part-of-speech tagging, musical score following, partial discharges and bioinformatics.

C. Neural network:

It has been seen that Credit card fraud detection has two highly peculiar characteristics. The first one is obviously the very limited time span in which the acceptance or rejection decision has to be made.The second one is the huge amount of credit card operations that have to be processed at a given time. To just give a medium size example, millions of Visa card operations take place in a given day, 98% of them being handled on line. Of course, just very few will be fraudulent (otherwise, the entire industry would have soon ended up being out of businesses), but this just means that the haystack where these needles are to be found is simply enormous.

II. LITERATURE REVIEW

In Credit Card Fraud Detection, They have proposed an use of HMM and Neural network in credit card fraud detection. The different steps in credit card transaction processing are represented as the underlying stochastic process. They have used the ranges of transaction amount as the observation symbols, whereas the types of item have been considered to be states of the HMM and Neural network. They have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It has also been explained how the fraud can detect whether an incoming transaction is fraudulent or not. Experimental results show the performance and effectiveness of our system and demonstrate the usefulness of learning the spending profile of the cardholders. Comparative studies reveal that the Accuracy of the system is close to 80 percent over a wide variation in the input data. The system is also scalable for handling large volumes of transactions [3] In "credit card fraud detection with a neural network" Using data from a credit card issuer, a neural network based fraud detection system was trained on a large sample of labeled credit card account transactions and tested on a holdout data set that consisted of all account activity over a subsequent two-month period of time. The neural network was trained on examples of fraud due to lost cards**,** stolen cards, application fraud, counterfeit fraud, mail-order fraud and NRI (non-received issue) fraud. The network detected significantly more fraud accounts (an order of magnitude more) with significantly fewer false positives (reduced by a factor of 20**)** over rule based fraud detection procedures. They discuss the performance of the network on this data set in terms of detection accuracy and earliness of fraud detection.[4].

This paper presents a security analysis of the proposed Internet banking model compared with that of the current existing models used in fraudulent Internet payments detection and prevention. Several modern models in preventing and detecting fraud are evolving and being applied to many banking systems. However, they have no effective detection mechanism to identify legitimate users and trace their unlawful activities. Also they are not secure enough to prevent fraudulent users from performing fraudulent transactions over the Internet. The proposed model facilitates Internet banking Fraud Detection and Prevention (FDP) by applying two new secure mechanisms, Dynamic Key Generation (DKG) and Group Key (GK) [6]. In "Study on Fraud Risk Prevention of Online Banks" paper. The paper is aimed, in the first hand, at giving a discussion on the fraud risks of online banking, introducing the current application situation of information sharing mechanism in respect of internet fraud outside China as well as the development of such concept in China. Then, a system is designed for sharing internet fraud information.

In the paper "Parallel Granular Neural Networks for Fast Credit Card Fraud Detection" .A parallel granular neural network **(**GNN**)** is developed to speed up data mining and knowledge discovery process for credit card fraud detection. The entire system was working on the Silicon Graphics Origin 2000, which is a shared memory multiprocessor system consisting of 24-CPU, 4G main memory, and 200GB harddrive. In simulations, the parallel fuzzy neural network running on a 24-processor system is trained in parallel using training data sets, and then the trained parallel fuzzy neural network discovers fuzzy rules for future prediction. The higher the fraud detection error is, the greater the possibility of that transaction being actually fraudulent.

III. DIFFERENT TYPE OF FRAUD TECHNIQUES

There are many ways in which fraudsters execute a credit card fraud. Frauds can be broadly classified into three categories, i.e., traditional card related frauds, merchant related frauds and Internet frauds. The different types of methods for committing credit card frauds are described below.

A. Merchant Related Frauds:

Merchant related frauds are initiated either by owners of the merchant establishment or their employees. The types of frauds initiated by merchants are described below:

a. Merchant Collusion:

This type of fraud occurs when merchant owners or their employees conspire to commit fraud using the cardholder accounts or by using the personal information. They pass on the information about cardholders to fraudsters.

b. Triangulation:

Triangulation is a type of fraud which is done and operates from a web site. The products or goods are offered at heavily discounted rates and are also shipped before payment. The customer while browse the site and if he likes the product he place the online information such as name, address and valid credit card details to the site. When the fraudsters receive these details, they order goods from a legitimate site using stolen credit card details. The fraudsters then by using the credit card information purchase the products.

B. Internet Related Frauds:

The internet is the base for the fraudsters to make the frauds in the simply and the easiest way. Fraudsters have recently begun to operate on a truly transnational level. With the expansion of trans-border, economic and political spaces, the internet has become a new worlds market, capturing consumers

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

from most countries around the world. The following technique described are most commonly used in Internet fraud.

a. Site Cloning:

Site cloning is where fraudsters close an entire site or just the pages from which the customer made a purchase. Customers have no reason to believe they are not dealing with the company that they wished to purchase goods or services from because the pages that they are viewing are identical to those of the real site. The cloned site will receive these details and send the customer a receipt of the transaction through the email just as the real company would do. The consumer suspects nothing, while the fraudsters have all the details they need to commit credit card fraud.

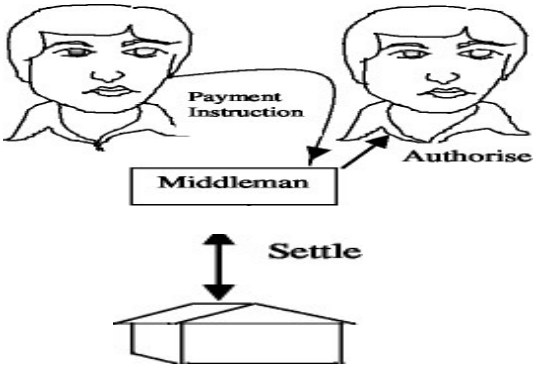

Figure.1: General Model of Internet Transaction

b. False merchant sites:

Some sites often offer a cheap service for the customers. That site requests the customer to fill his complete details such as name and address to access the webpage where the customer gets his required products. Many of these sites claim to be free, but require a valid credit card number to verify an individual s age. These kinds of sites in this way collect as many as credit card details.

c. Credit card generators:

These are the computer programs that generate valid credit card numbers and expiry dates. These generators work by generating lists of credit card account numbers from a single account number. The software works by using the mathematical Luhn algorithm that card issuers use to generate other valid card number combinations. This makes the user to allow to illegally generating as many numbers as he desires, in the form of any of the credit card formats.

IV. OTHER FRAUD TECHNIQUES

A. Lost/ Stolen Cards:

When one person loses his card or a card is stolen by someone or when a legitimate account holder receives a card and loses it or someone steals the card for criminal purposes. This the easiest way for the fraudsters where he gets the information of the cardholders without investing any on the modern technology.

a. Account Takeover:

The fraudster takes control of a legitimate account by either providing the customer's account number or the card number. The fraudster then contacts the card issuer, as the genuine cardholder, to ask the mail to redirect to a new address. The fraudster reports card lost and asks for a replacement to be sent.

b. Cardholder-Not-Present (CNP):

CNP transactions are performed only on the internet that is remotely, in such kind of frauds neither the card nor the cardholder is present at the point-of-sale. This take many types of transactions such as orders made over the phone or Internet, by mail order or fax. In such transactions, retailers are unable to physically check the card or the identity of the cardholder, which makes the user unknown and able to disguise their true identity. The details of the credit card are normally copied without the cardholder's knowledge, collected from the receipts thrown by the customer or obtained by skimming process. Fraudulently obtained card details are generally used with fabricated personal details to make fraudulent CNP purchases.

c. Fake and Counterfeit Cards:

This is another type of fraud where the creation of counterfeit cards, together with lost or stolen cards poses highest threat in credit card frauds. Fraudsters are constantly finding new and more innovative ways to create counterfeit cards. The below mentioned are some of the techniques used for creating false and counterfeit cards.

d. Erasing the magnetic strip:

This is the type of the fraud where the fraudsters erase the magnetic stripe by using the powerful electro-magnet. The fraudster then tampers with the details on the card so that they match the details of a valid card, which they may have attained, for example, when the fraudster begins to use the card, the cashier will swipe the card through the terminal several times, before realizing that the metallic strip does not work. The cashier will then proceed to manually input the card details into the terminal. This kind of fraud is having high risk because the cashier will be looking at the card closely to read the numbers.

***e. Creating a fake card*:**

Today we have sophisticated machines where one can create a fake card from using the scratch. This is the common fraud though fake cards require a lot of effort and skill to produce it. Modern cards are having many security features, all designed to make it difficult for fraudsters to make good quality fraudulent. After introducing the Holograms in the credit cards it makes very difficult to forge them effectively.

***f. Skimming*:**

Skimming is fast emerging as the most popular form of credit card fraud. Most cases of Counterfeit fraud involve skimming. It is a process where the actual data on a card's magnetic stripe is electronically copied onto another. Fraudsters have been found to carry pocket skimming devices,

a battery-operated electronic magnetic stripe reader, with which they swipe customer's cards to get hold of customer s card details. The fraudster does this whilst the customer is waiting for the transaction to be validated through the card terminal. The card holder doesn't t know about this and it is very difficult for him to identify. In other cases, the details obtained by skimming are used to carry out fraudulent card not-present transactions by fraudsters. Until the cardholder gets the bill to he don't understand what s the thing happened.

g. Phishing:

Phishing is a type of fraud designed to steal a person's identity. It is usually committed via spam e-mail or pop-up windows. Phishing works by a malicious person sending lots of false e-mails. The e - mails looks like they come from a website or company you trust, for example your bank. The message tells you to provide the company with your personal details including your payment card details. They can claim that the reason for this is a database crash or the like. To make the e- mails look even more authentic, the fraudster might put a link to a website that look exactly like the real one but is in fact a scam site. These copies are often called "spoofed websites". When you are on the spoofed site they can ask you for even more personal details that will be directly transmitted to the person who made the site.

V. ARCHITECTURE OF PROPOSED SYSTEM

Architecture of Proposed system consists of following component.

A. Actual User:

Basically he is the authorized client who is having internet banking account in particular bank He can do online Transaction with the help of Internet Banking account legally

B. Fraudulent User:

He is the unauthorized user who is not having legal Internet banking account in bank. who makes use of authorized users Internet banking account to do Transaction. Hence He is Fraudulent User. He obtains the password of Particular Customer By doing attacks that are mentioned in 1.4.

C. Bank Server:

Bank Sever is managed by Bank Manager who is responsible to add customers for internet banking account. All the processing of internet banking done here where Manger can change account status(Lock to Unlock and vice versa). It also records the Customer Transaction Pattern Using HMM algorithm. This is used to Detect pattern and to find Fraudulent Transaction. In case of Violation Bank server sends the one time password to the Mobile Number which is registered in the Bank Database for Particular Customer.

D. Bank Database:

It stores the Information about customers such as (Name, Contact Number, Email id, Account Number).It also Stores the previous Transaction information of Customer made also it records Sequence of Transaction and it is modeled through Hidden Markov Model. For about 10th Transaction are recorded sequence and from 11th Transaction HMM algorithm is running to find Fraudulent Transaction.

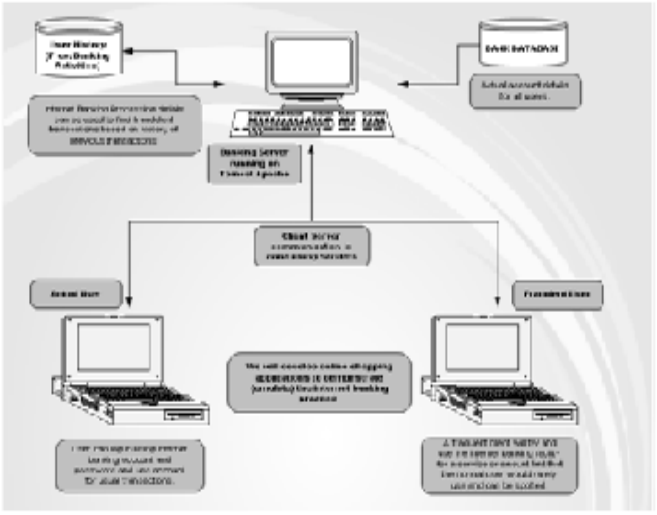

Figure 2: Architecture of Proposed System.

VI. USE OF HMM TO DETECT FRAUD

A. Process Flow Diagram:

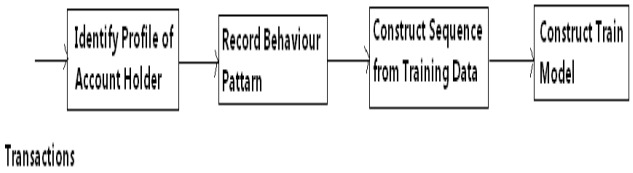

Figure 3: Training Phase of Process flow diagram.

The figure below illustrates about the two phases of the detection system used by HMM. In the training phase Train Model is created and based on the initial set of transactions Behavior profile of Internet Bank Holder is identified. This directs for expected transaction sequence for each account holder and the system is trained accordingly. In the detection And Prevention phase(Fig 3) the system looks for the deviation in expected and actual outcome and fraud is recognized. When fraud is Recognized Bank server sends One time passwords to Mobile Number.

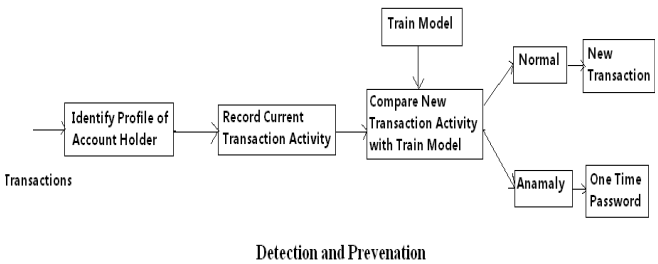

Figure 4: Detection and Prevention Phase of Process flow diagram.

VII. RULE-BASED APPROACH TO FRAUD DETECTION

In ASPeCT, several approaches are taken to identify fraudulent behaviour. In the rule-based approach, both the absolute and differential usage are verified against certain rules. This approach works best with user profiles containing explicit information, where fraud criteria given as rules can be referred to. User profiles are maintained for the directory number of the calling party (A-number), for the directory number of the called party (B-number) and also for the cells used to make/receive the calls. A-number profiles represent user behaviour and are useful for the detection of most types of fraud, while B-number profiles point to hot destinations and thus allow the detection of frauds based upon call forwarding. All deviations from normal user behaviour resulting from the different analysing processes are collected and alarms will finally be raised if the results in combination fulfil given alarm criteria.

The implementation of this solution is based on an existing rule-based tool for audit trail analysis PDAT (Protocol Data Analysis Tool) PDAT is a rule based tool for intrusion detection developed by Siemens ZFE PDAT works in heterogeneous environments, has the possibility of on-line analysis, and provides a performance of about 200 KB input per second. Important goals were flexibility and broad applicability, including the analysis of general protocol data, which is achieved by the special language PDAL (Protocol Data Analysis Language). PDAL allows the programming of analysis criteria as well as a GUI-aided (Graphical User Interface) configuration of the analysis at run-time. Intrusion detection and mobile fraud detection are quite similar problem fields; the flexibility and broad applicability of PDAT are promising for using this tool for mobile fraud detection. The main difference between intrusion detection and mobile fraud detection seems to be the kind of input data. The recording for intrusion detection produces 50 MB per day per user, but only for the few users of one UNIX system. In comparison, mobile telephone fraud detection has to deal with a huge amount of subscribers (roughly 1 Million) each of whom, however, produces only about 300 bytes of data per day. PDAT was able to keep all interim results in main memory, since only a few users had to be dealt with. For fraud detection, however, intermediate data has of course to be stored on hard disc.

The main tasks were the introduction of user profiles stored in a data base and the realisation of a new protocol that allows PDAT to understand both user profile as well as Toll Ticket formats. Once established, PDAT provides a comprehensive infrastructure based on a GUI for showing alarms and for editing alarm criteria during runtime. The new architecture is depicted in Figure 5.

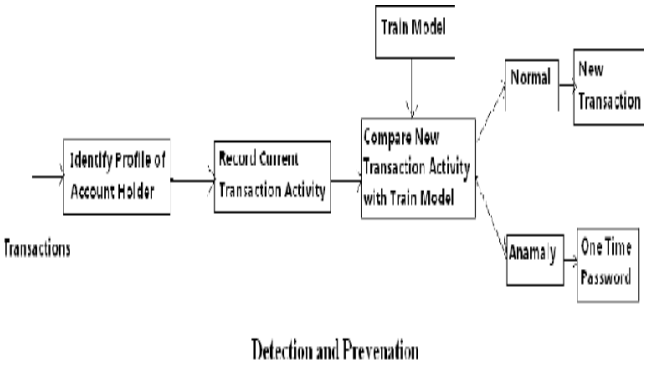

Figure.5 Architecture of rule-based fraud detection tool

VIII. NEURAL NETWORK BASED APPROACH TO FRAUD DETECTION

A second approach to identify fraudulent behavior uses neural networks. The multiplicity and heterogeneity of the fraud scenarios require the use of intelligent detection systems. The fraud detection engine has to be flexible enough to cope with the diversity of fraud. It should also be adaptive in order to face new fraud scenarios, since fraudsters are likely to develop new forms of fraud once older attacks become impractical. Further, fraud appears in the billing system as abnormal usage patterns in the Toll Ticket records of one or more users. The function of the fraud detection engine is to recognise such patterns and produce the necessary alarms. High flexibility and adaptivity for a pattern recognition problem directly point to neural networks as a potential solution. Neural networks are systems of elementary decision units that can be adapted by training in order to recognise and classify arbitrary patterns.

The interaction of a high number of elementary units makes it possible to learn arbitrarily complex tasks. For fraud detection in telephone networks, neural network engines are currently being developed world-wide (4,5). As a closely related application, neural networks are now routinely used for the detection of credit card fraud. There are two main forms of learning in neural networks: unsupervised learning and supervised learning. In supervised learning, the patterns have to be *a priori* labelled as belonging to some class. During learning, the network tries to adapt its units so that it produces the correct label at its output for each training pattern. Once training is finished the units are frozen, and when a new pattern is presented, it is classified according to the output produced by the network. In unsupervised learning the system is allowed to find patterns or clusters in the data in the hope that these clusters will be useful or meaningful in some way, either directly or indirectly.

A. Supervised Learning:

For supervised learning we utilise a multi-layer perceptron. It is defined as follows. The network is composed of elementary units called neurons. Each neuron produces at its output a simple non-linear transformation of its inputs depending on the value of the weights of the network, thus:-

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

$$y = \sigma(\sum_{i=1}^{n} w_i x_i + w_0), \quad \text{where } \sigma(z) = \tanh(z) \text{ or}$$

$$\sigma(z) = \frac{1}{1+e^{-z}}$$

Where *xi* is the value on the i-th input line and *wi* is the weight on that line. The neurons are then arranged in a two-hidden-layer network with *D* inputs, *H1* hidden neurons in the first layer, *H2* hidden neurons in the second layer, and *C* outputs. The outputs *zm* of the network can then be defined

$$h_{1_k} = \sigma(\sum_{l=1}^{D} w_{kl} x_l + w_{k0}), h_{2_i} = \sigma(\sum_{k=1}^{H_1} v_{ik} h_{1_k} + v_{i0}),$$

$$z_m = \sigma(\sum_{l=1}^{H_2} u_{lm} h_{2_i} + u_{l0})$$

B. Unsupervised Learning:

With unsupervised learning, statistical user profiles are generated by the classification of GSM Toll Tickets into one of a set of Toll Ticket prototypes. The user profiles are comprised of a vector of values essentially counting the number of times a Toll Ticket prototype gets excited by the presentation of a Toll Ticket. The task of the system, after developing user profiles over a specified period, is to raise alarms when it is presented with profiles where the difference between the CUP and the UPH is outside the realms of normal usage. An alert status will be raised if the profiles are significantly different. Note that the system requires only clean (non fraudulent) data for training. This system therefore has the potential to detect new types of fraud as and when they occur. Prototyping is a method of forming an optimal discrete representation of a naturally continuous random variable. The processing of continuous random variables by discrete systems generally reduces empirical information. Neural Networks are capable of forming optimal discrete representations of continuous random variables through their ability to converge, by lateral interaction, to stable uniformly distributed states.

The mapping of a continuous random variable X into a set of K discrete prototypes Q reduces the empirical information by the least amount if a uniform distribution {**P**(*q*) ,*i* ...*K i K* = 1 = 1 }, corresponding to the absolute maximum (*S K Q* = log) of information entropy, is assigned to Q. Grabec provides a way to extend this principal to multiple dimensions. When considering the set of all possible Toll Tickets, we clearly have a dimension to represent every parameter that we wish to include in the analysis. Each parameter in a Toll Ticket can assume a range of values and is thus itself a random variable. Grabec's technique will allow us to create a number of prototypes that dynamically and uniformly span the set of samples taken from the space of possible Toll Tickets. For a differential analysis we need to maintain the concept of two different spans over the Toll Tickets. We maintain the two profiles as probability distributions using two different decay factors a and b . When a Toll Ticket is presented to the system to update a user's CUP, each element of the CUP is multiplied by decay factor a . The entry in the profile corresponding to the prototype *i* , that was excited by the presentation of the incoming Toll Ticket, is then incremented by an amount (1−a) . Updating the CUP in this manner will maintain the profile as a probability distribution. After updating the CUP, a differential analysis is performed by the fraud engine on the CUP and UPH. Following presentation to the fraud engine, the UPH is updated using

$$H_i = \beta H_i + (1-\beta) C_i$$

Where *Hi* and *Ci* represent the *i*th element of the UPH and CUP respectively. By applying a multiplicative decay factor, any counter in the profile corresponding to a prototype, once excited, will never actually decay to zero. To perform the differential analysis on the user profiles we use a measure known as the Hellinger distance. In detection mode the fraud engine again calculates *d* and if the resultant value is greater than a preset threshold, then an alert status is raised proportional to *d dthreshold* − . It is anticipated that these alert statuses will be prioritized for investigation.

IX. CONCLUSION

In this paper,we saw different technique that is being used to execute credit card fraud how credit card fraud impact on the financial institution as well as merchant and customer, fraud detection technique used by VISA and MasterCard. Neural network is a latest technique that is being used in different areas due to its powerful capabilities of learning and predicting. This proposed methodology is aimed at detecting fraud in case of internet banking. In Internet Banking a Fraud detection system will run at the banks server and its Function to detect fraud in online transaction. This is a Prediction system. Fraud detection is carried out using Hidden Markov Model and Neural network. Initially After detecting a fraud it sends a Onetime password to Mobile number. Here prices are divided into three ranges. Low, Medium, and High. We model the sequence of operations in online banking transaction processing using a Hidden Markov Model (HMM) and show how it can be used for the detection of frauds.

X. ACKNOWLEDGEMENT

We would like to avail this opportunity to express our deep sense of gratitude and whole hearted thanks to our Guide **Prof.S.P Aware** for giving her valuable guidance, inspiration and affectionate encouragement to study this project.

We also acknowledge our overwhelming gratitude and immense respect to Dr. R. M Tugnayat H.O.D. I.T. Department, Principal Dr. A. W. Kolhatkar and other staff members who inspired us a lot to achieve the highest goal.

XI. REFERENCES

[1]. Hidden Markov Model by Jia Li. Department of Statistics "The Pennsylvania State University"

[2]. "A Revealing Introduction to Hidden Markov Models" by mark stamp.

[3]. "Credit Card Fraud Detection Using Hidden Markov Model" By Abhinav Srivastava, Amlan Kundu, Shamik Sural. IEEE Transaction, January-March 2008.

[4]. "credit card fraud detection with a neural network" by Ghosh and Reilly. IEEE" Proceedings of the Twenty- Seventh Annual Hawaii International Conference on System Sciences, 1994.

[5]. ACTS AC095, project ASPeCT: February 1996 Initial report on security requirements AC095/ATEA/W21/DS/P/02/B.

[6]. ACTS AC095, project ASPeCT: September 1996 Definition of fraud detection concepts. AC095/KUL/W22/DS/P/06/A

[7]. Katzer, T. Mehlhart, C. Wolff: 1993. PDAT – ein Protokolldaten-Analysewerkzeug fuer sichere Betriebssysteme und Anwendungen. Unix in Deutschland - GUUG, Network Verlag, Hagenburg, Germany.