Implementation of an Enhanced Hidden Markov Model in Detecting Credit Card Frauds

GRADUATE PROJECT REPORT

Submitted to the Faculty of
Department of Science and Engineering
Texas A&M University-Corpus Christi
Corpus Christi, TX

in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

By,

Sravani Pedamallu
Fall 2011

Committee Members

Dr. Mario A. Garcia
Committee Chairperson

Dr. Mufid Abudiab
Committee Member

Dr. David Thomas
Committee Member
I hereby affirm that I have followed the directions as published in the program Web page at

http://cs.tamucc.edu/docs/GraduateProjectAgreementForm.pdf

And I confirm that this project and documentation is my own personal work and all the material other than my own is properly referenced.

Student’s Name: ___________________________________________

Student’s Signature: _________________________________________

Date: ______________________________________________________
ACKNOWLEDGEMENT

I take this opportunity to offer my honor and profound greetings on the success of my project to Dr. Mario A. Garcia, Professor of the Department of Computer Science, Texas A & M University – Corpus Christi, for his generous help and great support. I felt motivated from his incredible guidance and this project would not have been possible without his contribution.

I would like to greatly thank Dr. Mufid Abudiab of the Department of Science and Engineering, Texas A & M University – Corpus Christi, for being part of my project and for positive encouragement. His constant support with valuable suggestions boosted up my energy in completing this project in time.

Also I am very thankful to Dr. David Thomas of the Department of Science and Engineering, Texas A & M University – Corpus Christi, for his constant effort in bringing up my project document into an acceptable standard form. His attention and planning of the course has helped me complete this project with good values.

I would like extend my sincere gratitude to the entire faculty of Department of Science and Engineering, Texas A & M University – Corpus Christi, for their suggestions and support which helped complete this project successfully and efficiently.

Finally, would like to express my heartfelt thanks to my family and friends who have been my inspired me with their ideas and motivating contribution in making this project a possible one successfully.
ABSTRACT

In the current days, with the rapid progression in the e-commerce technology, the usage of credit cards has increased radically due to its varied benefits. The mode of payment through credit card has made people’s life easy for both online and ordinary purchases and thus widespread. This enormous usage of credit card leads to different frauds [Edwin 2011]. In this paper, an enhanced form of the existing model is introduced wherein the sequence of operations in credit card transactions are reproduced, processing using a Hidden Markov Model (HMM) and is demonstrate how it can be used for the detection of frauds in credit cards.

The enhanced form of typical HMM is primarily trained with the standard procedures of a cardholder. If an incoming credit card transaction is not approved by the trained HMM with adequately high probability, it is considered to be fraudulent. During this process, it is also ensured that legitimate transactions are not rejected [Srivatsa 2008]. Through this paper, detailed experimental results are presented to illustrate the effectiveness of the approach and also compare it with other existing models that are available in the literature.
# TABLE OF CONTENTS

Acknowledgement ........................................................................................................................................ iii

Abstract .................................................................................................................................................... ii

Table of Contents ..................................................................................................................................... iv

List of Figures .......................................................................................................................................... vii

List of Tables .......................................................................................................................................... ix

1. Introduction ........................................................................................................................................... 1

   1.1 Credit card ......................................................................................................................................... 1

   1.2 Credit card frauds ............................................................................................................................. 2

   1.3 History ............................................................................................................................................. 4

       1.3.1 Background and related work ................................................................................................. 6

           1.3.11 Fusion of Dempster–Shafer theory and Bayesian learning ............................................. 6

           1.3.12 BLAST-SSAHA in credit card fraud detection ................................................................. 7

           1.3.13 Credit Card Fraud Detection using Hidden Markov Model (HMM) ........................... 9

           1.3.14 Fuzzy Darwinian Detection of Credit Card Fraud ........................................................ 10

           1.3.15 Credit Card Fraud Detection Using Bayesian & Neural Networks .......................... 11

       1.3.2 Evaluation of different credit card fraud detection systems ............................................. 12

   1.4 Rationale ........................................................................................................................................ 14

2. Narrative ............................................................................................................................................. 15

   2.1 Problem Statement .......................................................................................................................... 15

   2.2 Scope .............................................................................................................................................. 16

   2.3 Functionalities of this project ...................................................................................................... 16
2.4 Reducing the possibility of occurrence of frauds........................................16

3. Proposed System Design.................................................................................18

3.1 Enhanced Hidden Markov Model Approach in detecting Credit Card Frauds...18

3.2 Framework........................................................................................................18

3.2.1 In step procedure of this project development...........................................19

3.2.2 System Requirements..................................................................................20

3.2.3 System Architecture....................................................................................20

3.3 Proposed Mechanism......................................................................................23

4. Functionalities Of The Application...................................................................24

4.1 Modules Description.......................................................................................24

4.1.1 New User Registration...............................................................................28

4.1.2 Login............................................................................................................29

4.1.3 Security information...................................................................................31

4.1.4 Transaction..................................................................................................33

4.1.5 Verification..................................................................................................36

5. Testing And Implementation..............................................................................38

5.1 Testing.............................................................................................................38

5.2 Types of testing..............................................................................................38

5.2.1 White box testing.......................................................................................39

5.2.2 Black box testing.......................................................................................39

5.2.3 Unit testing................................................................................................39

5.2.4 Integration testing......................................................................................40

5.2.5 Validation testing.......................................................................................40
5.2.6 Output testing.................................................................40
5.2.7 User acceptance testing...............................................41
5.3 Test cases..............................................................................41
  5.3.1 Test Case-1: Successful New User Registration........41
  5.3.1 Test Case-2: Successful existing user login..............43
  5.3.1 Test Case-3: Successful Administrator Login............44
  5.3.1 Test Case-4: Making a successful genuine transaction.48
  5.3.1 Test Case-5: Making a successful fraud transaction.....52

6. Results.................................................................................60
7. Conclusion............................................................................62
   Bibliography and References...............................................64
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Block diagram of the Fusion of Dempster-Shafer theory and Bayesian learning</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Architecture of BLAST and SSAHA Fraud Detection System</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Process Flow of the HMM FDS</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Block diagram of the Evolutionary-fuzzy system</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Proposed Enhanced HMM Fraud Detection System Architecture</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Use case Diagram of Enhanced HMM Fraud Detection System Architecture</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Sequence diagram of Enhanced HMM Fraud Detection System Architecture</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Admin Login Page</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Admin view of credit card user accounts</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Admin view of blocked users</td>
</tr>
<tr>
<td>Figure 11</td>
<td>New User Registration Page</td>
</tr>
<tr>
<td>Figure 12</td>
<td>User Login Page</td>
</tr>
<tr>
<td>Figure 13</td>
<td>User account Page</td>
</tr>
<tr>
<td>Figure 14</td>
<td>First level security testing</td>
</tr>
<tr>
<td>Figure 15</td>
<td>User interface at second level of security</td>
</tr>
<tr>
<td>Figure 16</td>
<td>User interface to view transactions that are in process</td>
</tr>
<tr>
<td>Figure 17</td>
<td>User interface to view finalized transactions</td>
</tr>
<tr>
<td>Figure 18</td>
<td>New User Registration Page</td>
</tr>
<tr>
<td>Figure 19</td>
<td>User Login Page</td>
</tr>
<tr>
<td>Figure 20</td>
<td>User account Page</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Admin Login Page</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Admin interface showing profile page</td>
</tr>
</tbody>
</table>
Figure 23: Admin interface showing user accounts page..........................47
Figure 24: Admin view of blocked users.................................................49
Figure 25: User interface to view transactions that are in process..............35
Figure 26: User interface to view finalized transactions..........................36
Figure 27: First level security testing.....................................................33
Figure 28: User interface at second level of security.............................34
Figure 29: Notification for making successful transaction.......................49
Figure 30: Notification for e-mail message sent....................................50
Figure 31: User interface to view transactions that are in process.............55
Figure 32: User interface to view finalized transactions..........................56
Figure 33: First level security testing.....................................................57
Figure 34: User interface at second level of security.............................58
Figure 35: Notification message............................................................58
Figure 36: Notification message............................................................59
Figure 37: Mail confirmation message...................................................59
Figure 38: Comparison graph of existing and proposed HMM for accuracy.....60
LIST OF TABLES

Table 1: Comparison of various credit card fraud detection mechanisms ............13
Table 2: New user registration database table .................................................. 30
Table 3: Credit card verification database table ................................................. 37
Table 4: Transaction verification database table ............................................... 38
Table 5: Comparison graph of existing and proposed HMM ............................... 61
1. INTRODUCTION

1.1 Credit card

The typical credit card looks like a small rectangular card made of plastic which is issued to the users as a mode of payment. The credit-card holders are allowed to purchase any materials or service as long as the promises are kept by the credit card user. Security of the credit card relies upon its privacy of the card details i.e., credit card holder name and also its number. The credit cards can be used in two ways: a) physical usage and b) virtual/online usage. Physical usage is where an individual does use the credit card to pay for his purchases in any store personally and virtual or online usage is where the card owner uses the credit card to pay for purchased items online over the internet by just entering the required credit card details. With the increasing technology and the usage of internet for online shopping around the globe has brought a significant rise in the credit card usage in making transactions [Srivatsa 2008].

1.2 Credit card frauds

In general, a fraud is defined as a crime committed with intention to damage a person and is also a violation. Fraud may be committed for various reasons: for entertainment, to exploit a business / an organization, to take revenge, to cause financial loss, to damage identity and etc. Also there are several types of frauds: bankruptcy frauds, identity thefts, health frauds, religious frauds, credit card frauds, insurance frauds, forgery, tax frauds and many more. Here considering only the credit card frauds, they can be of two kinds: a) offline credit card frauds and b) online credit card frauds. Offline credit card frauds are those where an individual’s credit card is lost or stolen. If any
attacker or hacker, hack the details and use it to commit illegal actions is referred as online frauds. With the rapidly developing technology, usage of internet is drastically increasing. Substantially, this is leading to many credit-card fraudulent activities.

Under the vulnerable situations, the users must limit amount of information they are sharing to reduce the exposure and chances of getting attacked by a hacker. Certain steps can be followed to protect themselves in case of vulnerabilities and insecurities regarding their identity: firstly, the users must take considerable care and attention to all their documents consisting of their identity, accounts and other sensitive information. Information sharing between friends and relatives is other reason from research that causes credit card frauds because of current lifestyle conditions. So, this has to be avoided and proper precaution must be taken. While the old documents or devices are disposed or discarded, users must make sure that there is no personal information that can be possibly revealed or tracked by anyone. Bank account information like transactions and balances should be regularly checked by the users to avoid money loss that could be caused by attackers. Secondly, the use of computer systems and internet must be developed among the people. For example, just by installing anti-virus software is not sufficient enough to not get attacked by any malware. Without proper security across the network, the information over the internet must not be shared. Users should not access for their personal information from public wireless networks or others accounts and must carry a strong WPA key to their Wi-Fi access points. Thus, users need to look for security policies and keep their account protected from possible threats. Basic security precautions like effective control over cookies, anonymous browsing, reducing computer information
with-holdings, considering network address protection, using strong encrypting tools and changing passwords of all accounts often and also using passwords that are hard-to-crack can help the users from being attacked.

Not just the users that need to take care of their personal credit card information; the respective banks and organizations that are issuing credit cards must also take initiative actions and work collectively considering two important things: firstly, they must bring out strict policies over public to secure genuine credit card holders and their privacy. And secondly, they must organize awareness about the secure way of using credit-cards and attacks possible among the public by prevention campaigns from several smaller targets to bigger population.

If there are people who are already attacked by fraud persons, then those victims should take immediate actions related to situation. If a credit card related to a bank account of a person is hacked and fraud is detected by the victim, in order to protect his account from further financial destructions, he/she must contact the bank or bank’s anti-fraud centre or credit card agent, requesting to block their card and monitor the details. Also then should report and register a complaint with the police department for investigation. It is definitely a challenging task to battle against the damage caused for one’s loss. The information that is shared over the internet is never completely deleted. This is also a possible reason for cyber attacks. Hence it is very important to contact the sources of information and request them to delete the information as after effects of any fraud is difficult to recover and time consuming for any victim.
1.3 History

Lately, the fraud detections with respect to credit cards have been involving in much of research interest. Various methods were put forward, some of which have special focus using data mining and neural networks [Srivatsa 2008]. In this pipeline, Ghosh and Reilly introduced a detection system that uses neural network. They have constructed this that is skilled at a huge sample of labeled credit card transactions. Any missing cards, either stolen or lost and frauds like application fraud, fake fraud, mail-order fraud, and non-received issue (NRI) frauds are sample cases of the credit card account transactions [Ghosh 1994]. In the recent times, parallel granular neural networks (PGNNs) have been used by Syeda, for enhancing the speed of data mining and information finding methods in detection of credit card frauds. Proper system has been built for serving this purpose [Syeda 2002]. Then, Stolfo introduced a fraud detection system (FDS) for credit card frauds that used metal-learning skills to understand the forms of fraudulent credit card transactions. The metal-learning is a procedure where various techniques are combined and integrated with each other. In this manner, another model was proposed by Stolfo fraud and intrusion detection where in it was called as cost-based model. In this, they used Java agents for metal learning referred as JAM. JAM in the detection of credit-card frauds, is a distributed data-mining system [Stolfo 1999] [Srivatsa 2008].

The terms like true positive-false positive (TP-FP) spread and precision are defined as a part of this procedure considering them as significant performance metrics [Srivatsa 2008]. Later Aleskerov presented a data-mining system, “card-watch”, for fraud
detection of credit-cards. This model uses neural networks where a neural learning component behaves as an interface to a range of commercial databases. Kim and Kim observed two main causes for the intricacy of detection in credit card frauds: skewed distribution of statistics and mix of genuine and fraudulent transactions. Considering this identification, the fraud density of actual transaction information is taken as a confidence parameter and the weighted fraud score is generated to lessen the number of misdetections [Srivatsa 2008].

Brause implemented a new approach to achieve high fraud reporting that employs superior data mining practices and neural network procedures. Then, a mutual design for fraud detection of credit-card transactions was introduced by Chiu and Tsai that incorporates the strategies of web services and data mining procedures. In this scenario, the banks that are involved share the information related to the frauds in a varied and circulated situations. In order to have a proper medium of data exchange several web services methods are used. Stolfo and Prodromidis introduced an agent-based technique that uses distributed learning for fraud detections in credit card operations. From the name “agent-based technique” only once can presume that this involves artificial intelligence. In order to attain high precision, this procedure combines inductive learning and metal-learning procedures [Srivatsa 2008]. A game-theoretic method to detect credit card frauds has been lately proposed by Vatsa. In this model, communication between the attacker and the FDS will be as a multi-stage game played between two players wherein both try to exploit.
1.3.1 **Background and related work:**

Apart from the above mentioned credit card fraud detection techniques there are some of the recent credit card fraud detection techniques that gained attention. The following is the explanation in brief about each of these techniques:

1.3.1.1 **Fusion of Dempster–Shafer theory and Bayesian learning:**

For credit card fraud detection, this approach is a cross technique that merges the results obtained from present and precedent behavior. Any credit card owner has certain spending pattern for his purchases online that are recorded in his transactions account. This credit card fraud detection system comprises of mainly four elements:

I. **Rule-based filter:** the doubt level of every transaction that is made is extracted depending on the variations from the normal form of spending patterns.

II. **Dempster–Shafer adder:** in this component, all the transactions that are doubtful obtained by rule-based filter are combined to form a primary belief.

III. **Transaction history database:** here all the values formed as a primary belief are combined to form on the whole belief by its theory.

IV. **Bayesian learner:** here once after any transaction is believed to be suspicious, it is strengthened with fraudulent or weakened with genuine transaction.

This approach has high accuracy and also improves the fraud detection rate when compared with previous credit card detection techniques. The only issue with this mechanism is, it is very expensive and processing speed is less. The following figure-1 represents the architectural model of this mechanism.
1.3.12 BLAST-SSAHA in credit card fraud detection:

BLAH-FDS algorithm is the improved form comprises of BLAST and SSAHA algorithm. These two algorithms are pretty much proficient sequence aligning algorithms in detecting credit card frauds. In the sequence alignment of BLAH-FDS algorithm, there
are two stages where a profile analyzer obtains the correspondence between the transactions that are incoming in sequence with all the past and sequence of genuine transactions made in the past. The abnormal transactions detected by the profile analyzer are then passed into a deviation analyzer for checking with the past fraudulent transactions behavior if present. Thus based on these two analyzers a conclusion is drawn and final decision is taken. The performance of this mechanism in detecting the credit card frauds is good and its accuracy is high. Also processing speed is fast but the problem using this credit card fraud detection approach is that it cannot detect the duplicate transactions or cloned credit card frauds. The following figure-2 represents the architectural model of this mechanism.

Figure-2: Architecture of BLAST and SSAHA Fraud Detection System

[Edwin 2011]
1.3.13 Credit Card Fraud Detection using Hidden Markov Model (HMM):

The hidden markov model mechanism in detecting credit card frauds is a double embedded stochastic process. Here if any of the incoming transactions are not accepted by the trained hidden markov model with sufficient probability then it is considered as a fraudulent transaction. Here, the system has two phases of processing: a) training phase and b) detection phase.

Use Of HMM For Credit Card Fraud Detection

In this model, fraud detection system at the beginning only is trained with the normal spending pattern of the credit card holder. For every transaction made, it is compared with the fraud detection system (FDS) for verification process. This FDS will take the card details, amount for the purchase made to identify whether the transaction is genuine or fraud transaction. If the transaction does not match with the information in FDS, it confirms it to be malicious and informs the bank that issued the credit card. Then the transaction is not passed further and will be declined by the bank. The credit card holder then will be contacted by the bank person and alerted about the issue. As in this mechanism already the FDS consists of the normal spending behavior of the credit card owner, it reduces the effort of bank. The main disadvantage here is false positives are high. The following is the architectural model of the HMM in detecting credit card frauds where its work process is just mentioned. This is considered as the base model in the development of this project and is enhanced by using some security levels for better performance.
1.3.14 Fuzzy Darwinian Detection of Credit Card Fraud:

This detection method of credit card frauds uses genetic programming in order to develop some fuzzy logic rules that can be helpful in determining the suspicious and non-suspicious classes of transactions. When the information related to a transaction is provided to the FDS, the system using the classifiers, will determine the transaction as either safe or suspicious. The absolute system is capable of providing good accuracy rate and less false rate. This is not applicable in the case of online transactions practically as it is highly expensive. Also, its processing speed is very less.

Figure-3: Process Flow of the HMM FDS [Edwin 2011]
1.3.15 Credit Card Fraud Detection Using Bayesian and Neural Networks:

This Bayesian and Neural Networks mechanism is an automatic credit card fraud detecting system using a machine learning approach. Both the Bayesian and Neural Networks approaches are suitable for analysis in cases of uncertainty. In general, an artificial neural network will have an inter-connected group of artificial neurons and the pattern classification of frequently used neural networks. This is referred as feed-forward network and has three layers: input layer, hidden layer and an output layer. Here all the incoming transactions are passed through these three layers known as forward propagation. The artificial neural networks will hold the training information and compares with the inward transactions where the neural networks are originally fed with
the common spend pattern and behavior of the card holder. Any suspicious transactions are sent back to the neural networks which classifies the transactions as safe and suspicious. This is where the Bayesian networks use artificial intelligence concept comprising of various methods like data mining and machine learning algorithms to bring out results. The Bayesian belief networks are very efficient in cases like where small amount of data is known and incoming information is unstable or not completely available. This helps in data identification and classification and these neural networks need not be re-programmed. These provide good accuracy but require lot of training in achieving high processing speed.

1.3.2 Evaluation of different credit card fraud detection systems:

Constraints used:

All the above discussed credit card fraud detection methods are evaluated and compared using the certain constraints: accuracy, methodology, True positive, false positive, cost and training required, supervised learning.

a) **Accuracy**: It is defined as a portion of all the number of transactions which are identified correctly. That is the genuine transactions as genuine and fraud transactions as fraud.

b) **Methodology**: This specifies the mechanism followed by the credit card FDS.

c) **True Positive (TP)**: This gives the value of division of transactions detected correctly whether genuine or fraudulent. Here it counts only if genuine transactions are detected as genuine and fraud transactions as fraud and not any other.
d) **False Positive (FP):** This gives the value of division of transactions detected wrongly whether genuine or fraudulent. Here it counts only if genuine transactions are detected as fraudulent and fraud transactions as genuine and not any other.

e) **Supervised Learning:** This is where any system is fed with some information initially from the supervised data and known as machine learning task.

Table-1: Comparison of various credit card fraud detection mechanisms. All the mechanisms are having its own pros and cons. Results show that the fraud detection systems Fusion of Dempster and Bayesian theory, and Fuzzy Darwinian have very high accuracy in terms of TP. At the same time, the processing speed is fast enough to enable on-line detection of credit card fraud in case of BLAST-SSAHA Hidden Markov Model, and Bayesian and Neural Networks.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Fusion of Dempster–Shafer theory and Bayesian learning</th>
<th>Hybridization of BLAST–SSAHA</th>
<th>Hidden Markov Model</th>
<th>Bayesian and Neural Networks</th>
<th>Fuzzy Darwinian Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Methodology</td>
<td>Machine Learning</td>
<td>Sequence Alignment</td>
<td>Hidden Markov Model</td>
<td>Artificial Intelligence, machine Learning</td>
<td>Genetic Programming, Fuzzy Logic</td>
</tr>
<tr>
<td>Fraud Detection TP</td>
<td>98%</td>
<td>86%</td>
<td>70%</td>
<td>77%</td>
<td>19%</td>
</tr>
<tr>
<td>Fraud Detection FP</td>
<td>10%</td>
<td>10%</td>
<td>20%</td>
<td>10%</td>
<td>5.76%</td>
</tr>
<tr>
<td>Processing Speed</td>
<td>Medium</td>
<td>Very High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Training Required</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supervised Learning</td>
<td>Supervised</td>
<td>Un-Supervised</td>
<td>Supervised</td>
<td>Supervised</td>
<td>Supervised</td>
</tr>
<tr>
<td>Cost</td>
<td>Expensive</td>
<td>Inexpensive</td>
<td>Quite expensive</td>
<td>Expensive</td>
<td>Highly Expensive</td>
</tr>
<tr>
<td>Accuracy</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Very High</td>
</tr>
</tbody>
</table>
1.4 Rationale

In outlook of the reality that the conservative research for the credit card fraud detection has classically started in 1984. Since then, the study and in depth research in this field of credit card fraud detection is ongoing. Every day with the emerging technologies, new problems are also arising which is making this study enduring. Initially some techniques that were proposed were failed to handle new kinds of frauds. Some techniques were complex to implement or expensive. Thus, the quest for an efficient, reliable and inexpensive technique became the main targets of researchers and led to the improvement in study and brought superior mechanisms which handled the problems to a good extent.

Currently, the bank organizations that are supported by the government are performing their research on these fraud detection mechanisms to know how they work and can be implemented by various methodologies. In the direction to improve the basic security for credit cards from the fraudulent people, this project helps in detecting the credit card frauds easily and also with high processing speed, good accuracy and that is inexpensive. Here the typical Hidden Markov Model in detecting credit card frauds is taken and improved with new additions that will overcome the problems that are observed with many other credit card fraud detection techniques.

The results obtained from this developed project are highlighted in this paper. This developed enhanced technique should be handling most of the current various kinds of credit card frauds. There is also scope of enhancing this project even more in future.
2. NARRATIVE

2.1 Problem Statement

Earlier systems and mechanisms, the credit-card frauds are detected when the credit-card user has registered a complaint, i.e., after the fraud is committed. Major disadvantage is that, this situation will result in financial loss of the credit-card owner before the fraud is detected and solved. The major issue with many of the techniques stated above is that they entail labeled information for both actual and fraud credit card transactions in order to train the classifiers [Srivatsa 2008]. Bringing out the information related to fraud transactions of credit-cards is the challenging part in the real world. In addition, the new types of credit card frauds cannot be detected effectively by those techniques for which the labeled information does not exist. Also, large data is needed for which a log is maintained that consists of all the transactions.

Presently, due to rapid and wide usage of credit-cards (physical usage and virtual usage), it is difficult to draw out how and for what the credit-cards are used. Transactions made online, their IP addresses can be captured for corroboration. Thus, when a credit-card fraud is committed, this process needs help from the cyber crime in order to investigate the case [Srivatsa 2008]. Typically this process is not completely reliable, difficult and time taking. Thus, considering the disadvantages of the above mechanisms, a new system, HMM is proposed which is easier and best way to detect the credit-card frauds.
2.2 Scope

The main goal of this project is to detect the credit card frauds, i.e., for all the transactions made online, when an incoming transaction is received, the genuine transactions should be detected as genuine and fraud transactions should be recognized as fraud and provide the results. This application’s performance is calculated using the Hidden Markov Model concept to support the study for certain assumptions made for TPs and FPs. Finally, the obtained results are plotted as a graph and represented. The application is also tested for several test case scenarios. This developed project that is enhanced form Hidden Markov Model in detecting credit card frauds compared with the typical Hidden Markov Model in detecting credit card frauds.

2.3 Functionalities of this project

This developed project will be very much helpful for the banks and other organizations that are issuing credit-cards in detecting the credit card frauds committed. This will also help the organizations that are issuing credit-cards provide better services and in gathering more and more customers in wide sense. In this process of developing the project, a prototype is designed, followed by implementation, testing, evaluations and comparison with the typical Hidden Markov Model in detecting credit card frauds is presented in this paper.

2.4 Reducing the possibility of occurrence of frauds:

Detection of frauds depending on the study of existing purchase transactions information of actual card holder is a challenging way to lessen the rate of successful
credit card frauds. As people tend to display specific behaviorist outlines, all card holders can be symbolized by a set of patterns containing data in relation to the typical purchase category, the time since the last purchase, the amount of money spent, etc. Any sought of divergences from such patterns is a probable threat to the system. The credit card frauds are a wide range term for thefts committed using the credit card as a fake source of funds for any given transaction [Srivatsa 2008]. The credit card attackers use various techniques to commit a credit card fraud. To fight against these fraud activities successfully, it is very much important to know the how the mechanisms are carried out in identifying the credit card fraud. Credit card users need to look for security policies of the web sources before sharing information and keep their account protected from possible threats. Basic security precautions like effective control over cookies, anonymous browsing, reducing computer information with-holdings, considering network address protection, using strong encrypting tools and changing passwords of all accounts often and also using passwords that are hard-to-crack can help the users from being attacked.
3. PROPOSED SYSTEM DESIGN

3.1 Enhanced Hidden Markov Model Approach in detecting Credit Card Frauds

This project is constructed by using the credit card fraud detection by Hidden Markov Model as a base model. It is developed focusing on three main constraints:

- **Accuracy**: It is defined as a portion of all the number of transactions which are identified correctly. That is the genuine transactions as genuine and fraud transactions as fraud.

- **True Positive (TP)**: This gives the value of division of transactions detected correctly whether genuine or fraudulent. Here it counts only if genuine transactions are detected as genuine and fraud transactions as fraud and not any other.

- **False Positive (FP)**: This gives the value of division of transactions detected wrongly whether genuine or fraudulent. Here it counts only if genuine transactions are detected as fraudulent and fraud transactions as genuine and not any other.

3.2 Framework

This paper introduces an enhanced form of recent and possible approach, “Hidden Markov Model (HMM)”- for credit card fraud detection, that does not need any fraud transactions information of the credit-card and still able to detect the fraud actions. This model considers the spending routines of the credit-card holder. In this, transactions of a credit card processing series are modeled by the stochastic procedure. The information related to the purchases with respect to an individual credit card holder is not identified by that particular bank’s FDS which issued the credit-card. This is the primary factor of
Markov chain, which is signified but not noticeable. The credit card transactions can be viewed or known by stochastic process which gives the series of the spending information. Here many security levels are added into the application so that the account and transactions of purchases made can be more secure. Thus, this method is a best preference over various other techniques in addressing the issues. Also there is another major benefit by choosing this technique; it will result in radical decrease in the number of False Positives (FPs). The FPs is the transactions that are detected as fraud by the FDS, but in fact which are actual and genuine transactions [Srivatsa 2008]. Finally, this paper illustrates how the HMM technique is practically useful in detecting credit-card frauds and the results are presented.

3.2.1 **In step procedure of this project development:**

The steps followed in building this project from the scratch are briefly mentioned as follows:

1. Designing and developing a novel HMM Application
2. AJAX Enabled User Interface
3. Will use Stored Procedures Development and work with Database to prevent from SQL injections.
4. Customization of Admin and User Modules
5. Security provisions for all transactions
6. Crystal Reports Generation using Reports Software
7. Setup and Deployment of enhanced HMM Application (Generate .Exe / Setup file for Remote Systems)
3.2.2 System Requirements:

The basic system requirements that are required to be met in developing this project are:

- **Hardware requirements:**
  - SYSTEM: Pentium IV Dual core
  - HARD DISK: 300 GB
  - MONITOR: 15 VGA color
  - RAM: 1GB

- **Software requirements:**
  - Operating system: Windows 7 Professional
  - Front End: Asp .Net
  - Coding Language: Visual C# .Net
  - Back-End: Sql Server
3.2.3 **System Architecture:**

The figure-5 represents this proposed project’s simple system architecture that includes different modules in the process of credit card fraud detection:

**Figure-5:** Proposed Enhanced HMM Fraud Detection System Architecture
The UML diagram representation of the proposed system architecture is represented in the following figure-6 that shows all the user functionalities:

**Figure-6: Use case diagram of Enhanced HMM Fraud Detection System Architecture**

Here, in the user module, the user can register his credit card to FDS by using ‘new card’ module, the existing user can directly login to make transactions using ‘login’ module, to store or modify any personal information, the user can use ‘store info’ module, to make transactions and generate payments, ‘transaction’ module can be used and finally, to verify the transaction made using credit card is done using the ‘verification’ module.
Figure-7: Sequence diagram of Enhanced HMM Fraud Detection System

Architecture

Here, the process involved in credit card fraud detection using the enhanced HMM is represented in sequential manner. In the user module, when the user can registers with new credit card to FDS by using ‘new account’ module, then as an existing user can directly login to make transactions using ‘login’ module and make transactions that are done in ‘transaction’ module and the verification of the transaction made using credit
card is done using the ‘verification’ module with the help of ‘security’ module. Finally thus a complete transaction can be made successfully.

3.3 Proposed Mechanism

The project is classified in to multiple phases, where in the first phase the application is designed and developed from typical Hidden Markov Model in detecting credit card frauds. In the second phase, the developed application is made user friendly that can be easily used by organizations issuing credit cards and the credit card users to detect credit card frauds. At each phase, the application is tested and in the final phase, the application is tested wholly as one unit to check that its meeting its target constraints.
4. FUNCTIONALITIES OF THE APPLICATION

The project application consists of two main modules and is described in the following section:

4.1 Modules Description

The following are the modules used in the project: Admin and User modules. In the Admin module, the administrator takes care of the user accounts and all the genuine and fraud transactions. Whenever, a fraud is detected, immediately a notice to the user will be given through an email. In case, if a genuine user’s transaction is detected as fraud and then if the user requests the administrator, the blocked credit-card will be released by the administrator and user can use it again normally.

The following set of figures will represent the administrator module functions in the application in handling the users, keeping track of blocked users and the administrator’s account.
Figure-8: Admin Login Page

Here, the figure-8 represents the admin interface in the project application where in the administrator can login with his credentials to manage his/her personal account as well as carry out other functionalities.
Figure-9: Admin view of credit card user accounts

Here, the figure-9 represents the admin interface in the project application where in the administrator is able to view all the users who are registered to the credit card FDS. Here the user accounts are handled by the administrator as per the requirements and situations.
Figure-10: Admin view of blocked users

Here, the figure-10 represents the admin interface in the project application where in the administrator can view all the blocked user accounts whose transactions were not passed because of suspicious reasons.
In the User Module again the following operations can be performed with certain sub-modules: 1. New user registration, 2. Login, 3. Security information, 4. Transaction and 5. Verification. The following is the in detail explanation of each module:

4.1.1 New User Registration:

In this module, the customer will provide their personal information to register as a new user. The information is all about their personal and contact details. They can create their own login and password for their future use of the card.

![New User Registration Page](image)

Figure-11: New User Registration Page

Here, the figure-11 represents the new user interface in the project application where in the new user who would like to get registered to credit card FDS can provide their personal information and get registered to the system.
Table-2: The following table-2 represents the fields used in the process of new user registration. Each field has its own criteria and type of value to be specified. All these fields are to be filled in by the new user when getting registered to the credit card FDS for the first time only. This information provided only will be stored is what the maintained in the database as a user’s account and becomes helpful in making the transactions.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RegId</td>
<td>Registration ID</td>
</tr>
<tr>
<td>Username</td>
<td>Name for login</td>
</tr>
<tr>
<td>Password</td>
<td>Choose password</td>
</tr>
<tr>
<td>Firstname</td>
<td>User’s Firstname</td>
</tr>
<tr>
<td>Lastname</td>
<td>User’s Lastname</td>
</tr>
<tr>
<td>E-mailId</td>
<td>User’s E-mail ID</td>
</tr>
<tr>
<td>Address</td>
<td>Place of User</td>
</tr>
<tr>
<td>PwdQue</td>
<td>Security question</td>
</tr>
<tr>
<td>PwdAns</td>
<td>Security answer</td>
</tr>
<tr>
<td>CardNo</td>
<td>Credit card Number</td>
</tr>
</tbody>
</table>

4.1.2 Login:

In this module, the card purchaser is provided with a form consisting of username and password as fields. If the purchaser types a genuine username and password, he/she will be approved and will be given access to further resources on website. All that additional resources, that they will have access to can be configured separately.
Figure-12: User Login Page

Here, the figure-12 represents the home page in the project application where in the user can login with his/her credentials to manage his/her personal account as well as to make transactions.
Here, the figure-13 represents the user interface in the project application where in the user who would like to view his profile and account details can view them here and also modifications can be done.

4.1.3 Security information:

In this module, it will get the information of the credit-card purchaser in detail and it stores in database. If the card lost then this module will give out the form which helps in investigation. It has a set of questions where the card owner has to answer correctly to move to the transaction section. It contains entities, a trusted means to user, secure, search, process, and exchange personal and/or confidential information.
Figure-14: First level security testing

Here, the figure-14 represents user interface in the project application where in the user has to provide the credit card number for verification and answer the security question for security testing. The credit card fraud detection is based on this level of security questions initially.
Figure-15: User interface at second level of security

Here, the figure-15 represents user interface in the project application where in the user has to provide the answers for the security questions for security testing. The credit card fraud detection is based on this level of security questions.

4.1.4 Transaction:

In this module, the method and apparatus for pre-authorizing transactions includes providing a communications device to a vendor and a credit card owner. The credit card owner initiates a credit card transaction by communicating to a credit card number, and storing therein, a distinguishing piece of information that characterizes a specific transaction to be made by an authorized user of the credit card at a later time. The information is accepted as "network data" in the data base only if a correct personal identification code (PIC) is used with the communication. The "network data" will serve
to later authorize that specific transaction. The credit card owner or other authorized user can then only make that specific transaction with the credit card. Because the transaction is pre-authorized, the vendor does not need to see or transmit a PIC.

![Image of user interface to view transactions](image)

**Figure-16: User interface to view transactions that are in process**

Here, the figure-16 represents the user interface in the project application where in the user who would like to make his/her transactions.
Figure-17: User interface to view finalized transaction

Here, the figure-17 represents the user interface in the project application where in the user who would like to use the credit card and make a payment for his/her transaction.
Table-3: Credit card verification database table

The following table-3 represents the fields used in the process of Credit card verification of user when a transaction is to be passed. Each field has its own criteria and type of value to be specified. All these fields are to be filled in by the user when making the transactions. This information verifies the credit card user account with the details provided during registration and confirms if no suspicions.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CardNo</td>
<td>Credit card number</td>
</tr>
<tr>
<td>AcNo</td>
<td>Number for login into account</td>
</tr>
<tr>
<td>Bankname</td>
<td>Specifies bank name</td>
</tr>
<tr>
<td>CustomerName</td>
<td>Username</td>
</tr>
<tr>
<td>Address</td>
<td>Place of User</td>
</tr>
<tr>
<td>Cardtype</td>
<td>Choose bank organization that issued the card</td>
</tr>
<tr>
<td>Transactionplace</td>
<td>Security answer</td>
</tr>
<tr>
<td>TransAmount</td>
<td>Give the amount of per transaction</td>
</tr>
<tr>
<td>DateTime</td>
<td>Specifies date and time</td>
</tr>
</tbody>
</table>

4.1.5 Verification:

In this module, verification information is provided with respect to a transaction between an initiating party and a verification-seeking party, the verification information being given by a third, verifying party, based on confidential information in the possession of the initiating party. In verification the process will seeks card number and if
the card number is correct the relevant process will be executed. If the number is wrong, mail will be sent to the user saying the card no has been block and he can’t do the further transaction.

Table-4: Transaction verification database table

The following table-4 represents the fields used in the process of making transactions by user. Each field has its own criteria and type of value to be specified. All these fields are to be filled in by the user while making a transaction using the credit card. This information will be used for analysis and in detecting the credit card frauds.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TId</td>
<td>Transaction ID</td>
</tr>
<tr>
<td>HintQue</td>
<td>Security question</td>
</tr>
<tr>
<td>HintAns</td>
<td>Security answer</td>
</tr>
<tr>
<td>SecQue</td>
<td>Security question</td>
</tr>
<tr>
<td>Secpwd</td>
<td>Security answer</td>
</tr>
<tr>
<td>TransQue</td>
<td>Security question</td>
</tr>
<tr>
<td>Transpwd</td>
<td>Security answer</td>
</tr>
</tbody>
</table>
5. TESTING AND IMPLEMENTATION

5.1 Testing

- Testing is a process of executing a program with intent of finding an error.
- Testing presents an interesting anomaly for the software engineering.
- The goal of the software testing is to convince system developer and customers that the software is good enough for operational use. Testing is a process intended to build confidence in the software.
- Testing is a set of activities that can be planned in advance and conducted systematically.
- Testing is a set of activities that can be planned in advance and conducted systematically.
- Software testing is often referred to as verification & validation.

5.2 Types of testing

The various types of testing are:

- White Box Testing
- Black Box Testing
- Unit Testing
- Integration Testing
- Validation Testing
• Output Testing
• User Acceptance Testing

5.2.1 White box testing:

• It is also called as glass-box testing. It is a test case design method that uses the control structure of the procedural design to derive test cases.

• Using white box testing methods, the software engineer can derive test cases that:
  1. Guarantee that all independent parts within a module have been exercised at least once,
  2. Exercise all logical decisions on their true and false sides.

5.2.2 Black box testing:

• It’s also called as behavioral testing. It focuses on the functional requirements of the software.

• It is complementary approach that is likely to uncover a different class of errors than white box errors.

• A black box testing enables a software engineering to derive a set of input conditions that will fully exercise all functional requirements for a program.

5.2.3 Unit testing:

In this testing we test each module individually and integrate with the overall system. Unit testing focuses verification efforts on the smallest unit of software design in the module. This is also known as module testing.
The module of the system is tested separately. This testing is carried out during programming stage itself. In this testing step each module is found to working satisfactorily as regard to the expected output from the module. There are some validation checks for fields also. It is very easy to find error debut in the system.

5.2.4 Integration testing:

Data can be lost across an interface; one module can have an adverse effort on the other sub functions when combined may not produces the desired major functions. Integrated testing is the systematic testing for constructing the uncover errors within the interface. The testing was done with sample data. The Developed system has run successfully for this sample data. The need for integrated test is to find the overall system performance.

5.2.5 Validation testing:

At the culmination of the black box testing, software is completely assembled as a package, interfacing errors have been uncovered and corrected and a final series of software tests. That is, validation tests begin, validation testing can be defined many ways but a simple definition is that validation succeeds when the software functions in manner that can be reasonably expected be the customer. After validation test has been conducted one of the two possible conditions exists. The functions or performance characteristics confirm to specification and are accepted.
5.2.6 Output testing:

After performance of the validation testing, the next step is output testing of the proposed system since no system could be useful if it does not produce the required output in the specific format. Asking the user about the format required by system tests the output displayed or generated by the system under consideration.

Here the output format is considered the of screen display. The output format on the screen is found to be correct as the format was designed in the system phase according to the user need. For the hard copy also the output comes out as specified by the user. Hence the output testing does not result in any correction in the system.

5.2.7 User acceptance testing:

Some of my friends were who tested this module suggested that this was really a user friendly application and giving good processing speed.

- Testing used in this project:
  - Unit Testing
  - Integration Testing
  - Validation Testing
  - Output Testing
  - User Acceptance Testing
5.3 Test cases:

5.3.1: Test Case-1: Successful New User Registration

Here the following things are considered and verified:

- New user is able to open the page for registration
- New user is able to enter all the required information
- New user is able to register successfully.

**Figure-18: New User Registration Page**

Here, the figure-18 represents the new user interface in the project application where in the new user who would like to get registered to credit card FDS can provide their personal information and get registered to the system.
5.3.1: Test Case-2: Successful existing user login

In this scenario, the following things are considered and verified:

- The existing user should be able to view the login dialog box
- User should be able to enter the login username and password
- Should be able to successfully login to the account
- Should be able to view his/her account

![User Login Page](image)

**Figure-19: User Login Page**

Here, the figure-19 represents the home page in the project application where in the user can login with his/her credentials to manage his/her personal account as well as to make transactions.
Figure-20: User account page

Here, the figure-20 represents the user interface in the project application where in the user who would like to view his profile and account details can view them here and also modifications can be done.
5.3.1: Test Case-3: Successful Administrator Login

- The administrator should be able to view the login dialog box
- Administrator should be able to enter the login username and password
- Should be able to successfully login to the account
- Should be able to view his/her account
- Should be able to view all the users registered to the FDS
- Should be able to view blocked credit card users with details
- Should be able to send a notification through e-mail incase of detected fraud transaction of any user
- Should be able to release the user if it is a false positive upon request.

Figure-21: Admin Login Page
Here, the figure-21 represents the admin interface in the project application where in the administrator can login with his credentials to mange his/her personal account as well as carry out other functionalities.

Figure-22: Administrator interface showing his/her profile page

Here, the figure-22 represents the administrator interface with all the functions that can be performed by an administrator.
Figure-23: Administrator interface showing credit card user accounts

Here, the figure-23 represents the admin interface in the project application where in the administrator is able to view all the users who are registered to the credit card FDS. Here the user accounts are handled by the administrator as per the requirements and situations.
Figure-24: Administrator interface view of blocked users

Here, the figure-24 represents the admin interface in the project application where in the administrator can view all the blocked user accounts whose transactions were not passed because of suspicious reasons.

5.3.1: Test Case-4: Making a successful genuine transaction

- Upon login, the user should be able to make any purchases
- After completion of purchases, the transaction should be finalized to pay using credit card
- Enter the correct credit card number, which gets verified using the enhanced Hidden Markov Model concept
- Enter the correct transaction place as an answer for the first level of security question
- Successfully directed to new page with second level of security questions
- Enter the correct information for the second level of security questions
- Look for notification saying successful transaction
- Check for an e-mail notification of the successful genuine transaction mailed by the administrator

![User interface to view transactions that are in process](image)

**Figure-25: User interface to view transactions that are in process**

Here, the figure-25 represents the user interface in the project application where in the user who would like to make his/her transactions.
Figure-26: User interface to view finalized transaction

Here, the figure-26 represents the user interface in the project application where in the user who would like to use the credit card and make a payment for his/her transaction.
Figure-27: First level security testing

Here, the figure-27 represents user interface in the project application where in the user has to provide the credit card number for verification and answer the security question for security testing. The credit card fraud detection is based on this level of security questions initially.
Figure-28: User interface at second level of security

Here, the figure-28 represents user interface in the project application where in the user has to provide the answers for the security questions for security testing. The credit card fraud detection is based on this level of security questions.

Figure-29: Notification for making a successful transaction

Here, the figure-29 represents the notification message confirming to the user who made the successful transaction.
Figure-30: Notification for e-mail message sent

Here, the figure-30 represents the notification message confirming that an e-mail has been sent by the administrator to the user who made the successful transaction.

5.3.1: Test Case-5: Making a successful fraud transaction

- Upon login, the user should be able to make any purchases
- After completion of purchases, the transaction should be finalized to pay using credit card
- Enter the wrong credit card number and check for the message saying ‘Sorry card number not verified. Please try again’
- Then enter the correct credit card number, which gets verified using the enhanced Hidden Markov Model concept
- Enter the wrong transaction place as an answer for the first level of security question and observe the error message
- Then enter the correct transaction place as an answer for the first level of security question
- Successfully directed to new page with second level of security questions
- Enter the wrong information in any one or more fields for the second level of security questions and observe the error message
- Look for notification saying transaction aborted and also saying account disabled
- Check for an e-mail notification of the fraud transaction mailed by the administrator

Figure-31: User interface to view transactions that are in process

Here, the figure-31 represents the user interface in the project application where in the user who would like to make his/her transactions.
Figure-32: User interface to view finalized transaction

Here, the figure-32 represents the user interface in the project application where in the user who would like to use the credit card and make a payment for his/her transaction.
Figure-33: First level security testing

Here, the figure-33 represents user interface in the project application where in the user has to provide the credit card number for verification and answer the security question for security testing. The credit card fraud detection is based on this level of security questions initially.
Figure-34: Second Security Levels testing

Here, the figure-34 represents user interface in the project application where in the user has to provide the answers for the security questions for security testing. The credit card fraud detection is based on this level of security questions.

Figure-35: Notification message

Here, the figure-35, represents the notification message and obtained when one or more of the security questions are answered incorrectly.
Figure-36: Notification Message

Here, the figure-36, represents notification message saying that the user credit card usage service is disabled with suspicion and need to contact administrator for further usage.

Figure-37: Mail Confirmation message

Here, the figure-37 represents the message obtained when an e-mail notification is send to user from the administrator.
6. RESULTS

Based on the results obtained from several test cases, a comparative analysis study of existing HMM and this proposed enhanced HMM is done and represented as chart and also comparison table as follows: (considered for a random set of TP and FP transactions)

<table>
<thead>
<tr>
<th>TP</th>
<th>FP</th>
<th>Accuracy</th>
<th>New Accuracy</th>
<th>N</th>
<th>TP%</th>
<th>FP%</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>2</td>
<td>0.9973</td>
<td>1.875</td>
<td>32</td>
<td>93.75</td>
<td>6.25</td>
</tr>
<tr>
<td>35</td>
<td>3</td>
<td>0.921053</td>
<td>1.94205263</td>
<td>38</td>
<td>92.10536</td>
<td>7.894736</td>
</tr>
<tr>
<td>40</td>
<td>5</td>
<td>0.888889</td>
<td>1.77777778</td>
<td>45</td>
<td>88.8889</td>
<td>11.1111</td>
</tr>
<tr>
<td>45</td>
<td>1</td>
<td>0.976361</td>
<td>1.956521739</td>
<td>46</td>
<td>97.62099</td>
<td>2.37913</td>
</tr>
<tr>
<td>50</td>
<td>9</td>
<td>0.847958</td>
<td>1.69415254</td>
<td>59</td>
<td>84.79576</td>
<td>15.25424</td>
</tr>
<tr>
<td>55</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>55</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>60</td>
<td>5</td>
<td>0.933077</td>
<td>1.94613846</td>
<td>65</td>
<td>93.30789</td>
<td>6.692938</td>
</tr>
<tr>
<td>65</td>
<td>6</td>
<td>0.915491</td>
<td>1.83064915</td>
<td>71</td>
<td>91.5483</td>
<td>8.450704</td>
</tr>
<tr>
<td>70</td>
<td>10</td>
<td>0.9373</td>
<td>1.75</td>
<td>80</td>
<td>93.73</td>
<td>6.27</td>
</tr>
<tr>
<td>75</td>
<td>1</td>
<td>0.966942</td>
<td>1.97884211</td>
<td>76</td>
<td>96.69411</td>
<td>3.30589</td>
</tr>
<tr>
<td>80</td>
<td>2</td>
<td>0.97561</td>
<td>1.951239512</td>
<td>82</td>
<td>97.56096</td>
<td>2.439024</td>
</tr>
<tr>
<td>85</td>
<td>12</td>
<td>0.876289</td>
<td>1.75257732</td>
<td>97</td>
<td>87.62087</td>
<td>12.37113</td>
</tr>
<tr>
<td>90</td>
<td>4</td>
<td>0.957447</td>
<td>1.914893617</td>
<td>94</td>
<td>95.74468</td>
<td>4.255319</td>
</tr>
<tr>
<td>95</td>
<td>27</td>
<td>0.778889</td>
<td>1.537307049</td>
<td>112</td>
<td>77.88895</td>
<td>22.1115</td>
</tr>
<tr>
<td>100</td>
<td>17</td>
<td>0.854701</td>
<td>1.709401279</td>
<td>117</td>
<td>85.47019</td>
<td>14.52981</td>
</tr>
</tbody>
</table>

Average: 91.40204, 8.597956

Figure-38: Obtained graph from considering a random set of TP and FP transactions and generated for accuracy. Comparison is done for accuracy for existing HMM (accuracy) and enhanced HMM (new accuracy)
Table-5: Comparison table of existing HMM and this proposed enhanced HMM

The following table-5 represents a comparative analysis study of existing HMM and this proposed enhanced HMM is done and represented as comparison table considering several factors.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Hidden Markov Model</th>
<th>Enhanced Hidden Markov Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Methodology</td>
<td>Hidden Markov Model</td>
<td>Enhanced Hidden Markov Model</td>
</tr>
<tr>
<td>Fraud Detection</td>
<td>TP 70%</td>
<td>91%</td>
</tr>
<tr>
<td></td>
<td>FP 20%</td>
<td>8.5%</td>
</tr>
<tr>
<td>Processing Speed</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Training Required</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supervised Learning</td>
<td>Semi Supervised</td>
<td>Semi Supervised</td>
</tr>
<tr>
<td>Cost</td>
<td>Quite expensive</td>
<td>Inexpensive</td>
</tr>
<tr>
<td>Accuracy</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>
7. CONCLUSION

In this project, an enhanced form of Hidden Markov Model (HMM) is implemented and presented, that does not necessitate fraud signatures and however is able to detect frauds by taking into account a cardholder’s spending transactions.

All incoming transactions are presented to the FDS for corroboration. FDS receives the card details and the value of purchase to verify, whether the transaction is authentic or not. The types of purchases that are done in that operation are not known to the FDS. It tries to find any incongruity in the transaction based on the spending summary of the cardholder: shipping address and billing address, etc. If FDS confirms the transaction to be of fraud, it raises an alarm, and the issuing bank declines the transaction.
BIBLIOGRAPHY AND REFERENCES


