2012 International Conference on Information and Network Technology (ICINT 2012)
IPCSIT vol. 37 (2012) © (2012) IACSIT Press, Singapore

Fraud Detection in Online Banking Using HMM

Sunil Mhamane [+] and L.M.R.J Lobo

Dept. Of Computer Science and Engg., Walchand Institute of Technology, Solapur, India

Abstract. As online banking becomes the most popular mode of payment for both online as well as internet based Transaction, cases of fraud associated with it are also rising. In this paper We model the sequence of operations in internet banking transaction processing using a Hidden Markov Model (HMM) and showing how it can be used for the detection of frauds. If an incoming online banking transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, we will try to ensure that genuine transactions are not rejected.

Keywords: hidden markov model, man in browser attack, transactional.

1. Introduction

1.1. Online banking

In today's world of emerging technologies, enterprises are moving towards the Internet for businesses. People are rushing towards the e-commerce applications for their day-today needs, which in turn are making the Internet very popular. Online Banking has given both an opportunity and a challenge to traditional banking. In the fast growing world,banking is a necessity, which in turn takes a lot of time from our busy schedule. Going to a branch or ATM or paying bills by paper check and mailing them out, and balancing checkbooks are all time-consuming tasks. Banking online automates many of these processes, saving time and money. For all banks, online banking is a powerful tool to gain new customers while it helps to eliminates costly paper handling and manual teller interactions in an increasingly competitive banking environment. Banks have spent generations gaining trust of their customers.

1.2. Hidden markov model

A hidden Markov model (HMM) is a statistical model in which the system being modeled is assumed to be a Markov process with unobserved state. A HMM can be considered as the simplest dynamic Bayesian network. In a regular Markov model, the state is directly visible to the observer, and therefore the state transition probabilities are the only parameters. In a hidden Markov model, the state is not directly visible, but output, dependent on the state, is visible. Each state has a probability distribution over the possible output tokens. Therefore the sequence of tokens generated by an HMM gives some information about the sequence of states. Note that the adjective 'hidden' refers to the state sequence through which the model passes, not to the parameters of the model; even if the model parameters are known exactly, the model is still 'hidden'. Hidden Markov models are especially known for their application in temporal pattern recognition such as speech, handwriting, gesture recognition, part-of-speech tagging, musical score following, partial discharges and bioinformatics[1]. A hidden Markov model can be considered a generalization of a mixture model where the hidden variables, which control the mixture component to be selected for each observation, are related through a Markov process rather than independent of each other[2].

2. Literature Review

[+] Corresponding author. Tel.: + 08149618425.
E-mail address: sunil_mhamane@yahoo.co.in.

In “Credit Card Fraud Detection Using HMM” paper, They have proposed an application of HMM in credit card fraud detection. The different steps in credit card transaction processing are represented as the underlying stochastic process of an HMM. They have used the ranges of transaction amount as the observation symbols, whereas the types of item have been considered to be states of the HMM. They have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It has also been explained how the HMM can detect whether an incoming transaction is fraudulent or not. Experimental results show the performance and effectiveness of our system and demonstrate the usefulness of learning the spending profile of the cardholders. Comparative studies reveal that the Accuracy of the system is close to 80 percent over a wide variation in the input data. The system is also scalable for handling large volumes of transactions[3].

In “credit card fraud detection with a neural network” paper, Using data from a credit card issuer, a neural network based fraud detection system was trained on a large sample of labeled credit card account transactions and tested on a holdout data set that consisted of all account activity over a subsequent two-month period of time. The neural network was trained on examples of fraud due to lost cards, stolen cards, application fraud, counterfeit fraud, mail-order fraud and NRI (non-received issue) fraud. The network detected significantly more fraud accounts (an order of magnitude more) with significantly fewer false positives (reduced by a factor of 20*)* over rule based fraud detection procedures. They discuss the performance of the network on this data set in terms of detection accuracy and earliness of fraud detection. The system has been installed on an IBM 3090 at Mellon Bank and is currently in use for fraud detection on that bank’s cmlit card portfolio[4].

In “Offline Internet Banking Fraud Detection” paper .Object of this paper is to demonstrate one successful fraud detection model which is established in Greece. Apart from the offline internet banking fraud detection system itself, which is described briefly, there scope is to present its contribution in fast and reliable detection of any “strange” transaction including fraudulent ones[5].

In “Security Analysis for Internet Banking Models” paper They stated that Internet banking fraud can be performed internally by genuine staff or externally by customers or suppliers. This paper presents a security analysis of the proposed Internet banking model compared with that of the current existing models used in fraudulent Internet payments detection and prevention. Several modern models in preventing and detecting fraud are evolving and being applied to many banking systems. However, they have no effective detection mechanism to identify legitimate users and trace their unlawful activities. Also they are not secure enough to prevent fraudulent users from performing fraudulent transactions over the Internet. The proposed model facilitates Internet banking Fraud Detection and Prevention (FDP) by applying two new secure mechanisms, Dynamic Key Generation (DKG) and Group Key (GK) [6].

In “Study on Fraud Risk Prevention of Online Banks” paper .The paper is aimed, in the first hand, at giving a discussion on the fraud risks of online banking, introducing the current application situation of information sharing mechanism in respect of internet fraud outside China as well as the development of such concept in China. Then, a system is designed for sharing internet fraud information. The paper finally proposing that all the online banks should put more joint efforts in perfecting this mechanism for sake of international co operation[7].

In “Fraudulent Internet Banking Payments Prevention using Dynamic Key” In this paper, They have proposed an efficient new scheme which can prevent fraud by applying different security algorithms, generating and updating limited-use secret keys. It uses advanced authentication technologies and is well adapted to any possible future technology. Moreover, it does not rely on fixed values where hacking one secret will not compromise the whole system’s security. The generation of each set of keys is based on dynamically generated preference keys. The higher number the transactions performed, the less chance the system has of being compromised. The practical usefulness of the technique has been demonstrated by applying it to Internet banking payment systems. The results show that our technique enhances their security considerably. It has been shown that the proposed technique is secure against key compromise. For future

work, we aim to analyze the security of the system that applies the proposed technique. Moreover, we aim to apply the proposed technique to other kinds of internet applications, especially mobile commerce [8].

In the paper "Parallel Granular Neural Networks for Fast Credit Card Fraud Detection" . A parallel granular neural network (GNN) is developed to speed up data mining and knowledge discovery process for credit card fraud detection. The entire system is paraUelized on the Silicon Graphics Origin 2000, which is a shared memory multiprocessor system consisting of 24-CPU, 4G main memory, and 200GB hard-drive. In simulations, the parallel fuzzy neural network running on a 24-processor system is trained in parallel using training data sets, and then the trained parallel fuzzy neural network discovers fuzzy rules for future prediction[9].

3. Architecture and Modules of Proposed System

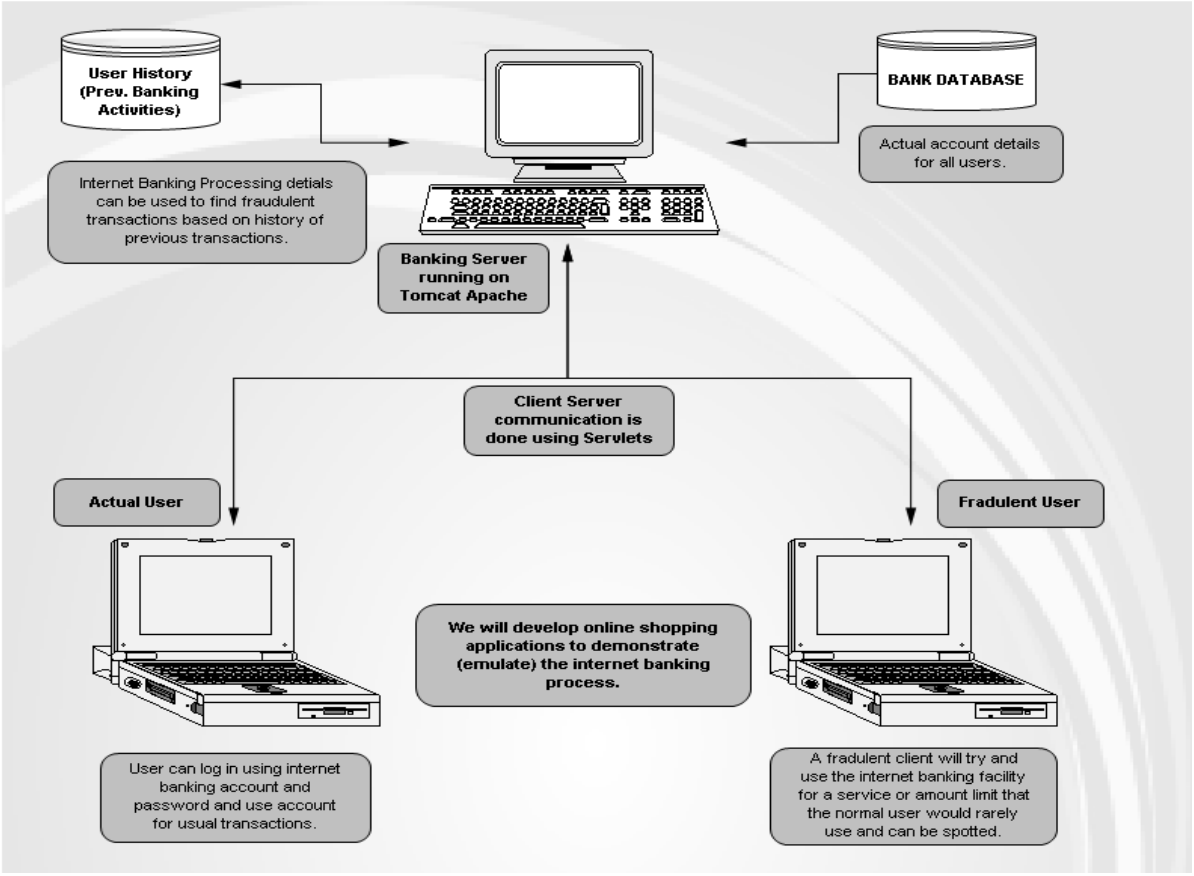

Fig. 1: Architecture of Proposed System

3.1. Modules

1. Client GUI: Using AWT / Swing. This GUI shall allow the user to log in and transact online using internet banking enabled account.

2. Client Server Interaction: A module using Java Networking shall be built that will allow the client application to call Servlets.

3. Client Side Item / Service Browser: A module that will allow the client to browse through all available items/services available on internet. Client can select any of these items/services and opt to buy them online.

4. Client Transaction Module: A module that will allow clients to enter their credentials / authentication information and proceed with a transaction. This module also presents the client with transaction report (success / failure / etc.).

5. Servlets: Client – Server communication is achieved through a series of Servlets. These Servlets will be hosted using Tomcat Apache on the server.

6. Account Database – A database containing account information of all clients is maintained on bank's server. The details may include account number, login, password, available balance, etc.

7. Transaction Database – A database containing history of client's online transactions will also be maintained on server. The databases shall be maintained using Object Serialization.

8. Fraud Detection Using HMM – A module implemented using Hidden Markov Model algorithm that will try to find out if the ongoing transaction is fraudulent or not will be implemented on server side.

9. Server GUI – Server side application GUI will be developed suing AWT/Swing. This module shall allow the administrator to log in and view account details of a specific client as well as add a new client to accounts database.

10.Server Report Generation – A module that will allow administrator to view all blocked accounts, re-activate them and change user credentials will be designed for server end.

4. Use Case Diagram

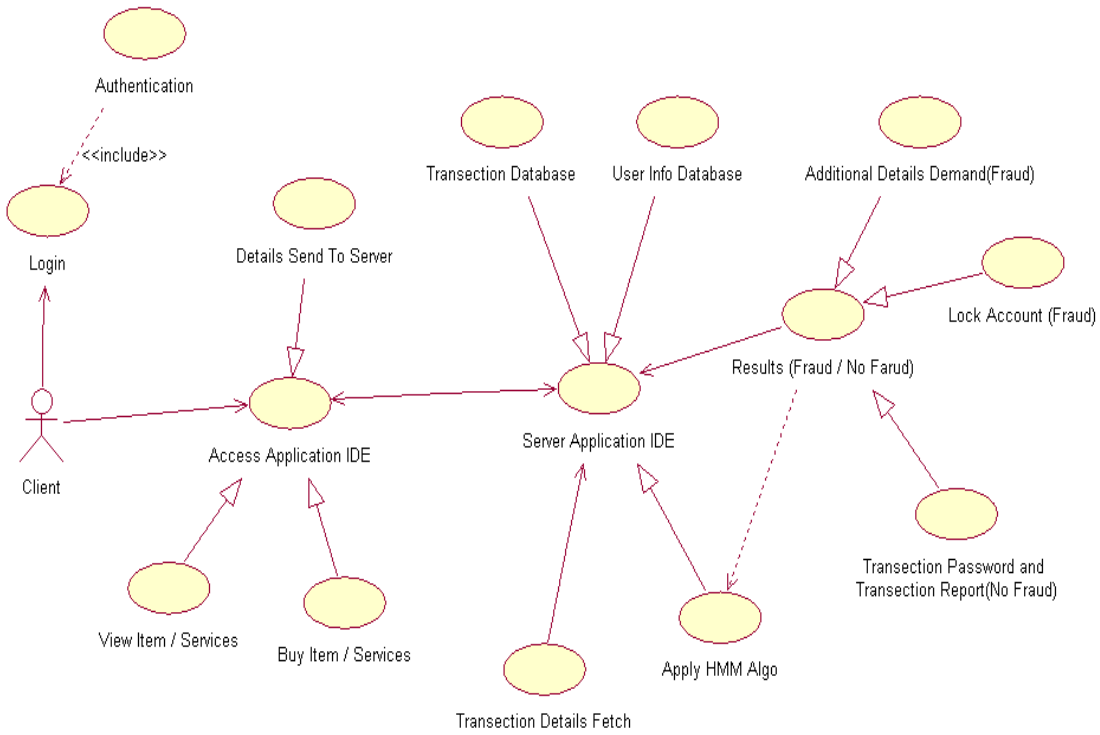

Fig. 2: Use-Case Diagram Of Proposed System

5. Conclusion

The proposed methodology is aimed at detecting fraud in case of internet banking. In Internet Banking a Fraud detection system will run at the banks server. And it's Function to do financial transaction without any fraud. It is considered under Prediction system. A method to attack signature based online banking methods is to manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background. Hidden Markov is used to track the user behavior. First user behavior is recorded and then for new transaction it is checked.

6. Future Work

Future work can be continued in the manner of Using Diffrent Algorithm For checking Fraud Detection making system more and more accurate ad also more reliable.Instead of HMM algorithm we can use another algorithms which is better than HMM.

7. References

[1] Hidden Markov Model by Jia Li. Department of Statistics "The Pennsylvania State University" http://www.stat.psu.edu/~jiali/course/stat597e/notes2/hmm.pdf

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

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

[4] "credit card fraud detection with a neural network" by Ghosh and Reilly. IEEE" Proceedings of the Twenty-

Seventh Annual Hawaii International Conference on System Sciences, 1994.

[5] Offline Internet Banking Fraud Detection" by Vasilis Aggelis.

[6] "Security Analysis for Internet Banking Models" By Osama Dandash,Phu Dung Le and Bala Srinivasan. Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing IEEE DOI 10.1109/SNPD.2007.5321142.

[7] "Study on Fraud Risk Prevention of Online Banks" By Qinghua Zhang. 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing.

[8] "Fraudulent Internet Banking Payments Prevention using Dynamic Key" By Osama Dandash Yiling Wang and Phu Dung Leand Bala Srinivasan. "JOURNAL OF NETWORKS, VOL. 3, NO. 1, JANUARY 2008".

[9] Parallel Granular Neural Networks for Fast Credit Card Fraud Detection Mubeena Syeda, Yan-Qing Zbang and Yi Pan. IEEE Transaction.