A SAFE ONLINE TRANSACTION VIA CREDIT CARD BASED ON HIDDEN MODEL

S.Latha[1],V.Jenifer[2], S.Pavithradevi[3],R.Hemasri[4], B.Glarin Benisha[5], Dr.M.Ramesh Kumar[6]
[1,2,3,4,5]Students (III Year), Department of Computer Science and Engineering,
VSB College of Engineering Technical Campus, Coimbatore, Tamilnadu, India.
[6]Associate Professor, Department of Computer Science and Engineering,
VSB College of Engineering Technical Campus, Coimbatore, Tamilnadu, India.

ABSTRACT

Identity crime is well known, common, and costly. Due to the rise and rapid growth of E-Commerce, use of credit cards for online purchases has significantly increased and it caused an explosion in the credit card fraud. As credit card 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 real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. Implementation of efficient fraud detection systems has thus become imperative for all credit card issuing banks to minimize their losses. Many modern techniques based on Data mining, Fuzzy logic, Machine learning, etc., has evolved in detecting various credit card fraudulent transactions. To reduce the damage of phishing and spyware attacks, banks, governments, and other security-sensitive industries are deploying one-time password systems. The performance of these models is evaluated using test data set to compare their accuracy in identifying fraud for different individuals. The focus is on fraud cases which can be detected at the transaction level. Though fraud prevention mechanisms such as CHIP&PIN are developed, these mechanisms prevent the most common fraud typesans1 such as fraudulent credit card usages.

Keywords: E-commerce, fraud detection systems, data mining, fuzzy logic, machine learning and one-time password.

1.1 INTRODUCTION

The purpose of this project is to find out significant factors of consumers' awareness on e-banking Transaction. This study is the first that seeks to ascertain the insight into e-banking, which has not been previously been investigated and much statistical importance makes this study a possible basis for future research. The motivation for using one-time passwords is that the compromise of one password should not affect the security of sessions involving another password. The one-time password serves to mutually authenticate the client and the server; there are no other long-term values like public keys or certificates.

1.2.Overview

Online banking and e-commerce are excellent examples of transaction processing systems in the business and consumer world. Users can customize their service to provide an automatic account update at regular intervals. Users may also specify the requirements for an update. Online Transaction Processing (OLTP) applications are client/server applications that give online users direct access to information. The OLTP applications process units of work, called transactions. A single transaction might request a bank balance; another might update that balance to reflect a deposit. In a transaction processing system, one execution of an application program processes a single transaction. The one-time data will be provided by the server, our main goal in this paper is to describe the technology and give sufficient detail to allow implementation.

2.1.Existing System

- In case of the existing system the fraud is detected after the fraud is done that is, the fraud is detected after the complaint of the card holder. And so the card holder faced a lot of trouble before the investigation finish.
- Also as all the transaction is maintained in a log, we need to maintain a huge data. And also now a day’s lot of online purchase are made so we don’t know the person how is using the card online, we just capture the IP address for verification purpose.
- So there need a help from the cyber crime to investigate the fraud. To avoid the entire above disadvantage we propose the system to detect the fraud in a best and easy way. The first existing defence is made up of business rules and scorecards.
- The second existing defence is known fraud matching. The existing nondata mining detection system of business rules and scorecards, and known fraud matching have limitations.

Drawbacks:

- Difficult to use
- Less efficient
- It requires large memory

2.2.Proposed System

- Online transaction processing, or OLTP, refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. The term is somewhat ambiguous; some understand a "transaction" in the context of computer or database transactions. Online Transaction Processing (OLTP) involves gathering input information, processing the information and updating existing to reflect the gathered and processed information.
- **Online transactions** required an additional **alpha-numeric secure password** after entering the card details, for systems. **A 6 digit OTP or One Time Password** was devised by Admin. Also, in online transactions, the Admin can directly send the code to the customer upon his request.
- The OTP (One Time Password) is a six digit number and you are requested to generate an OTP prior to every such transaction. OTP is intended to reduce the possibility of fraudulent transactions and would safeguard you, the customer.
- The Server using an assigned set of keys and sent the key as one-time passwords to Client cell phone or carried.
- Client will receive OTP via SMS & Mail from bank during transaction. Clients enter the OTP when requested during the transaction. The OTP is valid for only one transaction, and then it expires.

Advantages:

- The detail of user will check and generate key automatically that will be stored in temporary database (Using Generic Security Service Algorithm (GSS))
- The key will automatically send to user mobile and mail id
- Whenever the transaction is made them, different key will generate in database
- For a day if the transaction will exceed three times means, generate security questions for security purpose

2.3. Feasibility Study

A feasibility study is a preliminary study undertaken to determine and document a project's viability. The results of this study are used to make a decision whether to proceed with the project, or table it. If it indeed leads to a project being approved, it will - before the real work of the proposed project starts - be used to ascertain the likelihood of the project's success. It is an analysis of possible alternative solutions to a problem and a recommendation on the best alternative. It, for example, can decide whether an order processing be carried out by a new system more efficiently than the previous one.

Explanation

A feasibility study could be used to test a new working system, which could be used because:

- The current system may no longer suit its purpose,
- Technological advancement may have rendered the current system obsolete,
- The business is expanding, allowing it to cope with extra work load,

- Customers are complaining about the speed and quality of work the business provides,

Within a feasibility study, four areas must be reviewed, including Economical & Financial, Technical, Legal and Operational feasibility.

Economical & Financial Feasibility

This involves questions such as whether the firm can afford to build the system, whether its benefits should substantially exceed its costs, and whether the project has higher priority and profits than other projects that might use the same resources. This also includes whether the project is in the condition to fulfill all the eligibility criteria and the responsibility of both sides in case there are two parties involved in performing any project.

Technical Feasibility

This involves questions such as whether the technology needed for the system exists, how difficult it will be to build, and whether the firm has enough experience using that technology. The assessment is based on an outline design of system requirements in terms of Input, Output, Fields, Programs, and Procedures. This can be qualified in terms of volumes of data, trends, frequency of updating, etc, In order to give an introduction to the technical system.

Operational Feasibility

Operational feasibility is a test of feasibility that will check whether the systems are working when it is developed and installed in place of the existing system. The Proposed system is beneficial only if it can be turned into information system that will meet the organization's operational requirements.

3.1.Module Description

3.1.1.Authentication

In this module, the customer gives there information to enroll a new card. The information is all about their contact details. They can create their own login and password for their future use of the card.In Login module presents site visitors with a form with username and password fields. If the user enters a valid username/password combination they will be granted access to additional resources on website. Which additional resources they will have access to can be configured separately.

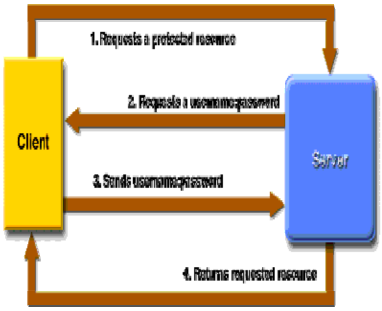
1. Requests a protected resource
2. Requests a username/password
Client
Server
3. Sends username/password
4. Returns requested resource

Fig – 4.1.1

With basic authentication, the following things occur:

A client requests access to a protected resource.

- The web server returns a dialog box that requests the user name and password.
- The client submits the user name and password to the server.
- The server validates the credentials and, if successful, returns the requested resource.

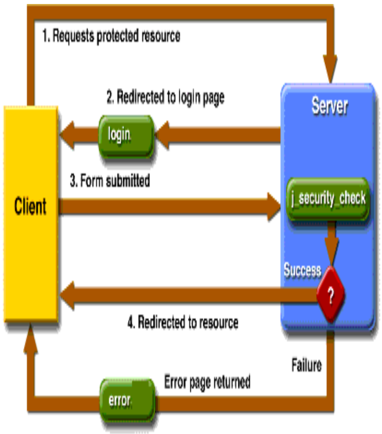

Fig -4.1.2

With form-based authentication, the following things occur:

- A client requests access to a protected resource.
- If the client is unauthenticated, the server redirects the client to a login page.
- The client submits the login form to the server.
- If the login succeeds, the server redirects the client to the resource. If the login fails, the client is redirected to an error page.

4.1.2. Security Information Processing

In Security information module it will get the information detail and its store's in database. If the card lost then the Security information module form arise. It has a set of question where the user has to answer the correctly to move to the transaction section. It contain informational privacy and informational self-determination are addressed squarely by the invention affording persons and entities a trusted means to user, secure, search, process, and exchange personal and/or confidential information.

Efficiency

- Paperless Transactions
- Reduce data entry (errors)
- Speed up transaction process
- Elimination of Fraud redundant steps

4.1.3. Transaction

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.

- Customer can be notified of back order before credit authorization.
- Avoids un-necessary transactions

4.1.4. Verification

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.

The user can login and complete the transaction normally from trusted machines, with use one-timepasswords.

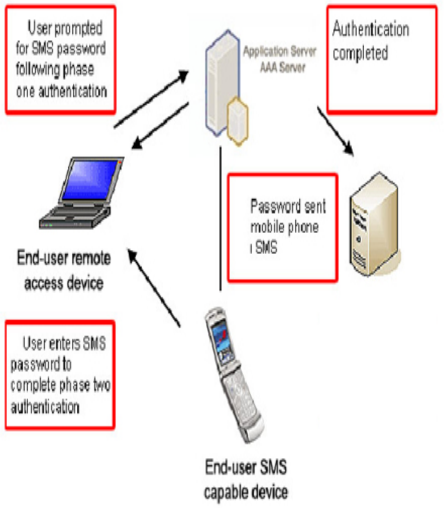
User prompted for SMS password following phase one authentication
Application Server AAA Server
Authentication completed
Password sent mobile phone ı SMS
End-user remote access device
User enters SMS password to complete phase two authentication
End-user SMS capable device

Fig -3

4.2.Input Design

Input Design is the process of converting user oriented inputs to a computer based format. The quality of the system input determines the quality of the system output. Input design determines the format and validation criteria for data entering to the system.

Input design is a part of overall system design, which requires very careful attention. If the data going into the system is incorrect then the processing and output will magnifies these errors. The analysis phase should consider the impact of the inputs on the system as a whole and on the other systems.

In this project, the inputs are designed in such a way that occurrence of errors are minimized to its maximum since only authorized user are administrator can able to access this tool.

The input is given by the administrator are checked at the entry form itself. So there is no chance of unauthorized accessing of the tool. Any abnormally found in the inputs are checked and handled effectively. Input design features can ensure the reliability of a system and produce results from accurate data or they can result in the production of erroneous information.

4.3.Output Design

Computer output is the most importantand direct source of information to the users. Designing the output should proceed in an organized, well thought out manner. The right output must be developed while ensuring that each output element is designed so that people will find easy to use the system.

When analysts design the output, they identify the specific output that is needed to meet the information requirements.

The success and failure of the system depends on the output, through a system looks attractive and user friendly, the output it produces decides upon the usage of the system.

The outputs generated by the system are checked for its consistency, and output is provided simple so that user can handle them with ease. For many end users, output is the main reason for developing the system and the basis on which they will evaluate the usefulness of the application.

Administrator Side Output

- Separate forms to display all the options available in the tool.
- The tool resides in the system tray as icon.

5. CONCLUSION

We have described a system that allows users one-time password access to accounts withoutchanging the server or the client. The method is entirely general and can be applied to almostany login server. Among the key contributions are a very simple user experience and a trulyrobust transaction. We authenticate users: thus there are additional secrets toremember or tokens for the user to carry. The service acts as a transparent between userand login server.

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

6.Scope Of Future Enhancements

A traditional, static password is usually only changed when necessary. The passwords themselves are generated in one of two ways as time-synchronized or counter-synchronized. Both approaches typically require the user to carry a small hardware device that is synchronized with a server, and both typically use some algorithm to generate the password. The OTP solutions in use today are all built on some sort of cryptographic processing to generate the current password from a synchronization parameter, a secret key, and possibly a PIN.

REFERENCES

[1] Aleskerov, E., Freisleben, B., and Rao, B., 1997. ***CARDWATCH: A Neural Network Based Database Mining System for Credit Card FraudDetection***, Proceedings of IEEE/IAFE: Computational Intelligence forFinancial Eng. (1997), pp. 220-226.

[2] R. Brause, T. Langsdorf, and M. Hepp, "***Neural Data Mining for CreditCard Fraud Detection***," Proc. IEEE Int'l Conf. Tools with Artificial Intelligence, pp. 103-106, 1999.

[3] C. Chiu and C. Tsai, "***A Web Services-Based Collaborative Scheme for Credit Card Fraud Detection***," Proc. IEEE Int'l Conf. e-Technology,e-Commerce and e Service, pp. 177-181, 2004.

[4] S.B. Cho and H.J. Park, "***Efficient Anomaly Detection by Modeling Privilege Flows Using Hidden Markov Model***," Computer and Security,vol. 22, no. 1, pp. 45-55, 2003.

[5] W. Fan, A.L. Prodromidis, and S.J. Stolfo, "***Distributed Data Mining inCredit Card Fraud Detection***," IEEE Intelligent Systems, vol. 14, no. 6,pp. 67-74, 1999.

[6] Ghosh, S., and Reilly, D.L., 1994. ***Credit Card Fraud Detection with aNeural-Network***, 27th Hawaii International l Conference on InformationSystems, vol. 3 (2003), pp. 621- 630.

[7] X.D. Hoang, J. Hu, and P. Bertok, "***A Multi-Layer Model for AnomalyIntrusion Detection Using Program Sequences of System Calls***," Proc.11th IEEE Int'l Conf. Networks, pp. 531-536, 2003.

[8] S.S. Joshi and V.V. Phoha, "***Investigating Hidden Markov Models Capabilities in Anomaly Detection***," Proc. 43rd ACM Ann. Southeast

Regional Conf., vol. 1, pp. 98-103, 2005.

[9] M.J. Kim and T.S. Kim, "***A Neural Classifier with Fraud Density Map for Effective Credit Card Fraud Detection***," Proc. Int'l Conf. Intelligent Data Eng. and Automated Learning, pp. 378-383, 2002.

[10] D. Ourston, S. Matzner, W. Stump, and B. Hopkins, "***Applications ofHidden Markov Models to Detecting Multi-Stage Network Attacks***,"Proc. 36th Ann. Hawaii Int'l Conf. System Sciences, vol. 9, pp. 334-344,2003.

[11] T. Lane, "***Hidden Markov Models for Human/Computer Interface Modeling***," Proc. Int'l Joint Conf. Artificial Intelligence, Workshop

[12] C. Phua, D. Alahakoon, and V. Lee, "***Minority Report in Fraud Detection: Classification of Skewed Data***," ACM SIGKDD ExplorationsNewsletter, vol. 6, no. 1, pp. 50-59, 2004.

[13] C. Phua, V. Lee, K. Smith, and R. Gayler, "***A Comprehensive Survey of Data Mining-Based Fraud Detection Research***," http:// www.bsys. monash.edu.au/people/cphua/, Mar. 2007.

[14] Syeda, M., Zhang, Y. Q., and Pan, Y., 2002 ***Parallel Granular networksfor Fast Credit Card Fraud Detection***, Proceedings of IEEE InternationalConference on Fuzzy Systems, pp. 572-577 (2002).

[15] Stolfo, S. J., Fan, D. W., Lee, W., Prodromidis, A., and Chan, P. K., 2000.***Cost-Based Modeling for Fraud and Intrusion Detection***: Results from theJAM Project, Proceedings of DARPA Information SurvivabilityConference and Exposition, vol. 2 (2000), pp. 130-144.

[16] S. Stolfo and A.L. Prodromidis, "***Agent-Based Distributed LearningApplied to Fraud Detection***," Technical Report CUCS-014-99, ColumbiaUniv., 1999.

[17] V. Vatsa, S. Sural, and A.K. Majumdar, "***A Game-theoretic Approach toCredit Card Fraud Detection***," Proc. First Int'l Conf. Information SystemsSecurity, pp. 263-276, 2005