**UPI FRAUD DETECTION USING CNN**

**ABSTRACT**

Now a day the usage of UPI has dramatically increased. As UPI becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In this project, we model the sequence of operations in UPI transaction processing using a Convolutional Neural Network (CNN) and show how it can be used for the detection of frauds. An CNN is initially trained with the normal behavior of a cardholder. If an incoming UPI transaction is not accepted by the trained CNN with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. We present detailed experimental results to show the effectiveness of our approach and compare it with other techniques available in the literature.

**CHAPTER 1**

**INTRODUCTION**

The popularity of online shopping is growing day by day. According to an ACNielsen study conducted in 2005, one-tenth of the world’s population is shopping online. Germany and Great Britain have the largest number of online shoppers, and UPI is the most popular mode of payment (59 percent). About 350 million transactions per year were reportedly carried out by Barclaycard, the largest UPI company in the United Kingdom, toward the end of the last century. Retailers like Wal-Mart typically handle much larger number of UPI transactions including online and regular purchases. As the number of UPI users rises world-wide, the opportunities for attackers to steal UPI details and, subsequently, commit fraud are also increasing. The total UPI fraud in the United States itself is reported to be $2.7 billion in 2005 and estimated to be $3.0 billion in 2006, out of which $1.6 billion and $1.7 billion, respectively, are the estimates of online fraud.

Credit-card-based purchases can be categorized into two types:

1) Physical card and

2) Virtual card.

In a physical-card-based purchase, the cardholder presents his card physically to a merchant for making a payment. To carry out fraudulent transactions in this kind of purchase, an attacker has to steal the UPI. If the cardholder does not realize the loss of card, it can lead to a substantial financial loss to the UPI company. In these cond. kind of purchase, only some important information about a card (card number, expiration date, secure code) is required to make the payment. Such purchases are normally done on the Internet or over the telephone. To commit fraud in these types of purchases, a fraudster simply needs to know the card details. Most of the time, the genuine cardholder is not aware that someone else has seen or stolen his card information. The only way to detect this kind of fraud is to analyze the spending patterns on every card and to figure out any inconsistency with respect to the “usual” spending patterns. Fraud detection based on the analysis of existing purchase data of cardholder is a promising way to reduce the rate of successful UPI frauds. Since humans tend to exhibit specific behaviouristic profiles, every cardholder can be represented by a set of patterns containing information about the typical purchase category, the time since the last purchase, the amount of money spent, etc. Deviation from such patterns is a potential threat to the system. Several techniques for the detection of UPI fraud have been proposed in the last few years.

* 1. **Literature Survey:-**

**UPI Fraud Detection:-**

UPI fraud detection has drawn a lot of research interest and a number of techniques, with special emphasis on data mining and neural networks, have been suggested. Ghosh and Reilly have proposed UPI fraud detection with a neural network. They have built a detection system, which is trained on a large sample of labelled UPI account transactions. These transactions contain exam-ple fraud cases due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud, and nonreceived issue (NRI) fraud. Recently, Syeda et al. have used parallel granular neural networks (PGNNs) for improving the speed of data mining and knowledge discovery process in UPI fraud detection. A complete system has been implemented for this purpose. Stolfo et al. suggest a UPI fraud detection system (FDS) using Metalearning techniques to learn models of fraudulent UPI transactions. Metalearning is a general strategy that provides a means for combining and integrating a number of separately built classifiers or models. A metaclassifier is thus trained on the correlation of the predictions of the base classifiers. The same group has also worked on a cost-based model for fraud and intrusion detection. They use Python agents for Metalearning (JAM), which is a distributed data mining system for UPI fraud detection. A number of important performance metrics like True Positive—False Positive (TP-FP) spread and accuracy have been defined by them. Aleskerov et al. present CARDWATCH, a database mining system used for UPI fraud detection. The system, based on a neural learning module, provides an interface to a variety of commercial databases. Kim and Kim have identified skewed distribution of data and mix of legitimate and fraudulent transactions as the two main reasons for the complexity of UPI fraud detection. Based on this observation, they use fraud density of real transaction data as a confidence value and generate the weighted fraud score to reduce the number of misdetections. Fan et al. suggest the application of distributed data mining in UPI fraud detection. Brause et al. have developed an approach that involves advanced data mining techniques and neural network algorithms to obtain high fraud coverage. Chiu and Tsai have proposed Web services and data mining techniques to establish a collaborative scheme for fraud detection in the banking industry. With this scheme, participating banks share knowledge about the fraud patterns in a heterogeneous and distributed environment. To establish a smooth channel of data exchange, Web services techniques such as XML, SOAP, and WSDL are used. Phua et al. have done an extensive survey of existing data-mining-based FDSs and published a comprehensive report. Prodromidis and Stolfo use an agent-based approach with distributed learning for detect-ing frauds in UPI transactions. It is based on artificial intelligence and combines inductive learning algorithms and Metalearning methods for achieving higher accuracy. Phua et al. suggest the use of metaclassifier similar to in fraud detection problems. They consider naive Bayesian C4.5, and Back Propagation neural networks as the base classifiers. A metaclassifier is used to determine which classifier should be considered based on skewness of data. Although they do not directly use UPI fraud detection as the target application, their approach is quite generic. Vatsa et al. have recently proposed a game-theoretic approach to UPI fraud detection. They model the interaction between an attacker and an FDS as a multistage game between two players, each trying to maximize his payoff. The problem with most of the abovementioned approaches is that they require labelled data for both genuine, as well as fraudulent transactions, to train the classifiers. Getting real-world fraud data is one of the biggest problems associated with UPI fraud detection. Also, these approaches cannot detect new kinds of frauds for which labelled data is not available. In contrast, we present a Hidden Markov Model (AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING)-based UPI FDS, which does not require fraud signatures and yet is able to detect frauds by considering a cardholder’s spending habit. We model a UPI transaction processing sequence by the stochastic process of an AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING. The details of items purchased in individual transactions are usually not known to an FDS running at the bank that issues UPI to the cardholders. This can be represented as the underlying finite Markov chain, which is not observable. The transactions can only be observed through the other stochastic process that produces the sequence of the amount of money spent in each transaction. Hence, we feel that AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING is an ideal choice for addressing this problem. Another important advantage of the AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING-based approach is a drastic reduction in the number of False Positives (FPs)—transactions identified as malicious by an FDS although they are actually genuine. Since the number of genuine transactions is a few orders of magnitude higher than the number of malicious transactions, an FDS should be designed in such a way that the number of FPs is as low as possible. Otherwise, due to the “base rate fallacy” effect, bank administrators may tend to ignore the alarms. To the best of our knowledge, there is no other published literature on the application of AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING for UPI fraud detection.

**AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING Background:-**

An AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING is a double embedded stochastic process with two hierarchy levels. It can be used to model much more complicated stochastic processes as compared to a traditional Markov model. An AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING has a finite set of states governed by a set of transition probabilities. In a particular state, an outcome or observation can be generated according to an associated probability distribution. It is only the outcome and not the state that is visible to an external observer. AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING-based applications are common in various areas such as speech recognition, bioinformatics, and genomics. In recent years, Joshi and Phoba have investigated the capabilities of AUTO ENCODER, LOCAL OUTLIER FACTOR, KMEANS CLUSTERING in anomaly detection.

**Title: BLAST-SSAHA Hybridization for UPI Fraud Detection Author:** Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar **Description:**

A phenomenal growth in the number of UPI transactions, especially for online purchases, has recently led to a substantial rise in fraudulent activities. Implementation of efficient fraud detection systems has thus become imperative for all UPI issuing banks to minimize their losses. In real life, fraudulent transactions are interspersed with genuine transactions and simple pattern matching is not often sufficient to detect them accurately. Thus, there is a need for combining both anomaly detection as well as misuse detection techniques. In this paper, we propose to use two-stage sequence alignment in which a profile analyzer (PA) first determines the similarity of an incoming sequence of transactions on a given UPI with the genuine cardholder's past spending sequences. The unusual transactions traced by the profile analyzer are next passed on to a deviation analyzer (DA) for possible alignment with past fraudulent behavior. The final decision about the nature of a transaction is taken on the basis of the observations by these two analyzers. In order to achieve online response time for both PA and DA, we suggest a new approach for combining two sequence alignment algorithms BLAST and SSAHA

**TITLE: Fast algorithms for mining association rules in large databases AUTHOR:** R. AGRAWAL AND R. SRIKANT.

## DESCRIPTION:

The major consequences are loss of billions of dollars each year, investor confidence or corporate reputation. A study area called Financial Fraud Detection (FFD) is obligatory, in order to prevent the destructive results caused by financial fraud. In this study, we propose a new method based on Grammar-based Genetic Programming (GBGP), multi-objectives optimization and ensemble learning for solving FFD problems. We comprehensively compare the proposed method with Logistic Regression (LR), Neural Networks (NNs), Support Vector Machine (SVM), Bayesian Networks (BNs), Decision Trees (DTs), AdaBoost, Bagging and LogitBoost on four FFD datasets. The experimental results showed the effectiveness of the new approach in the given FFD problems including two real-life problems. The major implications and significances of the study can concretely generalize for two points. First, it evaluates a number of data mining techniques by the given real-life classification problems. Second, it suggests a new method based on GBGP, NSGA-II and ensemble learning.

**TITLE: Why we tag: Motivations for annotation in mobile and online media AUTHOR:** M. AMES AND M. NAAMAN.

## DESCRIPTION:

Financial fraud is a criminal act, which violates the law, rules or policy to gain unauthorized financial benefit. The major consequences are loss of billions of dollars each year, investor confidence or corporate reputation. A study area called Financial Fraud Detection (FFD) is obligatory, in order to prevent the destructive results caused by financial fraud. In this study, we propose a new method based on Grammar-based Genetic Programming (GBGP), multi- objectives optimization and ensemble learning for solving FFD problems. We comprehensively compare the proposed method with Logistic Regression (LR), Neural Networks (NNs), Support Vector Machine (SVM), Bayesian Networks (BNs), Decision Trees (DTs), AdaBoost, Bagging and LogitBoost on four FFD datasets. The experimental results showed the effectiveness of the new approach in the given FFD problems including two real-life problems. The major implications and significances of the study can concretely generalize for two points. First, it evaluates a number of data mining techniques by the given real-life classification problems. Second, it suggests a new method based on GBGP, NSGA-II and ensemble learning.

## TITLE: Fuzzy Darwinian detection of UPI fraud

### **AUTHOR:** PETER J. BENTLEY, JUNGWON KIM, GIL-HO JUNG AND JONG-UK CHOI

**DESCRIPTION:**

By the exponential growth of UPI user the fraudulent transactions also have increased dramatically. The genuine transaction and fraudulent transactions are almost similar, so it is very hard to discover a fraudulent transaction form the genuine one. In this paper we have proposed fraud detection algorithm based on Fuzzy-ID3. Intermediate nodes we split using attribute having highest information gain. The leaf nodes classifies the transactions as fraud, doubtful or normal. Experimental result exhibits that the technique is efficient one in detecting frauds.

## Title: UPI fraud detection using Big data

### **Author:** Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick,

**Description:**

Big data is the frontier of a firm’s ability to store, process and access all the data and it needs to operate effectively for decision making, reduce risks and serve customer. The 3 main characterstic of big data volume (data quantity), velocity (data speed), variety (data type), Big data can handle more than 1 million customer transaction per hour. Hadoop is an apache top level project, open source implementation of frameworks for reliable, scalable, distributed computing and data storage. It is a flexible and highly-available architecture for large scale computation and data processing on a network of commodity hardware. Big data helps financial institutions to approach fraud in different ways and possibly get different results. For the UPI fraud detection we need bank, transaction and customer data.

# SURVEY TABLE

|  |  |  |  |
| --- | --- | --- | --- |
| **SOURCE** | **SAMPLE/STUDY DESCRIPTION** | **PURPOSE** | **RESULTS** |
| BLAST-SSAHA  Hybridization for UPI Fraud Detection  Author: Amlan  Kundu, Suvasini  Panigrahi, Shamik Sural and Arun K. Majumdar | A phenomenal growth in the number of credit card  transactions, especially for online purchases, has recently led to a substantial rise in fraudulent activities. Implementation of efficient fraud detection systems has thus become imperative for all credit card issuing banks to minimize their losses | The transactions and simple pattern matching is not often sufficient to detect them accurately. Thus, there is a need for combining both anomaly detection as well as misuse detection techniques | In order to achieve online response time for both PA and DA, we suggest a new approach for  combining two sequence alignment algorithms BLAST and SSAHA |
| Title: Fast algorithms for mining association rules in large databases.  Author: R. Agrawal and R. Srikant.  . | Financial fraud is a criminal act, which violates the law, rules or policy to gain unauthorized financial benefit. The major consequences are loss of billions of dollars each year, investor confidence or corporate reputation | , in order to prevent the destructive results caused by financial fraud. In this study, we propose a new method based on Grammar-based Genetic Programming (GBGP), multi- objectives optimization and ensemble learning for solving FFD problems | First, it evaluates a number of data mining techniques by the given real-life classification problems. Second, it suggests a new method based on GBGP, NSGA-II and  ensemble learning. |

|  |  |  |  |
| --- | --- | --- | --- |
| Title: Why we tag: Motivations for annotation in mobile and online media.  Author: M. Ames and  M. Naaman. | Financial fraud is a criminal act, which violates the law, rules or policy to gain unauthorized financial benefit. The major consequences are loss of billions of dollars each year, investor confidence or corporate reputation. | The comprehensively compare the proposed method with Logistic Regression (LR), Neural Networks  (NNs), Support  Vector Machine  (SVM), Bayesian  Networks (BNs), Decision Trees (DTs), AdaBoost, Bagging and LogitBoost on four FFD datasets. | The major  implications and significances of the study can concretely generalize for two points. First, it evaluates a number of data mining  techniques by the given real-life classification problems. Second, it suggests a new method based on GBGP, NSGA-II and  ensemble |
| Title: “Fuzzy Darwinian Detection of UPI Fraud Author: Peter J. Bentley, Jungwon Kim, Gil-Ho Jung and Jong-Uk Choi | The exponential growth of UPI user the fraudulent transactions also have increased dramatically | The genuine transaction and fraudulent transactions are almost similar, so it is very hard to discover a fraudulent transaction | In this paper we have proposed fraud detection algorithm based on Fuzzy-ID3. Intermediate nodes we split using  attribute having highest information gain. |

|  |  |  |  |
| --- | --- | --- | --- |
| **SOURCE** | **SAMPLE/STUDY DESCRIPTION** | **PURPOSE** | **RESULTS** |
| Title: Credit card fraud detection using Bayesian and neural networks,  Author: Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick | Financial fraud is a criminal act, which violates the law, rules or policy to gain unauthorized financial benefit. | The major  consequences are loss of billions of dollars each year, investor confidence or corporate reputation. A study area called Financial Fraud Detection (FFD) is obligatory | evaluates a number of data mining  techniques by the given real-life classification problems. Second, it suggests a new method based on GBGP, NSGA-II and  ensemble learning. |

**CHAPTER 3**

**SYSTEM ANALYSIS**

**EXISTING SYSTEM**

All the existing method to detect the UPI was on the mode like the detection occurs only after the complaint of the card holder about fraud done. It is not a convenient way to avoid the loss happens to the cad holder. After getting the complaint they detected the fraud on the basis of the IP address. For this they need the help of the Cyber crime to detect the fraud and make action on it. It takes so much man power.

***Disadvantages***

1. The main disadvantage of the existing system is the detection occurs only after gets a written complaint.
2. In the existing system there is physical inconvenience exists.
3. The period occurs to detect the fraud will cause so many losses to the card holder.
4. There is no particular security system in the existing so a hacker can easily access others card.

**PROPOSED SYSTEM**

Here we are introducing a project for the UPI fraud detection using Convolutional Neural Network (CNN). It is done on the basis of the spending profile of the card holder. The usual spending of the cardholder is being checked by the FDS (Fraud Detection system) in the bank .The system checks all the spending of the user. When it turns unusual the method blocks the transaction on the card. And it alerts the bank. It occurs automatically. It doesn’t need any man power.

***Advantages***

1) The main advantage is that the detection occurs much faster than any other method.

2) In all the existing systems the real card holder should checked for the Fraud detection. But in our method there is no need of the physical inconveniences of the card holder. All the checking and the detection occur automatically.

3) This project needs no man power for the detection.

4) This project provides most accurate method in UPI fraud detection.

**MODULES**

There are five main types of modules in the fraud detection

* Register.
* Sign in.
* Security.
* User side.
* Purchase.

**MODULE DESCRIPTION**

**1. Login**

The Login module gives a login form to the user with a user name and password. The user can access the special features only when they enters correct user name and password

**2. Register**

In this module the hard holder registers new card. For this they are gives their personal details, UPI details. In this module the user also can fix security questions and answers for security purpose

**3. Security**

In this module we provide special features are the user can fix a spending limit, set security questions and answers. The purpose of this segment is this security questions arise when the user exceeds the spending limit. The user can access further only when they answer these questions correctly.

**4. User side**

This module is for the user to view the home page, purchase things or view reports. This report deals with what the user did with the UPI like purchase, transactions etc.

**5. Purchase**

In this module all the transaction process like purchase with the UPI occurs. The user submits the total amount to be credited after the completion of purchase. The transaction occurs only when the total amount is below the spending limit. If it exceeds the limit security questions are asked. The user can proceed only when the answers are correct. Otherwise the card will be blocked.

**SYSTEM REQUIREMENTS**

**Hardware Requirements:**

* SYSTEM : Pentium IV 2.4 GHz
* HARD DISK : 40 GB
* FLOPPY DRIVE : 1.44 MB
* MONITOR : 15 VGA colour
* MOUSE : Logitech.
* RAM : 256 MB
* KEYBOARD : 110 keys enhanced.

**Software Requirements:**

* Operating system : Windows
* Front End : Anaconda IDE
* Coding Language : Python
* Back End : Sql Server

**CHAPTER 3**

**SYSTEM STUDY**

**FEASIBILTY STUDY**

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

* ECONOMICAL FEASIBILITY
* TECHNICAL FEASIBILITY
* SOCIAL FEASIBILITY

**ECONOMICAL FEASIBILITY**

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

**TECHNICAL FEASIBILITY**

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

**SOCIAL FEASIBILITY**

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity.

The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

**System Design**

Design is concerned with identifying software components specifying relationships among components. Specifying software structure and providing blue print for the document phase. Modularity is one of the desirable properties of large systems. It implies that the system is divided into several parts. In such a manner, the interaction between parts is minimal clearly specified. Design will explain software components in detail. This will help the implementation of the system. Moreover, this will guide the further changes in the system to satisfy the future requirements

**Input Design:**

Input design is the process of converting user-originated inputs to a computer-based format. Input design is one of the most expensive phases of the operation of computerized system and is often the major problem of a system.

In the project input forms are login, registration, fraud user login,security details,giving product.

OUTPUT DESIGN:

Output design generally refers to the results and information that are generated by the system for many end-users; output is the main reason for developing the system and the basis on which they evaluate the usefulness of the application.

In the project output forms are view product, viewing purchased product,connection,node information,path node.

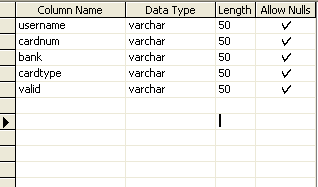
DATABASE DESIGN

The database design is a must for any application developed especially more for the data store projects. Since the chatting method involves storing the message in the table and produced to the sender and receiver, proper handling of the table is a must.

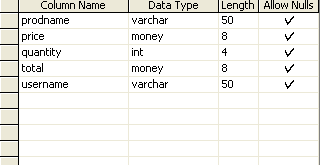
In The Project Database Designs are user resistration,connection,fraud user information, product details.

**TABLE DESIGN:**

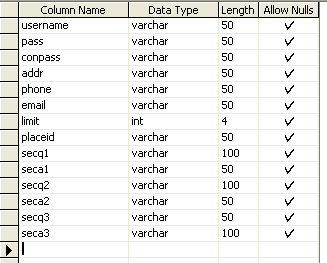
**Card details:**



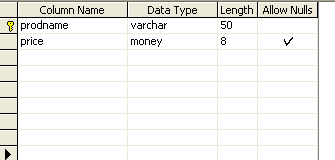
**Cart:**



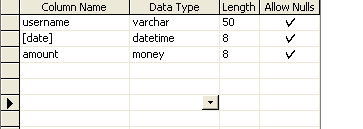
**Fraud users:**



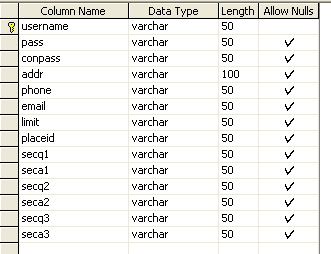
**Product details:**



**Purchasing the product:**



**Sign up:**



SYSTEM TESTING

**UNIT TESTING:**

The procedure level testing is made first. By giving improper inputs, the errors occurred are noted and eliminated. Then the web form level testing is made. For example storage of data to the table in the correct manner.

In the company as well as seeker registration form, the zero length username and password are given and checked. Also the duplicate username is given and checked. In the job and question entry, the button will send data to the server only if the client side validations are made.

The dates are entered in wrong manner and checked. Wrong email-id and web site URL (Universal Resource Locator) is given and checked.

**INTEGRATION TESTING:**

Testing is done for each module. After testing all the modules, the modules are integrated and testing of the final system is done with the test data, specially designed to show that the system will operate successfully in all its aspects conditions. Thus the system testing is a confirmation that all is correct and an opportunity to show the user that the system works.

**VALIDATION TESTING:**

The final step involves Validation testing, which determines whether the software function as the user expected. The end-user rather than the system developer conduct this test most software developers as a process called “Alpha and Beta Testing” to uncover that only the end user seems able to find.

The compilation of the entire project is based on the full satisfaction of the end users. In the project, validation testing is made in various forms. In question entry form, the correct answer only will be accepted in the answer box. The answers other than the four given choices will not be accepted.

SYSTEM IMPLEMENTATION

Implementation is the most crucial stage in achieving a successful system and giving the user’s confidence that the new system is workable and effective. Implementation of a modified application to replace an existing one. This type of conversation is relatively easy to handle, provide there are no major changes in the system.

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly.

Initially as a first step the executable form of the application is to be created and loaded in the common server machine which is accessible to the entire user and the server is to be connected to a network. The final stage is to document the entire system which provides components and the operating procedures of the system.

**CONCLUSION**

In this project, we have proposed an application of CNN in UPI fraud detection. The different steps in UPI transaction processing are represented as the underlying stochastic process of an CNN. We have used the ranges of transaction amount as the observation symbols, whereas the types of item have been considered to be states of the CNN. We 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 CNN 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.

SCOPE FOR FUTURE DEVELOPMENT

Every application has its own merits and demerits. The project has covered almost all the requirements. Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Changing the existing modules or adding new modules can append improvements. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one.

**REFERENCES**

[1] Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, “BLAST-SSAHA Hybridization for UPI Fraud Detection,” IEEE Transactions On Dependable And Secure Computing, vol. 6, Issue no. 4, pp.309-315, October-December 2009.

[2] Amlan Kundu, Suvasini Panigrahi, Shamik Sural and Arun K. Majumdar, “UPI fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning,” Special Issue on Information Fusion in Computer Security, Vol. 10, Issue no 4, pp.354- 363, October 2009.

[3] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Arun K. Majumdar, “UPI Fraud Detection using Hidden Markov Model,” IEEE Transactions On Dependable And Secure Computing, vol. 5, Issue no. 1, pp.37-48, January-March 2008.

[4] Peter J. Bentley, Jungwon Kim, Gil-Ho Jung and Jong-Uk Choi, “Fuzzy Darwinian Detection of UPI Fraud,” In the 14th Annual Fall Symposium of the Korean Information Processing Society, 14th October 2000.

[5] Sam Maes, Karl Tuyls, Bram Vanschoenwinkel, Bernard Manderick, “UPI fraud detection using Bayesian and neural networks,” Interactive image-guided neurosurgery, pp.261- 270, 1993.

[6] Amlan Kundu, S. Sural, A.K. Majumdar, “Two-Stage UPI Fraud Detection Using Sequence Alignment,” Lecture Notes in Computer Science, Springer Verlag, Proceedings of the International Conference on Information Systems Security, Vol. 4332/2006, pp.260- 275, 2006. [7] Simon Haykin, “Neural Networks: A Comprehensive Foundation,” 2nd Edition, pp.842, 1999.