Analysis on Secured e-payment Authentication Model for E-commerce Portals

Sahan Yasiru Walpitagamage

139184N

Dissertation submitted to the Faculty of Information Technology, University of Moratuwa, Sri Lanka for the partial fulfillment of the requirements of the Master of Science in Information Technology.

April 2016

Declaration

We declare that this thesis is our own work and has not been submitted in any form for another degree or diploma at any university or other institution of tertiary education. Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

Name of Student: Sahan Yasiru Walpitagamge

Signature of Student: ……………………………

Date: 28/04/2016

Supervised by:

Name of Supervisor: Dr. Lochandaka Ranathunga

Signature of Supervisor: UOM Verified Signature

Date: 28/4/2016

Acknowledgment

The success of any project mainly depends on the encouragement and guidelines given by others. I would like to take this opportunity to express my gratitude to the people who have helped to make this project success. First of all I would like to express my greatest appreciation to my project supervisor Dr. Lochandaka Ranathunga who untiringly shared his knowledge, experience and valuable guidance to complete this project successfully. I would also like to express my gratitude to the professionals who spared their valuable time with me in sharing their knowledge. Finally my parents and the support of University of Moratwa are also sincerely acknowledged.

Thank you.

Abstract

The research focuses on to introducing a secure e-payment authentication model for e-commerce portals. E-commerce can be defined as one of the most rapidly development mechanisms in the world economy. Therefore, a secured payment authentication model is essential for any e-commerce portal. Also today there are various security mechanisms to ensure the security of these e-commerce portals. However, the research background analysis has recognized that there are still problematic areas in existing payment methods. Therefore, this research mainly focuses on introducing a secured e-payment authentication model for e-commerce portals which will ensure the exchange of money more securely and conveniently over the internet.

The introducing system is a web based electronic payment authentication processing system that can be used to make a secured electronic payment. In order to provide high security to the electronic transactions, the system validates the payments by using a onetime transaction code generating software installed into users PC or mobile phone. This code generating software uses unique hashing polynomial equation for each individual. The system only validates the transactions, only if the user enters the correct secure code in the transaction processing web page. The solution can mainly provide good security against the man in the middle attacks and the phishing attacks. Also this system has been designed to minimize the issues in existing electronic payment systems by providing a great convenient to the users. As a result, this research can be brought into play as a guide for e-payment authentication.

Table of Contents

List of Figures

List of Tables

Chapter 01

Introduction

1.1 Introduction

The concept of e-commerce has been developed to a larger extent during the last few years. Similarly today there are various number of electronic payment systems (EPS) available to be used. However, there are various problems existing electronic in the present payment system methods (EPS).

Electronic commerce is where business transactions take place via telecommunications net-works, especially the Internet [1]. E-commerce has become a very important aspect of modern business to enter and face competition in the global market. On other hand the revolution of e-commerce opens to customers a wide range of selections as well as they can purchase the latest products, latest brands of new technology on any internet accessible place in to the world. E-commerce is booming rapidly and playing a key role in the Sri Lankan economy at this moment.

Any e-commerce portal electronic payment system (EPS) plays a major role. EPSs enable a customer to pay for the goods and services online by using integrated hardware and software systems [2]. Today there is a wide range of EPSs available to be used but each one has its own pros and cons. On the other hand for any electronic payment system, security is one of the most important aspects. Currently even though there are lots of security mechanisms implemented to protect the EPSs transactions, there are still concerns regarding the exchange of money securely and conveniently over the internet. Therefore, this research mainly focuses on introducing a secured e-payment authentication system for e-commerce portals.

1.2 Background and Motivation

Today there are various kinds of electronic payment systems available for customers to use. However, there are some issues which should be circumvented or avoid in the existing electronic payment systems. Because of that reason some of the customers are still reluctant to use electronic commerce. One research has found that 17% of shoppers avoid using e-commerce transactions to pay for goods and services due to on line security concern [3]. Therefore it has a direct impact on the sales of the e-commerce portals. In this research project, there is an attempt to fill that research gap and find a secure e-payment authentication model for E-commerce portals.

The background analysis of this research has found that though there are many methods to ensure the security of electronic payments, one of the best today commonly used method is to use a onetime password (OTP) to perform the transaction. Generally, it can be generated in two ways; one is by using a secure token to generate it or the other by sending a onetime secure code to the registered mobile phone via SMS.

Using a secure token is more secure but it has some cost. For an example the PayPal charges 29.90$ from their customers to issue a new or replacement token [4]. On the other hand it is not convenient for customers, because they have to always keep the token with them and if the token is lost they have to wait some time to get a replacement for that. Sending a onetime password to a registered phone is cost effective and a bit convenient. But there is less security because it has a possibility of a man in the middle attack when the code is being transferred to a customer's mobile phone. If the customer is overseas his or her mobile connection should work in that county because the security code is only sent to the registered mobile phone number.

By introducing a method to minimize the issues in the above mentioned methods it is necessary to provide more security and convenient method of electronic payments to customers. Therefore, this research mainly tries to fill that research gap.

1.3 Aim and Objective

Research Aim

The aim of this research is to find out a secured e-payment authentication system for e-commerce portals which can be used to transfer money on line in more secure and convenient way than existing e-payment authentication systems. These research objectives are developed to achieve the main goal of the research.

Research objectives

To achieve the main research objective, the main objective should be divided in to four specific sub objectives. The following are the sub objectives of this research.

- To examine the currently available e-payment authentication systems models and identify the problems associated with them.
- To examine the identified security problems and find the methods to prevent those problems
- To introduce a secured e-payment authentication system to minimize the existing security threads towards to electronic commerce transitions.
- To find out up to which level proposed system can address the current security threads for e-payment systems.

In the above mentioned objectives, the first two objectives can be achieved simultaneously and other two final objects can be achieved by being based on the result of first objectives. Under the methodology section the proposed method to achieve these objectives is described.

1.4 Structure of dissertation

Chapter 02 describes the Present movements in Electronic Commerce and Electronic Payment Systems. Chapter 03 is about technology adoption in project. Chapter 04 is on Approach to find a secured e-payment authentication model. Design of the secure electronic payment mode is on chapter 05. Chapter 06 on The System Implementation Background and chapter 07 will present discussion.

1.5 Summary

The e-commerce is an upcoming technology for the developing world. Therefore e-commerce has created new concepts and marketplaces for the business world. The e-commerce can be defined as one of the rapidly development mechanisms in the Sri Lankan economy. On the other hand today there are various kinds of electronic payment systems available for customers. However, there are some issues which should be circumvented or avoid in the existing electronic payment system methods. Therefore this research mainly focuses on introducing a secured e-payment authentication model for e-commerce portals which will enable to exchange of money more securely and conveniently over the internet.

Chapter 02

Present movements in Electronic Commerce and Electronic Payment Systems

2.1 Introduction

The term Electronic Commerce or the e-commerce simply can be described as the conduct of a financial transaction by electronic means usually on the World Wide Web [5].In other terms shopping for products or services over electronic systems, computer networks, or especially the World Wide Web can be defined as e-commerce [6].

Similarly electronic payment systems (EPS) play a major role in e-commerce business. So far there are nearly 10% of the world's population have shopped online at least once [7].Also today E- Commerce privacy and security concerns are the number one reason of web users for not going to purchase over the web [8]. Electronic payment systems should have a number of requirements need to be fulfilled. They are security, acceptability, convenience, cost, anonymity, control, traceability and control of encryption methods [9].

2.2 Electronic Commerce and its Present Movements

E-Commerce can be categorized based on the types of partners directly involved in the transactions or business processes. There are four general electronic commerce categories which are Business-to-business (B2B), business-to-consumer (B2C), consumer-to-consumer (C2C), and business-to-government (B2G) [10].

E-commerce benefits organizations, customers and also for the society. For organizations some of the main advantages of electronic commerce implementations are reducing operational cost, allowing mass customization and business can be conducted at any time any place globally. On the other hand electronic commerce increases the sales opportunities. Even a small firm can have access to potential customers all around the world. Also organizations can use E-Commerce to identify new suppliers and business partners, to obtain competitive bid information in addition to increasing the speed and accuracy of information transferring and it leads to the reduction of cost on both parties. In the customer point of view e-commerce increases purchasing opportunities and transactions. It can be conducted for 24 hours of all seven days from any location in the world [11].Finally e-commerce benefits the society by enabling flexible work practices which help to increase the quality of all people in the society [12].

The worldwide Business-to-consumer (B2C) e-commerce sales reached $1.471 trillion in year 2014 which is nearly 20% over 2013. It is expected that e-commerce sales worldwide will be reach $2.356 trillion in year 2018. In 2015 Asia-Pacific will be becoming the leading region for e-commerce sales and China accounting for a significant portion of e-commerce sales in Asia-Pacific [13].

The personal computers are the favorite device for online browsing and buying products among the other devices in all regions and the mobile phones are a close second pick. The smart phones and tablets are huge trends today. Therefore, m-commerce is becoming popular day by day. Then, online sellers now make sure that their websites have at least a mobile version. And in most cases they go beyond that level such as checking them at different mobile platforms and make a plan for creating versions for new trending technologies [14, 15].

The social media and brand emails have become the most popular ways of marketing online selling products and social media make 23% and 22% of customers who tend to buy products they have never bought before. Pre order products and personalized products are going to be the biggest trend in next five years. Also online marketing is going on the as way of providing personalization unique experience to customers [14].

Today online customers spend a considerable amount of time to research about the products before buying. These online buyers believe they get the best prices in online than those products offered in the store. They also like getting email notifications from retailers to stay updated about the new deals [16, 17].

One of the main problems in e-commerce is privacy and security. The considerable amounts of online shoppers are afraid of giving their credit card information online. The shipping costs and confusing websites are other barriers for shoppers. Therefore, free shipping and user-friendliness are important [1].Nowadays free shipping is common for online purchases but the next level is free shipping on returns. Today online retailers are trying to turning a one-time shopper into a loyal customer [16, 17].

2.3 Electronic Payment Systems and its Present Movements

Electronic commerce and electronic payment systems are two elements of the same set. The Electronic payment system is defined as a payment service that utilizes ICT, including cryptography and telecommunications networks [18].

There are wildly available electronic payment methods for use. Some of the common types of payment methods are payment cards, electronic cash systems, electronic funds transfer and electronic wallets [19].Out of them, the payment cards and electronic cash systems are the most commonly used methods. Today mobile based electronic system is becoming popular day by day. It is believed that mobile payments volume will be more than $617billion by 2016. Other than that today NFC and the social network payments are the two of the latest ones [20].Social payments have two major categories, one is used as peer-to-peer transfers and the other online purchases. Venmo is one of the famous mobile based social payments transfer services that allows users to send instant payments to their contacts. To use this application the user needs to make an account or log in their account Facebook account [21]. Also new payment methods are continually being discovered day by day.

E- Commerce Privacy and security concerns are the number one reason of web users for not going to purchase over the web [22]. E-commerce security is a part of the information security framework and specifically it applies to the components affecting electronic commerce such as computer security, data security and broader realms of information security framework.

The industry predicts that the amount of online credit card fraud could be in the region of $11.1 billion in year 2013. The experts believe that hackers have stolen more than one million credit card numbers from e-commerce sites. Also it was found that 75% of card frauds were skimming and malwares installed in to POS (Point of Sales) machines and only 15% was account for online transaction in year 2013[23, 24].

And it strategically deals with protecting the integrity of the business network and its internal systems by accomplishing transaction security between the customer and the business. The main four features of e-commerce security are authentication, authorization, encryption and auditing, integrity, nonrepudiation and availability [25].

Customers and merchants will have practically common set of wishes and concerns for electronic commerce payments. Some of the main considerations are security of the transaction, acceptability of wide range of parties, convenience to use, cost friendliness, privacy of the payment mechanism and durability of the payment system which means the electronic money should not be easily lost even the system crashes [26].

On the other hand financial institutions also have a set of expected requirements for electronic payment systems. Financial institutions and regulators look for immediate control of the electronic payments. In here the transactions should be controlled and cleared individually that any security break can be identified as soon as possible. Financial institutions will also search for a system Traceability of the transactions. If a crime is detected the culprit can be identified. In particular, traceability will be important to track international funds flows and tax evasion, and control over the spread of encryption mechanisms [26].

There are several limitations in the traditional electronic payment systems. The very first one is it has lack of security. Current internet based payment methods can be easy target for stealing money or personal information even if they transmit data through the secured transactions mechanisms like Secured Socket Layer (SSL). The next main limitation is lack of applicability of these payment methods. Another problem is lack usability of the existing EPS. Some EPS request large amount of information when make payments and using complex web site interfaces. The next main problem is high level of transaction cost in online payment for both customers and merchants. Most of the existing payment systems use expensive infrastructure to process the payment and a very good example for this is credit cards and payment gateways [27].

The three main types of security threats for e-commerce transaction are denial of service, unauthorized access and theft and fraud. Denial of service or DDOS Attack is an attempt to make a machine or network resource unavailable to its intended users by sending large requests simultaneously. Unauthorized access is illegal to systems or data. The popular examples are Active attacks, Passive attacks, Masquerading or spoofing and Sniffers. Theft and fraud comes under unauthorized access. In here Fraud occurs when the stolen data is used or modified [28].

Aigbe and Akpojaro research about current Security Issues in different Electronic Payment systems. That analysis reveals that electronic payment systems with authentication mechanisms involving two or more authentication factors tend to be more secured and increase users' confidence in using electronic payment systems. In the same study identified that two factor authorizations has some usability issue [29]. In a similar study about electronic payment systems done by Kaur, founded that encryption is important in order to protect the privacy of the electronic payment systems [30]. The study reveals that two factor authorizations with encryption can contribute toward enhancing clients' perceptions that the web and financial transactions are secure. However two factor authentication technologies are overall perceived as usable but regardless of some motivation or context of use. According to the Bruce Schneider's' findings Two-factor authentication dose not provides good security against Trojan-based attacks, and are not completely effective against phishing attacks [31].

Today banking world is starting to authenticate online card transactions using the '3-D Secure' protocol, which is mainly branded as Verified by Visa and MasterCard Secure Code. In 3DS pop up a password form to a bank customer who attempts an online card payment. If the password is correct only it returns to the merchant website to complete the transaction. The main weaknesses of the 3DS are it has considerable amount of phishing sites targeting 3-D Secure. On the other hand users are more likely to choose a poor password, or one they use elsewhere. Also customers are likely to choose bad phrases. The rapid growth of the man-in-the-middle attacks and malware ensures that 3DS is not sustainable security methods to prevent current security threats towards electronic transactions. Technically single sign-on is the wrong model. And it needs transaction authentication. As a solution when the transaction takes place authentication code should require to precede the transaction. The authentication code can be sent using SMS messaging or Chip Authentication Program [32].

2.4 Summary

E-commerce has become a more important aspect of modern business world. E-commerce benefits to organization, customers and also for the society. Electronic commerce and electronic payment systems have strong relationship. There are wild available electronic payment methods for use. E- Commerce Privacy and security concerns are the number one reason of web users for not going to purchase over the web. Also there are several limitations in the traditional electronic payment systems. Today banking world is starting to authenticate online card transactions using the '3-D Secure proved better security their customers.

Chapter 03

Development of web technologies

3.1 Introduction

Web technologies are one of the rapidly growing up technologies in today's world. Internet is call as network of network which interconnected millions of computers. The Web technologies came to seen with invention of internet. There are different types of web technologies are available to use for different works. On the other hand today internet crimes are increasing never before. Therefore, web security concern as one of most important area.

3.2Web Architecture

The essential elements of the internet are the Web browsers used for surf the Web, web servers for providing information to these browsers and the computer networks. To view the Internet still most people use web browsers. Web browsers connect to the internet via modem or ISD. In here web browsers on the client side send request to the web server. Once the web server recived that request it sends response to client. In here when the web server receives a request for a page, it sends it back to the local computer for viewing through the browser. Web browsers on the client end translate HTML codes in to readable format. The following diagram shows the web architecture of the web based application [33, 34].

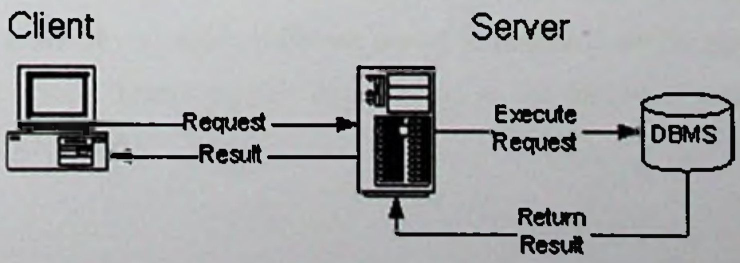


Figure 3.1: Basic Two-Tier Architecture [31]

3.3 User interface Designing Technologies

HTML

HTML is a markup language which is mainly using for design the web pagers. HTML stands for hypertext markup language. It is the official language of the World Wide Web and was first conceived in 1990. The HTML states the web browser how to display web pages contains for the user. Each individual markup code is referred to as tags or elements. The most important thing is HTML is platform independent language that is common for all computers web browsers on the web. HTML page has mainly two parts. The first part is header and second one is its body. The header section contains the information about the web page such as page title and the Meta tags for search engines. The body section contains the information need to be passing to the client browser. In year 2014 October HTML 5 was introduced with many more new features. But still most of the people are using HTML 4. Since this is a light weight web designing language with quick response time. This project has selected HTML as the main web page designing language in this project [35].

CSS

The first version of the CSS release in 1996 and called as CSS1. The CSS stands for Cascading Style Sheets. CSS is a style language that defines layout of HTML documents. In other word HTML codes define the structure of the web page and the CSS is a formatting structured content of that web pagers.CSS also a platform independent language for any web browsers on the web. There are benefits of use CSS, the very first one is it has the ability to control the layout of the many web pagers by using a signal style sheet. Also possibility of apply different layout to different media-types and more precise control of layout. Therefore, this has selected as the main web page designing language in this project [36].

3.4Programing Technologies

PHP

PHP (Personal Home Page) is a powerful server side scripting language use to develop dynamic and interactive web pagers. It is powerful enough to run largest web sites like Facebook and World Press. Today comparing with other available server side programming languages, 81.5% of web sites use PHP as the server side programming language [37].

It was originally created by Rasmus Lerdorf in year 1994 and the first version released in early 1995.PHP 3.0 was introduced in 1997 and similar to resembles exists in today PHP. In year 2000 May officially PHP 4.0 released. The currently available least PHP version is 5.6.14 [38].

PHP from similar to client side JavaScript but in PHP code is executed on the web server and generating HTML codes to send the client. The client receives the results but would not know what the underlying code [39].

In PHP version 5onwards it supports the Object Oriented Programming. PHP application can link with many databases such as MySQL, MS SQL and Oracle or even interact with databases using ODBC. Also it can interact with draw graphs, create PDF files, and parse XML files. It is possible to write own user define PHP extension modules by using C language. Also PHP codes can be simply combining with HTML codes, different tinplating engines and support with many web frameworks. The most important thing is unlike some other server side languages, PHP has cross platform compatibility [38]. Also PHP is famous as a light weight programming language. Therefore, it requires fewer amounts of resources and has very fast response time.

If it is a good electronic payment system, it should response fast and also able to run even in less amount of resources. Therefore, PHP has selected as the main programming language to implement this project.

.Net Frame Work

Microsoft .Net is a software development platform developed by Microsoft. The first version of the .NET framework was released on February 2002.The available least version is Net 4.6.1.It can runs on Microsoft Windows operating system. The .NET platform provides tools and libraries which allow developers to develop applications and services much convenient, faster and secure manner. C# in .Net frame work has selected as the second programming language to implement this project [40].

3.5 Database Implementation Technologies

MYSQL

MySQL is one of the most popular and widely used open source relational database management systems in the world. Today more than 100 million worldwide applications use MYSQL as their database management system. Leading high profile web-based applications including Facebook, YouTube, Yahoo, Twitter and many more have chosen MYSQL as their RDBMS. The first version of the MySQL was created by a Swedish company call MySQL AB in year 1995May [41].

There are many reasons behind the popularity of the MYSQL database system. One reason is it a lightweight DBMS that gives high performance by taking very small amount of hardware resources. Next one, it can install easily without going through the complex configuration process. The next big reason is it has easy interface to other software. Most popular programming languages have libraries of functions for connect with MySQL. Also since this is an open source DBMS it has active responsiveness to community [42].

Select the correct database is important for any electronic payment system. It should response fast and also able to run even in less amount of resources. Therefore, MySQL has selected as the DBMS of this project.

3.6 Summary

In client server architecture when the web server receives a request for a page, it sends it back to the local computer for viewing through the browser.HTML and the CSS is the wildly use web designing technologies available to use. HTML and the CSS have selected as the main web page designing languages in this project. PHP is a powerful server side scripting language use to develop dynamic and interactive web pagers. It is a lightweight programming language which can run on less resources environment. Therefore, PHP has selected as the main programing language to implement this project. Also .Net frame work has selected as the second programming language to implement small part of this project. MySQL has selected as the DBMS of this project. It is one of the most popular and widely used open source relational database management systems in the world.

Chapter 04

Approach to Find a Secured e-payment Authentication Model

4.1 Introduction

This research project there is an attempt to fill the research gap and find a secure e-payment authentication model for E-commerce portals. In order to achieve final research goal it essential to follow a step by step approach. This section describe about the research approach taken to achieve the final objective of this research.

4.2 Experiment Steps

This project mainly focuses on to find out the secure electronic payment module for e commerce portals. Therefore, this project is going to be a research base software implementation. The requirements of this project are clear and possibility of change the requirements are very less. On the other hand since this is research based project it is essential to come up with system good design based on the background research findings and identified requirements. There is very less probability of fail the project. Hence this project is going to use Waterfall method as the software implementation model. Therefore, following mentioned steps were followed to achieve the objectives of the project.

- Requirements Gathering
- System Design
- System Implementation
- System Verification or Testing
- Installation & Maintenance

4.3 Requirements Gathering

Requirement gathering is an important stage for any project implementation. Because the success of any project is depend on this step. There are lots of requirements gathering techniques are available to use for different circumstances. In this research mainly used interviews and background case analysis techniques as the requirements gathering techniques. The main reason for conducting unstructured interview sessions with industry experts is to get their expert knowledge to fine tune the system requirements. Finally the system requirements were identified and divided it as functional requirements and the nonfunctional requirements.

4.3.1 Non-functional Requirements

Usability

In simple world usability can be define as user-friendliness of a system. Therefore, this system should be ease to use for any level of user. If the system is ease to use it takes less time to accomplish a specific task. Also it is important system should be easier to learn. The process should be able to learn by observing the objects available in the screen. The final outcome of system usability is increase the satisfaction level of the system users.

Availability

Since this is the electronic payment system, it is important to maintain the high availability of the system. Therefore, system should be available use anytime anywhere without any problem. In order to maintain good system availability, reliability of the system is also very important.

Reliability

Reliability mainly talks about ability of a system function under stated conditions for a specified period of time. In order to assure the reliability of the system, redundancy mechanisms need to be considered. The system uptime should be very less and if something went wrong it should have ability to recover the condition in very short time.

Performance

In performance evaluation of a system usually measures based on the time and resources used perform a useful work. Mainly system should have less response time and should use both hardware and software resource in a careful manner.

Disaster recovery Plan

It is important to have a Disaster recovery plan for this kind of critical system. This Disaster recovery Plan (DRP) should contains a set of policies and procedures to follow in a disaster situation to the recovery or continuation the business process.

4.3.2 Functional Requirements

Prevent the Unauthorized Electronic Transactions

Prevention of unauthorized electronic transaction is the main requirement of this project. Unauthorized transactions are performing without the knowledge of the person who has an authority to do it. This is one of the most critical problems in electronic payment systems. Therefore, this system should design for prevent unauthorized transactions as much as possible. In here it is essential to focus on more about the issues identified in existing electronic payment methods.

Ensure the Integrity of the Electronic Payments

Maintaining and assuring the accuracy and consistency of data is needed to be consider when transfer confidential information over the internet. Integrity is also very important factor needed to be considering when implementing a secure electronic payment system because, electronic payments are transfer through the internet and there is high risk of break the integrity. Therefore, it is essential to implement a mechanism to check integrity of the data. In order to protect the data integrity of the system, digital signature or the check sum should be used when transferring data through public network.

Secure the Client End by Implementing SSL

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client [43]. Implementing a secure socket layer is essential for any system which transfers confidential information through the public network. This will be help to ensure the confidentiality of the information transfer client end to server.

Automatic System Session Time Outs

The automatic system session time out is common feature for many web based systems in today. The system should be able automatically destroy the session if it keeps ideal for more than 10 minutes. This will help to prevent system from session hijacking and ensure the user privacy. On the other hand it will helps to increase the sever performance by destroying the long waiting sessions.

Protect the System from the Phishing Attack

The phishing attack is the attempt to steal the sensitive information of the web users by represent as a trustworthy party. Phishing attacks are most common thread for web based systems. Therefore, as secure electronic payment system it is required to protect users from this risk. In here system should be design to help user to validate before they put their sensitive information on the system.

Practice PHP and MySQL Best Security Practices

The next main requirement is use the best security practices when implementing the solution. Otherwise hackers can be take the advantage of this because, most of the times hackers use the software security holes to gain authorized access to the systems.

4.4 Summary

This project is going to be a research base software implementation. In this chapter mainly forcused to get a approch to system desing stage. After review the project background this project selected to use Waterfall method as the software process implementation model. As the first approach of the project, system requirements were identified and categorized them as functional and the nonfunctional requirements. These requerments will be converted into system desing.The other main experimentsteps in the software process use were discussed in detailed manner in next chapters of this document.

Chapter 5

Design of the Secure Electronic Payment Model

5.1 Introduction

The design process of secure electronic payment system is a very crucial task because it may need to consider many different areas to follow. The design should be capable of minimized the security threads and give greater convenient to the users. Therefore, it is essential pay more attention to the finding of the background analysis to come up with good design. Finally the identified requirements should be fulfill with the system design. The introduced solution is name as Safer Pay.

5.2 Solution Overview

Safer Pay is a web based electronic payment system design to give maximum level of security for the electronic payments. The system design also mainly considered to provide maximum level of convenient to the system users compare to the existing electronic payment systems. Mainly there are three types of users involved in this system namely, Customers, Banks and Merchants.

The system allows any customers to register with the service and do electronic payments via online basis. The only main pre requirement is the user should have a bank account with one of the registered banks with the service. In this system a customer first needs to register themselves for that service, then the system will create a profile for each user. At the registration process customer needs input their bank account details and the other information. It should be automatically validated using java scripts and Ajax. In here the main consideration should be the password validation because as secured e-payment it is really important to have these kinds of basic security approaches.

Once the registration was completed successful users can logon to their profiles. The next step is user need setup their profile. First they should need to give a transaction password.

This password will be use only to authenticate transactions. Then users should need to download the secure key generating software to their desktop or mobile phone. This application will use to generate one time transaction code when customers doing the transactions. The secure token application uses a polynomial equation to generate the one time transaction code. In here user specific random hash keys values assign to that polynomial equation. Finally this account should be approved by the bank belongs to that registered user. If the account details approved by the bank, now account is ready to use.

Customers can only do the electronic transaction for merchants who registered with the service. When the time transaction takes place, customers need only to give the username, transaction password and the one time transaction code generated from the secured token application. In order to generate the one time transaction code, customers need to enter random code received form the system into their secured token generator software.

Then the application server will authenticate information received form the user and decide to allow or decline the transaction. If the details are matched the system will send the response to the user registered bank to perform the transaction. Then the bank response back with the transaction status. Finally the system will inform the transaction status to customers and the merchant. To match the secure token, applications sever and secure token generator should run the same algorithm.

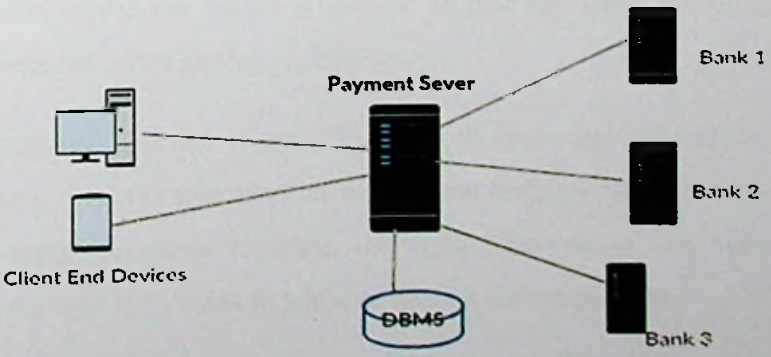


Figure 5.1: The high level system diagram

5.3 Authentication Code Generation Process

The system mainly authenticates the transactions based on one time transaction code generated through the secured token generator software. Therefore, in order to generate the transaction code, users need to enter random code received form the system into their secured token generator software. The random number is the five digit number which will show it to the users each time when they are trying to do a transaction. That random number is an event base number change at each event.

The transaction code is generating using a polynomial equation. The random code is assigned to variable value$\underline{x}$ of that equation. The two digits user specific random numbers are assigning to other variable values of the equation. The base polynomial equation use to generate the transaction code is mentioned below.

$$TC = ax^n + bx^m + cx^p + dx^a + E$$

Equation 5.1: Polynomial equation used to generate the transaction code

The each user registration process, the random values assign to the polynomial equation variables. Then the assigned values are stored in the server end system database. In the same time these random values insert in to the secured token generator software polynomial equation source code. Next the system compiles that source code and generate dynamic executable which is specific to that one user. Finally enable user to download the secured token generator software.

The same polynomial equation is using by the both client end software and the system server. Therefore, once the user to enter the random code received form the system into their secured token generator software, the application server can authenticate code received form the user and decide to allow or decline the transaction.

The reason for use polynomial equation to generate this transaction code is polynomial equations can be used to generate complex numbers. Therefore, it is really hard to identify the number patterns. On the others hand, values assign to the equation is different to one user one. Hence it is really difficult to guess the transaction code for third party.

5.4 System Modules in Detail

Safer pay mainly interacts with three parties. Those parties are Customers, Banks and Merchants. Each party has separate modules to perform. The following section describes the each modules functionality in detail.

Payment Process Module

This is the core module of this system. Because, this is the module customers use to perform the secure transactions. In order to perform transaction customers need to give the username, transaction password and the one time secured token generated from the registered device.

- Authenticate requested payments
- Response about the transaction status to each party.

User Master Data Management Module

This module is use by customers to manage their system profile master data. The module available the following functions to customers.

- Manager personal profile details
- Manage bank accounts link to the system. Under this system allows removing existing linked bank accounts or linking new bank with the system.
- Change their transaction and logging passwords.
- In the event of device lost disable current secure token application and download new application
- View the performed transaction details.

Bankers Module

This module is available for registered bank with the system. This module helps banks to manage their system profile. The module available the following functions.

- Approve customer accounts to perform the transactions.
- Process the authorized transactions
- View the transaction detail reports

Merchants Module

This module is available for registered merchants with the system. This module helps merchants to manage their system profile. The module available the following functions.

- Manage profile details.
- Manage accounts linked with the system
- View the received transaction detail report.

Admin Module

This is the module use to do the system administration works and system admins only have access to this module. The module available the following functions.

- Work with customer complains
- Monitor transaction logs
- Add, Remove ,Updated registered user accounts

5.5 The System Functionalities

5.5.1 The System Use Case Diagram

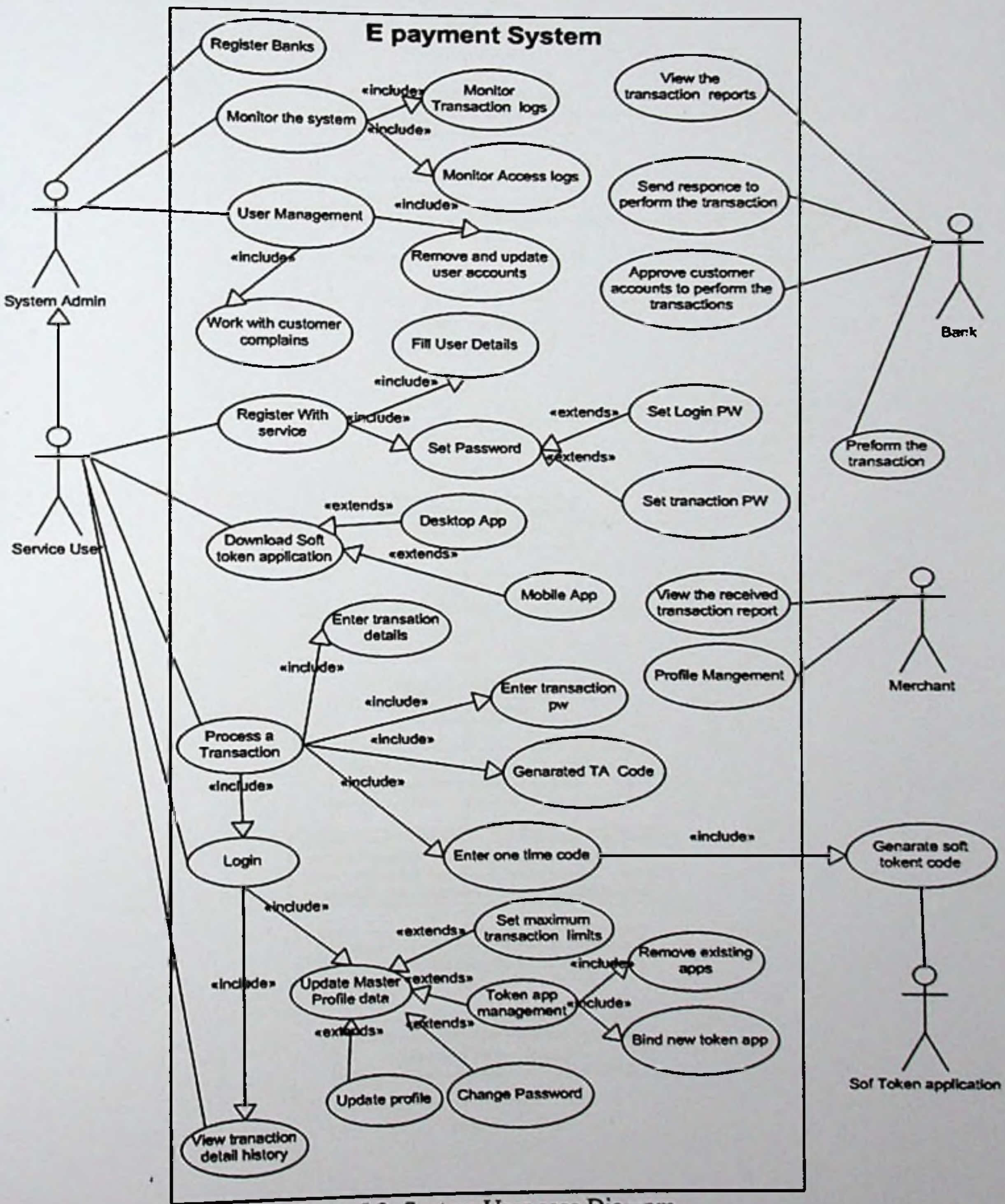


Figure 5.2: System User case Diagram

5.5.2 Flow Chart of the User Registration Process

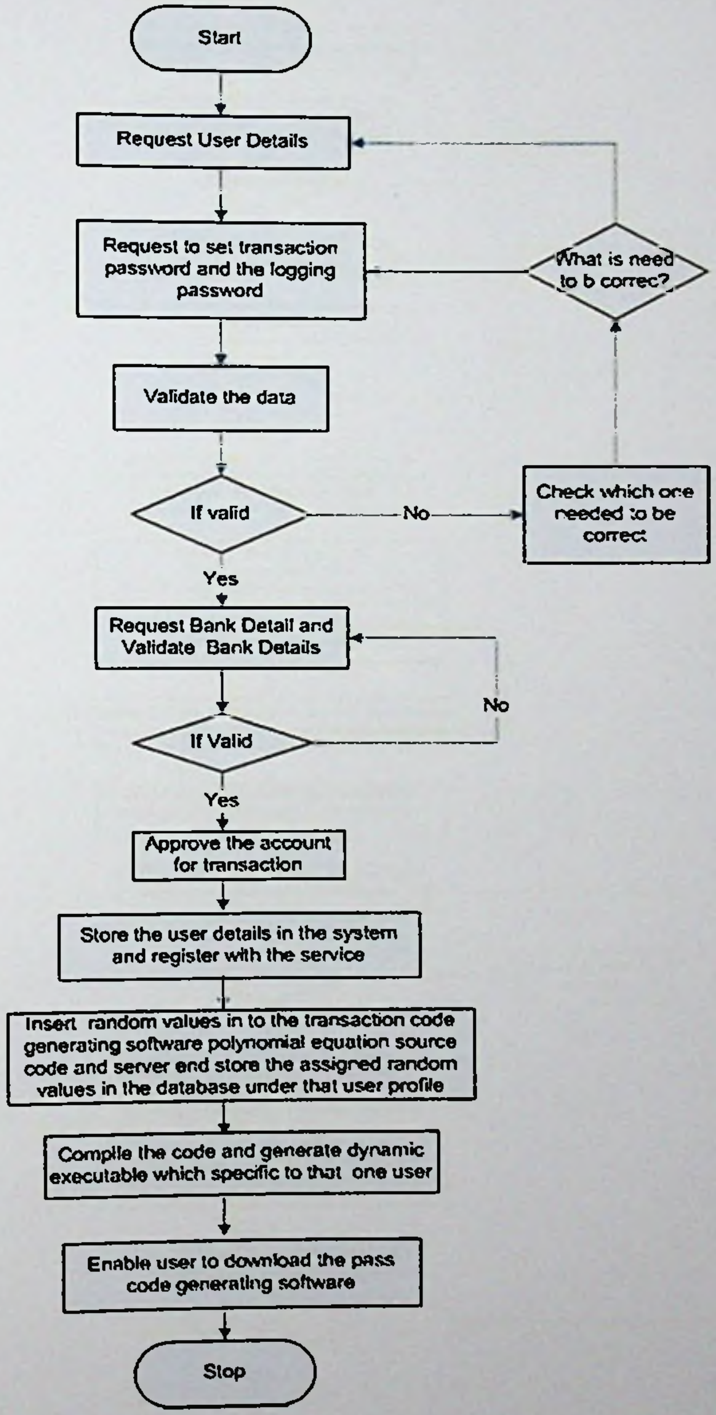

Start
Request User Details
Request to set transaction password and the logging password
What is need to b correc?
Validate the data
If valid
No
Check which one needed to be correct
Yes
Request Bank Detail and Validate Bank Details
No
If Valid
Yes
Approve the account for transaction
Store the user details in the system and register with the service
Insert random values in to the transaction code generating software polynomial equation source code and server end store the assigned random values in the database under that user profile
Compile the code and generate dynamic executable which specific to that one user
Enable user to download the pass code generating software
Stop

Figure 5.3: User Registration Process Flow Chart

5.5.2 Flow Chart of the Transaction Processing

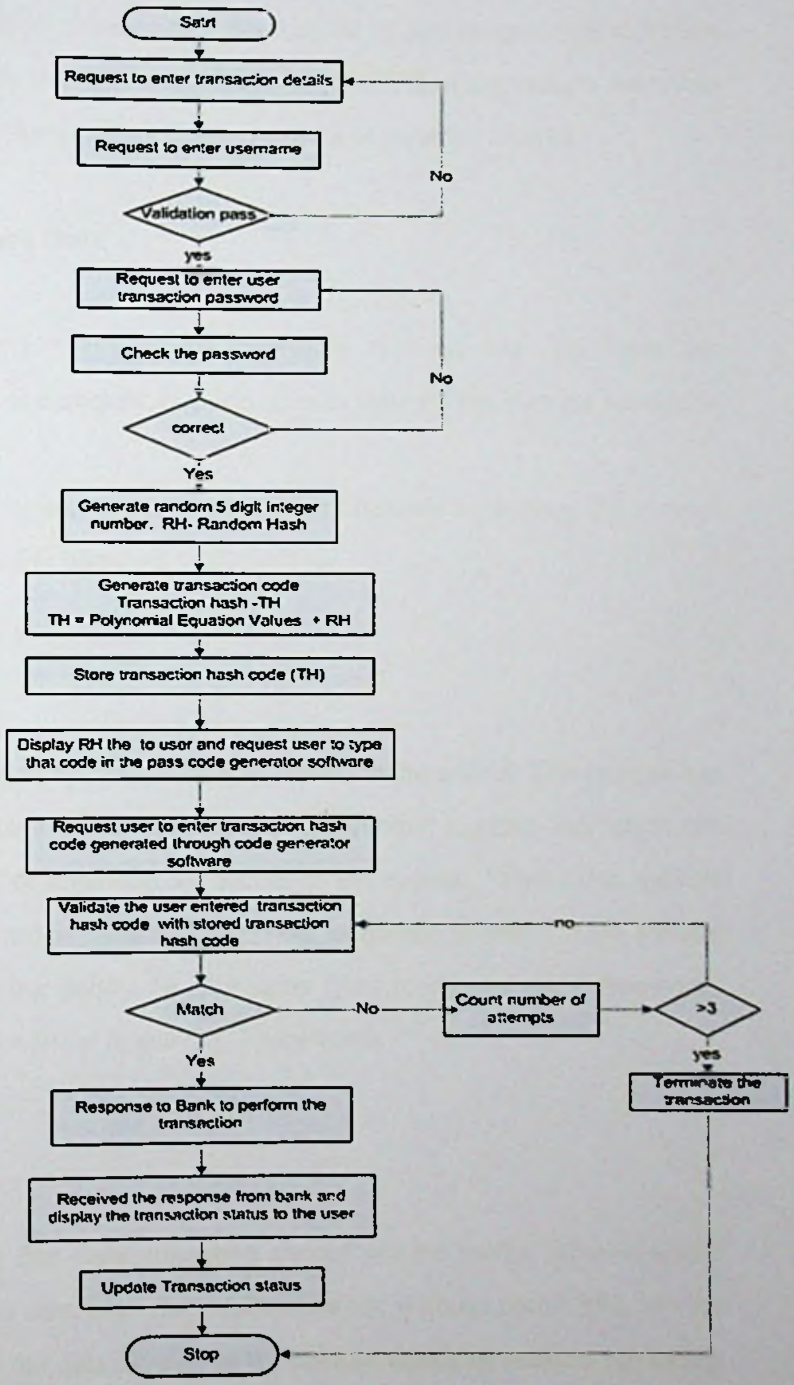

Satrt
Request to enter transaction details
Request to enter username
No
Validation pass
yes
Request to enter user transaction password
Check the password
No
correct
Yes
Generate random 5 digit integer number. RH- Random Hash
Generate transaction code Transaction hash -TH TH = Polynomial Equation Values + RH
Store transaction hash code (TH)
Display RH the to user and request user to type that code in the pass code generator software
Request user to enter transaction hash code generated through code generator software
Validate the user entered transaction hash code with stored transaction hash code
no
Match
No
Count number of attempts
>3
yes
Terminate the transaction
Yes
Response to Bank to perform the transaction
Received the response from bank and display the transaction status to the user
Update Transaction status
Stop

Figure 5.4:Transaction Authenticate Processing

5.6 Additional Security Enhancements for Solution

In order to provide maximum level of security it is essential to pay attention on different types of security threads towards web based applications. The following section describes the different types of security enhancements design to prevent security attacks.

Automatic System Session Time Outs

This will protect against users who left the computer without log out from the application. Therefore, system is designed to automatically destroy the current session if it is ideal more than 10 minutes.
In PHP session_destroy() and session_unset() functions can be used to destroy the current sessions if the session expire its life time.

Validate System Logins

This is also a very important security feature which needed to be added. The system has four different logging screens to logon to the system. If a proper logging validation not implemented, there can be risk of unauthorized access to the system. Therefore, system designs to encrypt user password with SHA2 function available in PHP. Also system designed with Password enforcing policy. In here users need to change their passwords every 3 months and they will not allow to use last 3 passwords.

Implement SSL

The SSL should use anywhere that communication should not be public. This is also a very important, because transfer data over the public network without using SSL is very risky. There is a risk of hacked the data by man in the middle attack or session hijacking. It is designed to implement SSL to payment processing page and the logging pagers. The data transfer client end to server should be encrypted using 265 bit SSL encryption in order give more security.

Prevent Against Phishing Attacks

Phishing attacks are most common type of security thread in today. Educating user about the phishing attack is not enough because today hackers are use different techniques to do this. Therefore, it not an easy task to identify it directly. The system design should implement in order to prevent users form phishing attacks.

In Safer Pay when the client performing a transaction, first it will ask the system username. Then the system validates that username and if it is a valid one system shows the word phrase belongsto the user. The user should only proceed the transaction if the word phrase is belongs to him or her. This word phrase should be given by the user at the registration process. From this design it is possible to prevent phishing attacks.

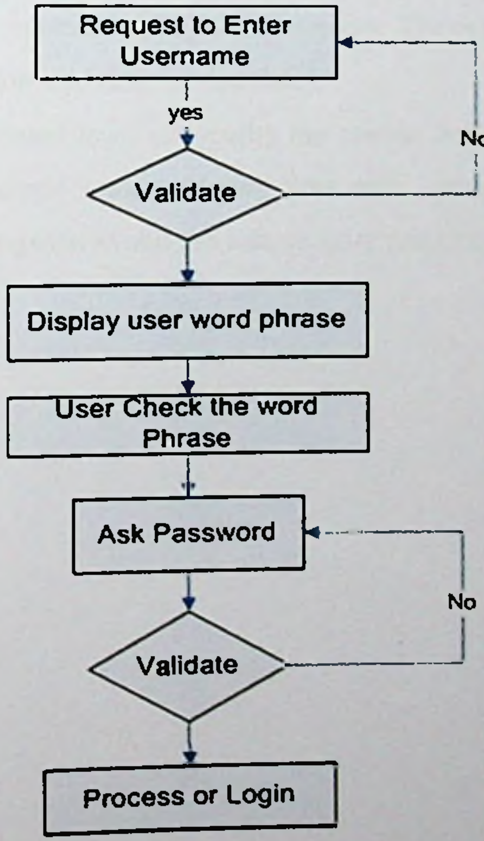


Figure 5.5: Phishing Attacks Validate Processing

Use the best security practices in PHP and MySQL

The application mainly uses PHP as the server side programing language and MySQL as the system database. Therefore it essential the system should be design according to the best security practices available in the PHP and MySQL. Otherwise this loophole may be use by the hackers to do harmful activates.

5.7 Summary

The system designed to fulfill the identified requirements and deliver maximum level of security to the electronic payments. The introduced solution is name as Safer Pay. Mainly there are three types of users involved in this system namely, Customers, Banks and Merchants. The system has main five modules. The payment process module and user master data management module used by the customers. The other modules are Banker's Module, Merchant's Module and Admin Module.

In order to provide maximum level of security the system designed with other security enhancements, like automatic system session time outs, secure client end with SSL, design for prevent phishing attacks and use best security practices in PHP and MySQL.

Chapter 6

The System Implementation Background

6.1 Introduction

Implement the solution based on the system design is the next important part of the project. This section talks about the system implementation detail. First it is essential to select correct tools to implement the solution and those selected tools need to be setup correctly. Once the implementation environment was setup correctly then system implementation should start according to the system design.

6.2 Software used to the Development

In the implementation process select the correct software development tools are important. The following section describes the tools used to implement the system.

Adobe Dreamweaver

It is a popular responsive web design tool developed by Adobe. This project Dreamweaver is used as a HTML, CSS and PHP editor.

Wamp Server

Wamp Server is software that can be installed on Microsoft Windows operating system. The Wamp Server consisting of the Apache web server, MySQL database and PHP programming language. Also it supports OpenSSL for SSL. The Apache is use for run the core application. The MySQL database available in Wamp Server used for creates the application database.

Visual Studio 2010

Visual Studio 2010 is a complete suite of software development and management tools. This tool used for develop client end secure token generating application.

6.3 Recommended System Requirements

Server Requirements

Hardware Requirements	
Processor	Intel® Xeon® E3-1220 v3 3.1GHz, 8M Cache
Memory	16 GB
Hard Disk	1TB with RAID 3
Network	Gigabyte Ethernet

Table 6.1: Sever Software Requirements

Software Requirements	
Web Server OS	Centos6
Web Server	Apache 2.2 or above
Database Technology	MySQL Version 5.5 or above

Table: 6.2 Sever Software Requirements

Client Requirements

Hardware Requirements	
Processor	Dual Core 2.5MHz
Memory	1GB
Hard Disk	Minimum 5 MB
Network	Minimum 512kbps Internet connection

Table: 6.3 Client End Hardware Requirements

Software Requirements	
OS	Windows, Linux
Web browser	IE 7, Fire Fox

Table: 6.4 Client End Software Requirements

6.4 Summqry

This section main focused to review the implementation background of the system. At this stage of the project it is very difficult to say much information about this section. The development tools are selected to achieve the design requirements easily. The recommended system requirements also defined when the system implements in production environment.

Chapter 7

System Testing and the Evaluation

7.1 Introduction

Testing and the evaluation is one most important the critical aspect of any research project. It is the process by which a system compared against identified requirements and specifications through testing. The results of the project evaluated to measure the progress and the performance of the final output results.

The testing of this system can be mainly divided into three levels

- Unit Testing
- System Testing
- User Acceptance Testing

The unit testing is the smallest level of the testing and it checks that each unit is working properly according to the system requirements. The unit testing of this system competed at the development process of the each unit.

The functional or the system testing is used to examine the system high-level design. Also it helps to find out the customer requirements were met. Therefore, the black box testing techniques was used to perform the system testing. In black box testing technique it examines the functionality of a system based on the system specifications.

After successfully complete the system testing, the product should be delivered to the system users. Once the product is delivered to the users, they run and test the system based on their expectations of the functionality. This result is important because system users are the people who finally use the system.

7.2 Test cases

Home Page – Login to System

Test Case ID	**001**
Procedure	Click on the login button without providing username
Input data	Lave Blank
Actual Results	Display error and ask to enter username
Expected Results	Display error and ask to enter username
Tested by	Buyer, Seller, Admin

Test Case ID	**002**
Procedure	Click on the login button with invalid username
Input data	Invalid Username
Actual Results	Display error and request to enter correct username
Expected Results	Display error and request to enter correct username
Tested by	Buyer, Seller, Admin

Test Case ID	**003**
Procedure	Click on the login button with valid username
Input data	Valid Username
Actual Results	Direct user into system password request page
Expected Results	Direct user into system password request page
Tested by	Buyer, Seller, Admin

Test Case ID	**005**
Procedure	Click on the login button with invalid password
Input data	invalid Username
Actual Results	Display error and request to enter correct password
Expected Results	Display error and request to enter correct password
Tested by	Buyer, Seller, Admin

Test Case ID	**006**
Procedure	Click on the login button without providing password
Input data	Lave Blank
Actual Results	Display error and ask to enter password
Expected Results	Display error and ask to enter password
Tested by	Buyer, Seller, Admin

Test Case ID	**007**
Procedure	Click on the login button with correct password
Input data	Correct system password
Actual Results	Direct user into system home page
Expected Results	Direct user into system home page
Tested by	Buyer, Seller, Admin

Payment Processing Process

Test Case ID	**008**
Procedure	Click on the submit button without providing username
Input data	Lave Blank Fill the amount
Actual Results	Display error and ask to enter username
Expected Results	Display error and ask to enter username
Tested by	Buyer

Test Case ID	**009**
Procedure	Click on the login button with invalid username
Input data	Invalid Username Fill the amount
Actual Results	Display error and ask to enter username correct username
Expected Results	Display error and ask to enter username correct username
Tested by	Buyer

Test Case ID	**010**
Procedure	Click on the login button with valid username and amount
Input data	Valid Username Fill the amount
Actual Results	Move to next second authentication page and display the word phrase belongs to that user
Expected Results	Move to next second authentication page and display the word phrase belongs to that user
Tested by	Buyer

Test Case ID	**011**
Procedure	Click on the verify button with blank values for both Token Code and Transaction Password
Input data	Blank Token Code Blank Transaction Password
Actual Results	Request to enter values for Token Code and Transaction Password
Expected Results	Request to enter values for Token Code and Transaction Password
Tested by	Buyer

Test Case ID	**012**
Procedure	Click on the verify button with blank values for both Token Code and Transaction Password
Input data	Blank Token Code Blank Transaction Password
Actual Results	Request to enter values for Token Code and Transaction Password
Expected Results	Request to enter values for Token Code and Transaction Password
Tested by	Buyer

Test Case ID	**013**
Procedure	Click on the verify button with invalid Token Code and invalid Transaction Password
Input data	Invalid Token Code Invalid Transaction Password
Actual Results	Display Error and mentioned transaction status as failed
Expected Results	Display Error and mentioned transaction status as failed
Tested by	Buyer

Test Case ID	**014**
Procedure	Click on the verify button with valid Token Code and invalid Transaction Password
Input data	Valid Token Code Invalid Transaction Password
Actual Results	Display Error and mentioned transaction status as failed
Expected Results	Display Error and mentioned transaction status as failed
Tested by	Buyer

Test Case ID	**015**
Procedure	Click on the verify button with invalid Token Code and valid Transaction Password
Input data	Invalid Token Code Valid Transaction Password
Actual Results	Display Error and mentioned transaction status as failed
Expected Results	Display Error and mentioned transaction status as failed
Tested by	Buyer

Test Case ID	**016**
Procedure	Click on the verify button with valid Token Code and valid Transaction Password
Input data	Valid Token Code Valid Transaction Password
Actual Results	Display transaction reference number and mentioned transaction status as success.
Expected Results	Display reference number and mentioned transaction status as success.
Tested by	Buyer

Secure Token Recovery

Test Case ID	**016**
Procedure	Logon to the system and go to token recovery link.
Input data	Enter incorrect system logging password
Actual Results	Display Error
Expected Results	Display Error
Tested by	Buyer

Test Case ID	**017**
Procedure	Logon to the system and go to token recovery link.
Input data	Enter correct system logging password
Actual Results	Disabled the old token and enable new token software to download
Expected Results	Disabled the old token and enable new token software to download
Tested by	Buyer

7.3 The User Acceptance Testing

The main objective of this testing is to determine whether the system satisfies the user requirements and expectations. In order to find the user acceptance, the final system is given to twenty randomly selected users with a basic training about how to use the system. Then users were instructed to use the system by themselves. Finally user feedbacks were collected by using small questionnaire distributed among the users. The sample of the distributed questionnaire mentioned in the Appendixes D section.

The results shows that seventeen out of twenty users believed this system can provide good security against the security threads towards on line electronic payment transfer compare to existing electronic payment systems. Also twelve believed that system can easily learn and simple.

7.4 The System Evolution and Results

The evolution is really important to all the party who involved with the system development project. Mainly it helps to identify what has been accomplished through the system project development process. On the other hand it helps to find out the problems faced during the project implementation process. Finally evolution is important to suggest any further development to the project.

This project consisted with main five objectives. It is necessary to find out the the ultimate objectives of the project were achieved or not. Therefore, finally the system had been reviewed by the endusers and observed that the ultimate objectives of the project were achieved. The system can provide the good security against the current security threads towards the electronic payment systems. The end users of the system believed that system can easily learn and has quick response time. The detailed description of the project results mentioned in below.

Project Evolution Results in Points

- The SaferPay can provide good security against the Man in the Middle Attacks. Because the system mainly authenticates the transactions using one time secure code and that code is a combination of the two codes generated in two different ends. The transaction code is anevent based one. Alsoperson who stole the transaction code cannot generate secure code without having the secure token generation application belongs to that user.
- The system design implemented to prevent users form phishing attacks. The phishing attacks can prevent through enhanced two step authentication model. In this method user only provides the confidential information if the username identified by the system and the word phrase is belong to that user.
- The system is also equated with strong password policies. The users should change their password every three months and system always checks the complexity level of the passwords before accept them. The password policies will be a front line of defense to confidential user information because the week passwords are always at higher risk of attacks.
- The system designed to secure the MySQL from the possible SQL Injection attempts. All the data filler through the PHP secure class before send them in to data base queries.
- As a good security practices the system stored the password and other confidential data in encrypted (Sha2) manner in database. The main objective of this is to secure the confidential data in event of authorized access to system databases.
- The Automatic System Session Time Outs will protect against users who left the computer without log out from the application.
- The system takes the necessary precautions to prevent the session hijacking attacks. As best practice to prevent sensitive data should travel through secure communication channel. Therefore, system transmits the data through the SSL/HTTPS protocols.

7.5 Summary

This section main focused to Testing and the evaluation. The testing of this system can be mainly divided into three levels which are Unit Testing, System Testing, and User Acceptance Testing. The unit testing of this system competed at the development process of the each unit. The black box testing techniques was used to perform the system testing. The final system is given to twenty randomly selected users to check the user acceptance. The SaferPay can provide good security mainly against the Man in the Middle Attacks, phishing attacks and the SQL Injection attempts.

Chapter 8

Conclusion & Further work

8.1 Introduction

E-Commerce can be defined as one of the rapidly development mechanisms in world. There are various kinds of electronic payment systems available for customers. However, there are some issues which should be circumvented or avoid in the existing electronic payment system methods.

In this project first it examined the currently available e-payment authentication systems models and identify the security threads and problems associated with them. This objective was achieved through the prevoius research background analysis. The next objective is to introduce a secured e-payment authentication system to minimize the existing security threads towards to electronic commerce transitions. The introduced solution is name as Safer Pay. The payments are authenticating by secure token that generated through secure token generating application. This solution can provide more security because securer code is generated in combination of the two ends. Also it equip with other additional security enhancements. The final step is to find out up to which level proposed system can address the current security threads for e-payment systems. The project evaluation and the user acceptance testing mainly used for achieved this objective. The results showed that this system can provide good security against the man in the middle attacks and the phishing attacks. Also most of the users believed this system can provide good security against the security threads towards on line electronic payment transfer compare to existing electronic payment systems.

8.2 Importance of Research

Because of the security problems in the existing electronic payment systems some of the customers are reluctant to use electronic commerce. Therefore it is directly impact with the sales of the e-commerce portal.

In this research project there is an attempt to fill the research gap and find a secure e-payment authentication model for E-commerce portals. As a result this model will helps to increase the security level of the e-commerce portals and increase the customer confidence about the security of their payments. Finally due to the proposed e-commerce portals can enhance the customer satisfaction by providing quality secure payment method to their customers and it helps to save resources in industry and their customers.

8.3 Limitations of the Research

The main limitation to this research is working with security which is not an easy task because, security is a wide area and it requires very good understanding about different areas related to the security. In that case expert knowledge in these areas may require. Also it is really difficult to find a model for assurance of hundred present security for electronic payment systems but the proposed model will be able to minimize the security threats comparing to issues of the existing electronic payment models. Also it requires some time to carefully analyze things. This research project is scheduled to be completed in less than one year, the time constraints also will be another limitation.

8.4 Research Further Works

- The secure token generating application can be developed for different platform such as Android, Apple IOS and Windows mobile
- The system can be develop for directly communicate with core banking systems of the registered banks without any user involvement.
- Currently the system designed to validate electronic payment in e-commerce portals. This design can develop to validate any kind of electronic payment such as electronic payments in POS or any other electronic fund transferring activities.
- It is essential to implement reverse engineering prevention methods for secured token application.

Reference

[1]E. Turban, J. Lee, D. King and H.M. Chung, Electronic Commerce: A Managerial Perspective, Prentice Hall, 1999.

[2] H. Bidgoli, Electronic commerce. San Diego: Academic Press, 2002

[3]M. Niranjanamurthy and D. Chahar, 'The study of E-Commerce Security Issues and Solutions', International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 7, 2013.

[4] Paypal.com, 'PayPal Security Key', 2015. [Online]. Available: https://www.paypal.com/us/cgibin?cmd=xpt/Marketing_CommandDriven/securitycenter/PayPalSecurityKey-outside&bn_r=o. [Accessed: 05- Feb- 2015].

[5] Gary Scjmedider. "Introduction to Electronic Commerce" in electronic commerce, 9th edition., Thomson, 2007, pp.1-50.

[6]Rana Tassabehji ,Understanding e-commerce for Business,vol.1,2009

[7] Marketing Charts, '875MM Consumers Have Shopped Online #8211; Up 40% in Two Years', 2008.[Online].Available:http://www.marketingcharts.com/online/875mm-consumers-have-shopped-online-up-40-in-two-years-3225/. [Accessed: 05- Feb- 2015].

[8] G. Udo, 'Privacy and security concerns as major barriers for e-commerce: a survey study', Information Management & Computer Security, vol. 9, no. 4, pp. 165-174, 2001.

[9]P. Havinga, G. Smit and A. Helme, 'SURVEY OF ELECTRONIC PAYMENT METHODS AND SYSTEMS', 2013.

[10]Gary Scjmedider. Introduction to Electronic Commerce in electronic commerce, 9th edition., Thomson, 2007, pp.1-50.

[11]RanaTassabehji, Applying E-Comerce in Business, New Delhi, 2003

[12]RanaTassabehji ,Understanding e-commerce for Business,vol.1,2009

[13] Emarketer.com, 'Worldwide Ecommerce Sales to Increase Nearly 20% in 2014 - eMarketer', 2015. [Online]. Available: http://www.emarketer.com/Article/Worldwide-Ecommerce-Sales-Increase-Nearly-20-2014/1011039. [Accessed: 03- Nov- 2015].

[14] Nielsen, 'E-COMMERCE: EVOLUTION OR REVOLUTION', nielsen, 2014.

[15] Inc.com,'7 E-Commerce Trends to Watch in 2015', 2015. [Online]. Available: http://www.inc.com/rebecca-borison/top-trends-in-ecommerce-for-new-year.html. [Accessed: 03- Nov- 2015].

[16] Amasty, 'E- COMMERCE TRENDS FOR 2014', 2015.

[17] LexisNexis, '2014 LexisNexisÂ® True Cost of FraudSM Study', 2014.

[18] Tesch, D.; Kloppenborg, T.J.; Frolick, M.N.; It Project Risk Factors: The Project ManagementProfessionals Perspective, The Journal of Computer Information Systems; Summer 2007; 47, 4;ABI/INFORM Global, pg. 61.

[19]A. Koponen, 'E-COMMERCE, ELECTRONIC PAYMENTS', Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, 2015.

[20]G. Schneider, E-Commerce: Strategy, Technology, and Implementation, 9th ed. 2012.

[21]O. Sorokina, 'Everything You Need To Know About Social Payments', Hootsuite, 2015.

[22] G. Udo, 'Privacy and security concerns as major barriers for e-commerce: a survey study', Information Management & Computer Security, vol. 9, no. 4, pp. 165-174, 2001.

[23] LexisNexis, '2014 LexisNexis® True Cost of FraudSM Study', 2014.

[24]D. Abrazhevich, Electronic payment systems: a user-centered perspective and interaction design. Eindhoven: TechnischeUniversiteit Eindhoven, 2004.

[25]M. Niranjanamurthy and D. Chahar, 'The study of E-Commerce Security Issues and Solutions', International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 7, 2013.

[26]P. Havinga, G. Smit and A. Helme, 'SURVEY OF ELECTRONIC PAYMENT METHODS AND SYSTEMS', 2015

[27]D. Abrazhevich, Electronic payment systems: a user-centered perspective and interaction design. Eindhoven: TechnischeUniversiteit Eindhoven, 2004.

[28]M. Niranjanamurthy and D. Chahar, 'The study of E-Commerce Security Issues and Solu-tions', International Journal of Advanced Research in Computer and Communication Engineer-ing, vol. 2, no. 7, 2013.

[29]Aigbe, P., Akpojaro, J., 2014. Analysis of Security Issues in Electronic Payment Systems. Int. J. Comput. Appl. 108.

[30]Kaur, J., 2011. Empirical Study in the Security of Electronic Payment Systems Anita Goyal.

[31]Schneier, B., 2005. Two-factor authentication: too little, too late. Commun ACM 48, 136.

[32] S. J Murdoch and R. Anderson, 'Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication', Computer Laboratory, University of Cambridge, UK.

[33] ComputerWeekly, 'Understanding web technology', 2015. [Online]. Available: http://www.computerweekly.com/feature/Understanding-web-technology. [Accessed: 06-Nov- 2015].

[34] Weblogs.foxite.com, 'Introduction to Client Server Architecture | | Foxite.COM Community Weblog - Andy KramekFoxite.COM Community Weblog – Andy Kramek', 2015. [Online]. Available: http://weblogs.foxite.com/andykramek/2008/09/29/introduction-to-client-server-architecture/. [Accessed: 06- Nov- 2015].

[35] R. Shannon, 'The History of HTML | From the HTML 1.0 spec to XHTML 1.0..', Yourhtmlsource.com,2015.[Online].Available:http://www.yourhtmlsource.com/starthere/historyofhtml.html. [Accessed: 10- Nov- 2015].

[36] Cssneuse.net, 'The History of CSS - Css Neuse - CSS Information', 2015. [Online]. Available: http://www.cssneuse.net/the-history-of-css.php. [Accessed: 10- Nov- 2015].

[37] W3techs.com, 'Usage Statistics and Market Share of Server-side Programming Languages for Websites, November 2015', 2015. [Online]. Available: http://w3techs.com/technologies/overview/programming_language/all. [Accessed: 09- Nov- 2015].

[38] Php.net, 'PHP: What is PHP? - Manual', 2015. [Online]. Available: http://php.net/manual/en/intro-whatis.php. [Accessed: 09- Nov- 2015].

[39] Scholar.lib.vt.edu, 'A brief history of PHP', 2015. [Online]. Available: http://scholar.lib.vt.edu/manuals/php3.0.6/intro-history.html. [Accessed: 09- Nov- 2015].

[40] Msdn.microsoft.com, '.NET Framework Versions and Dependencies', 2015. [Online]. Available: https://msdn.microsoft.com/en-us/library/bb822049(v=vs.110).aspx. [Accessed: 09- Nov- 2015].

[41]H. MySQL, 'Database Friends: History of MySQL', Databasefriends.co, 2014. [Online]. Available: http://www.databasefriends.co/2014/02/history-of-mysql.html. [Accessed: 10- Nov- 2015].

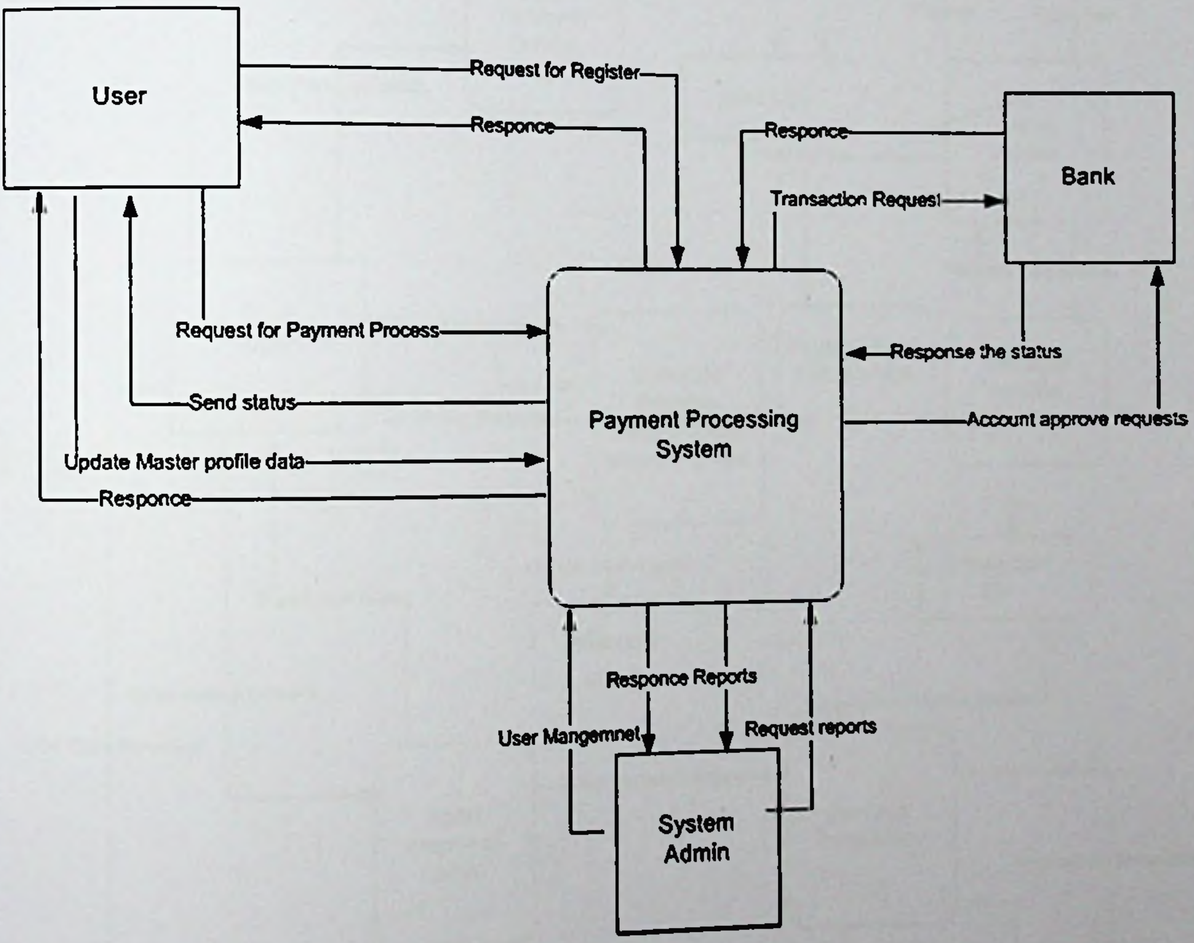
[42]S. Tahaghoghi and H. Williams, Learning MySQL. Sebastopol, Calif.: O'Reilly, 2007.

[43] Digicert.com, 'What Is SSL (Secure Sockets Layer)? | DigiCert.com', 2015. [Online]. Available: https://www.digicert.com/ssl.htm. [Accessed: 12- Nov- 2015].

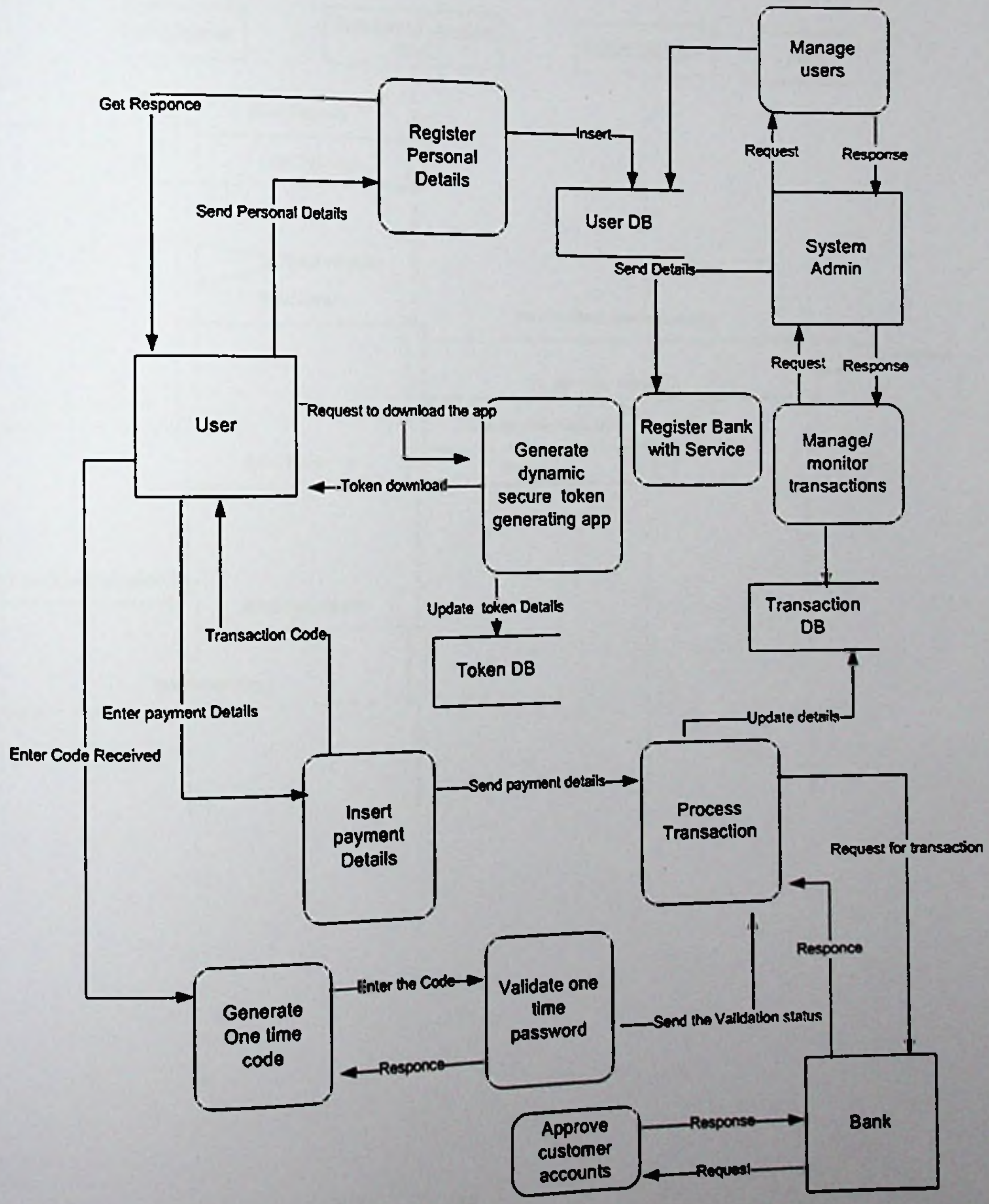
Appendix

Appendix A – The System Diagrams

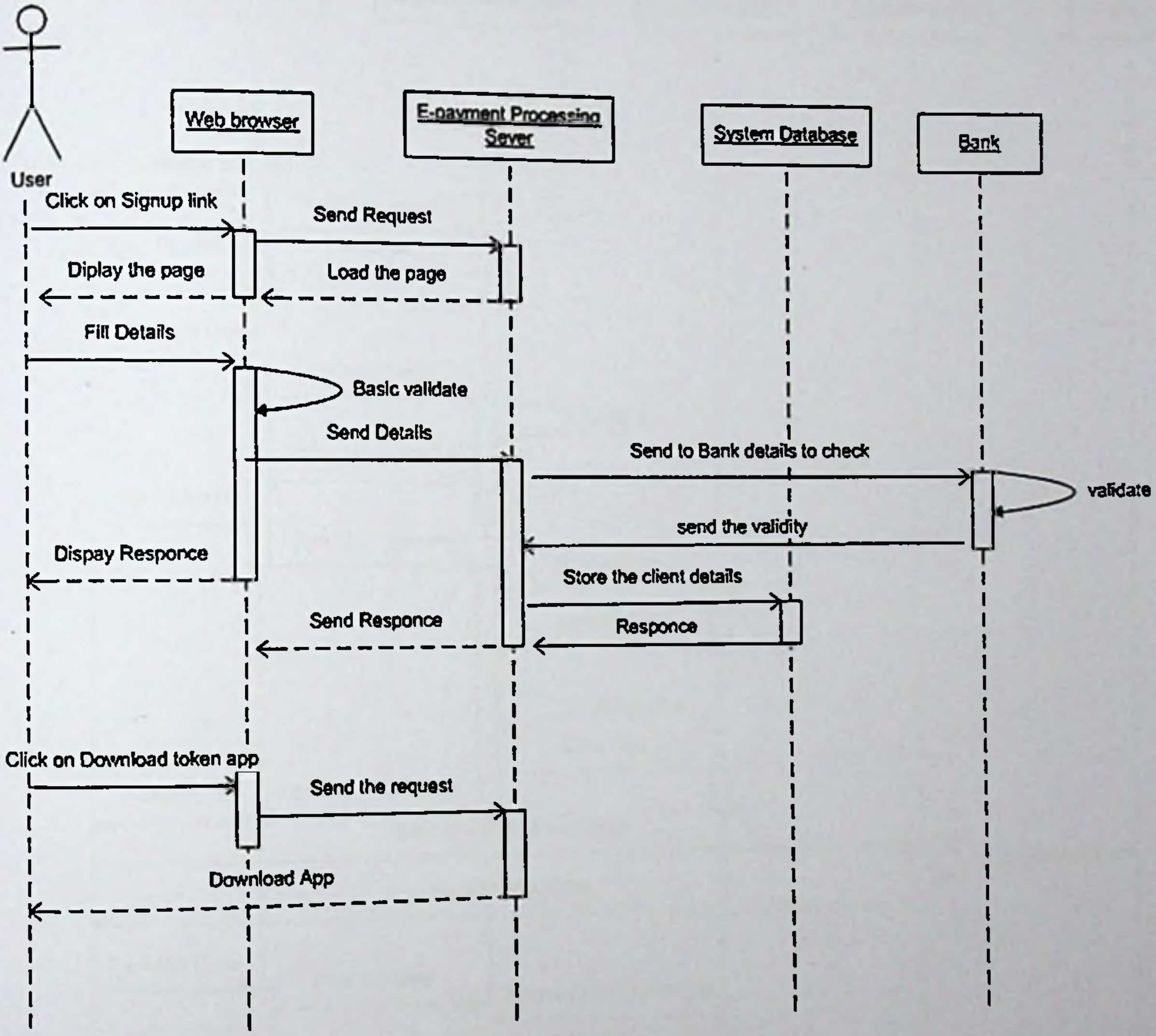
System Context Diagram



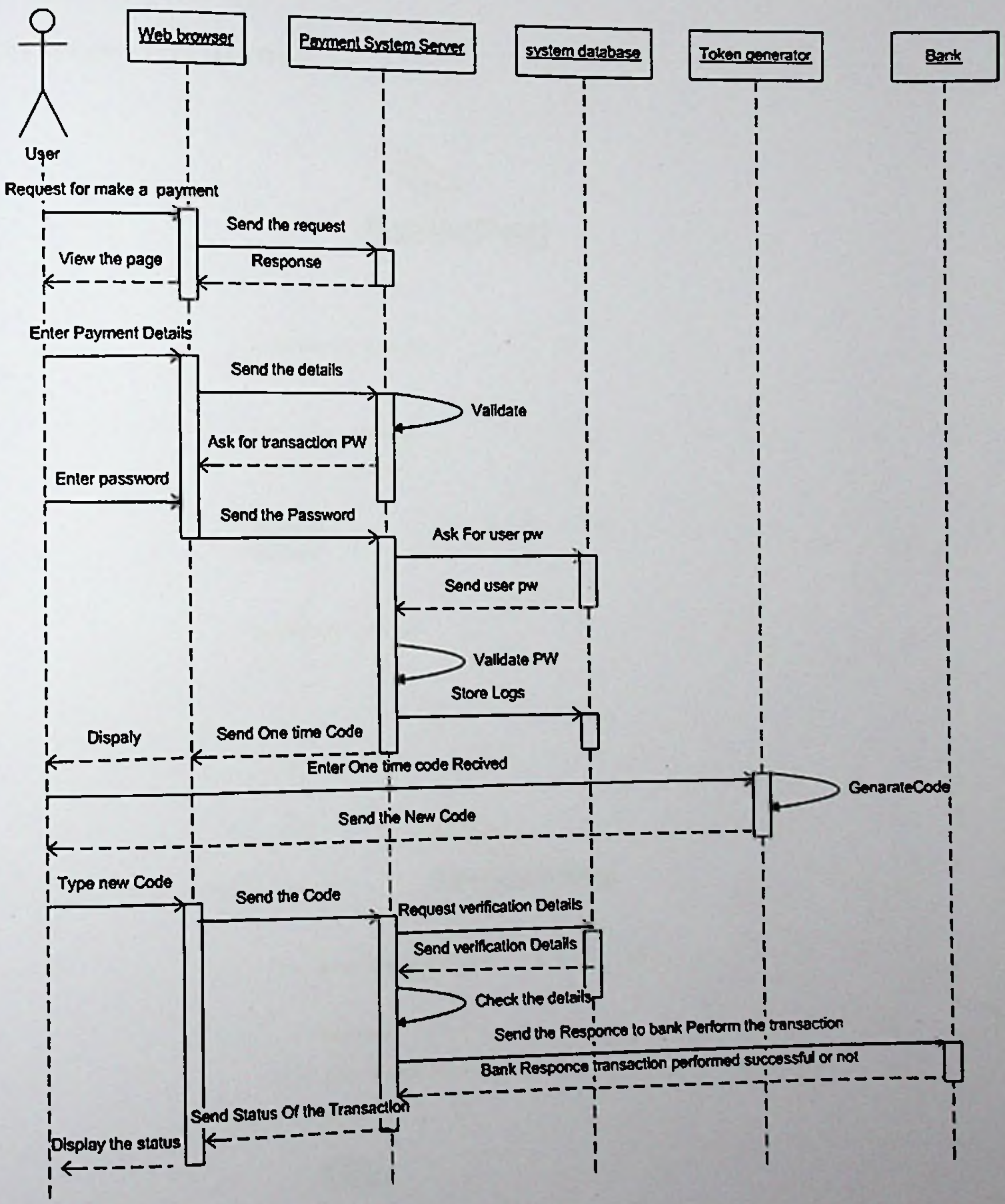
Level 1 Data Flow Diagram



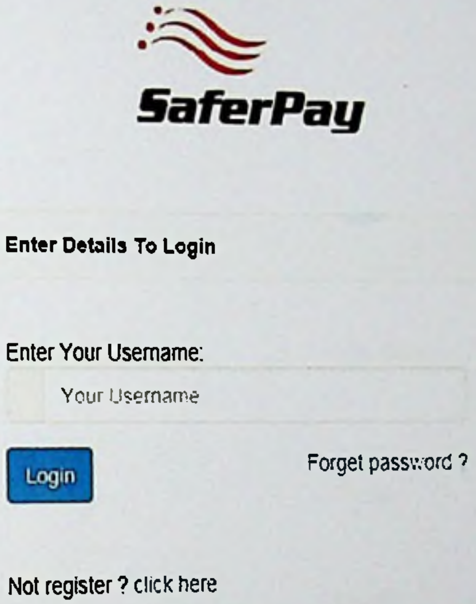
User Registration Process - Sequence Diagram



User Process a Transaction - Sequence Diagram



The System Login Interfaces

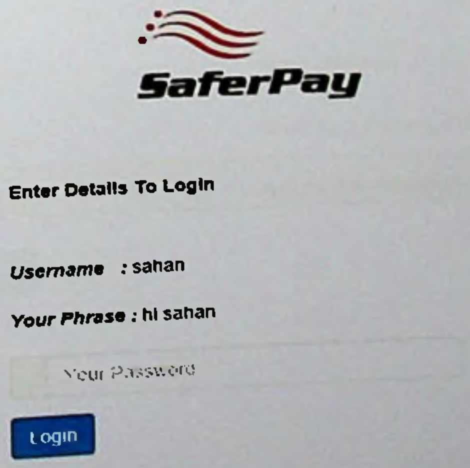


Enter Details To Login

Enter Your Username:

Forget password ?

Not register ? click here

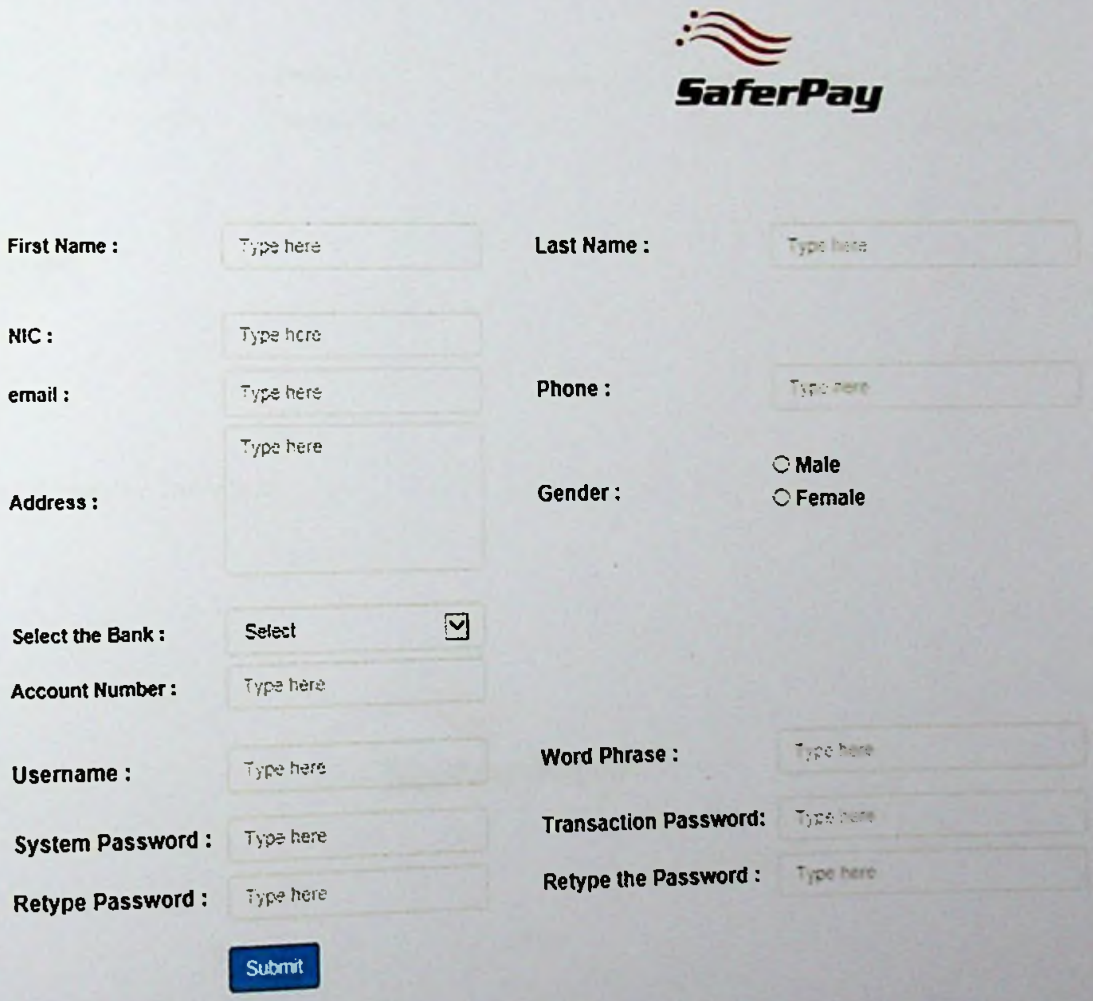


Enter Details To Login

Username : sahan

Your Phrase : hi sahan

The Buyer Registration From



SaferPay

First Name : Type here

Last Name : Type here

NIC : Type here

email : Type here

Phone : Type here

Address : Type here

Gender : ○ Male ○ Female

Select the Bank : Select

Account Number : Type here

Username : Type here

Word Phrase : Type here

System Password : Type here

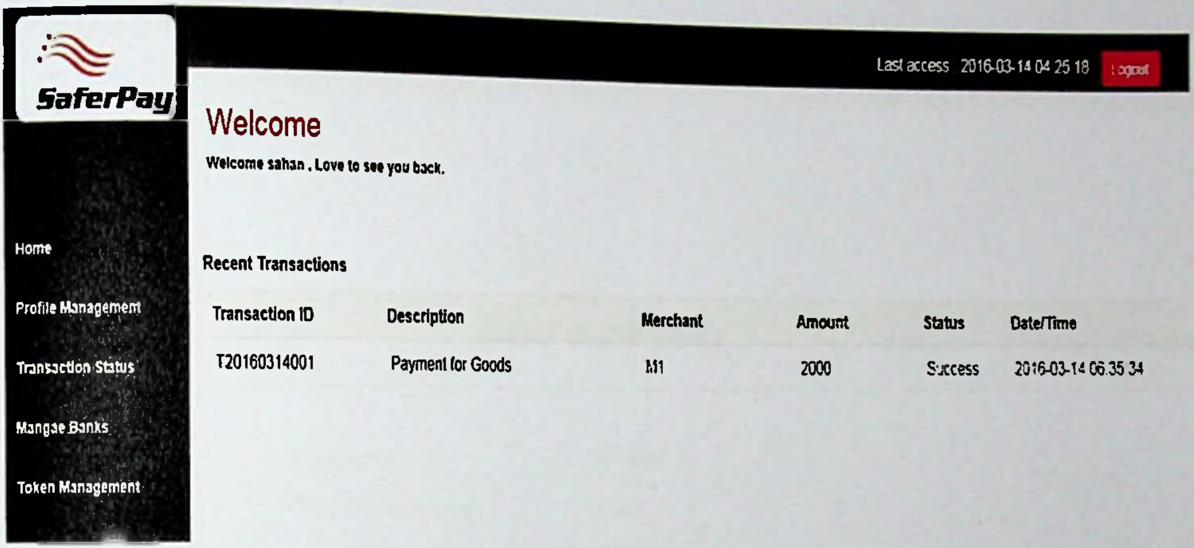
Transaction Password: Type here

Retype Password : Type here

Retype the Password : Type here

Submit

The User Home Page After Successfully Login



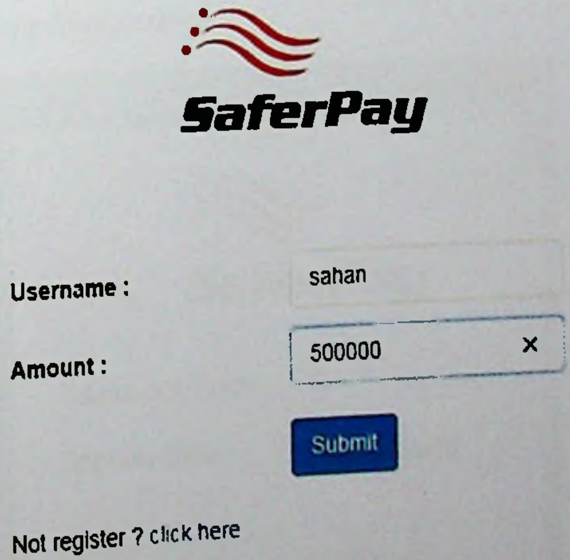
Welcome

Welcome sahan . Love to see you back.

Recent Transactions

Transaction ID	Description	Merchant	Amount	Status	Date/Time
T20160314001	Payment for Goods	M1	2000	Success	2016-03-14 06.35 34

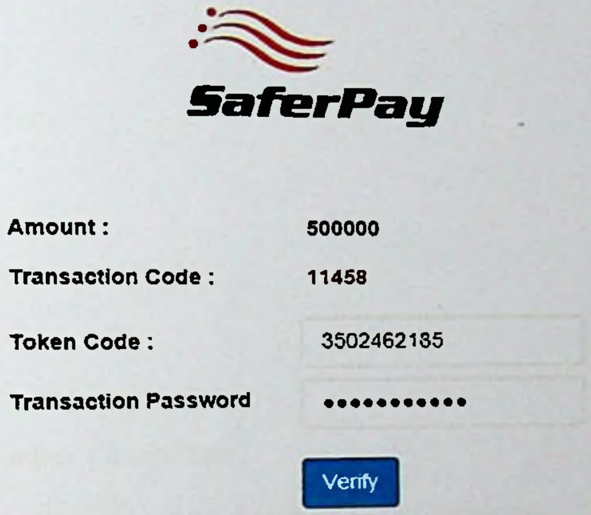
Payment Transfer Interface



Username : sahan

Amount : 500000

Transaction Authenticate Page



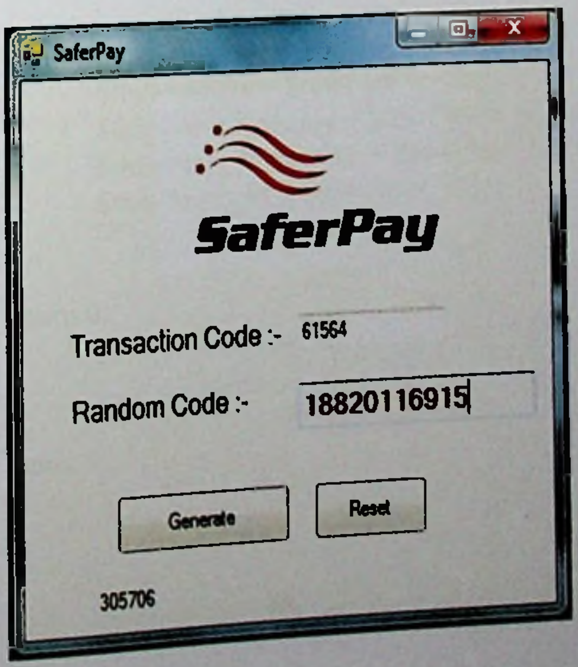
Amount : 500000

Transaction Code : 11458

Token Code : 3502462185

Transaction Password ●●●●●●●●●●●

Secure Code Generating Application



Transaction Code :- 61564

Random Code :- 18820116915

305706

User class.php

```
<?php
class user
{
        var $username;
        var $user_id;
        var $login_count;
        var $user_level;
        var $email;
        var $active;
        var $word_phrase;
        var $last_login_date;


                functionuser_check($user)
        {
                $sql = sprintf("SELECT * FROM tbl_user WHERE username = '%s'",
$user);
                $result = mysql_query($sql);
                if (mysql_num_rows($result) > 0)
                {
                        while ($row = mysql_fetch_array($result))
                        {
                                $this->username = $row['username'];
                                $this->active = $row['active_flage'];
                                $this->word_phrase = $row['word_phrase'];
                                $this->last_login_date = $row['last_login_date'];
                                $this->user_id = $row['user_id'];


                        }
                        return 0;
                }
                else
                {
                        return 1;
                }
        }
```

```
                function login($user,$pass)
        {
                $pass = sha1($pass);
                $sql = sprintf("SELECT * FROM tbl_user  WHERE username = '%s'
AND system_password = '%s' AND active_flage  = 'Y'", $user, $pass);
                $result = mysql_query($sql);
                if (mysql_num_rows($result) > 0)
                {
                while ($row = mysql_fetch_array($result))
                        {
                                $this->set_login_count($user);
                                $this->email = $row['email'];
                                $this->first_name = $row['first_name'];
                                $this->last_name = $row['last_name'];
                                $this->last_login_date = $row['last_login_date'];
                                $this->login_count = $row['login_count'];
                                $this->user_level = $row['usergroup'];


                        }
                        return 0;

                }
                else
                {
                        return 1;
                }
        }
        functiontransaction_login($user,$pass)
        {
                $pass = sha1($pass);
                $sql = sprintf("SELECT * FROM tbl_user  WHERE username = '%s'
AND transaction_password = '%s' AND active_flage  = 'Y'", $user, $pass);
                $result = mysql_query($sql);
                if (mysql_num_rows($result) > 0)
                {
                        while ($row = mysql_fetch_array($result))
                        {
                     $this->user_id = $row['user_id'];

                        }
                                return 0;

                }
                else
        {
            return 1;
        }
    }

    functionget_email($user)
    {
        $sql = sprintf("SELECT * FROM tbl_user WHERE username = '%s'
AND active = 'Y'", $user);
        $result = mysql_query($sql);
        if (mysql_num_rows($result) > 0)
        {
            while ($row = mysql_fetch_array($result))
            {
                $email = $row['email'];
            }
            return $email;
        }
        else
        {
        return 'Error';
        }
    }

    functionget_login_count($user)
    {
        $count = 0;
        $sql = "SELECT * FROM tbl_user WHERE username = '$user'";
        $result = mysql_query($sql);
        while ($row = mysql_fetch_array($result))
        {
            $count = $row['login_count'];
        }
        return $count;
    }

    functionset_login_count($user)
    {
        $lc1 = $this->get_login_count($user);
        $lc1 = $lc1 + 1;
        $date = date('Y-m-d H:i:s');
        $sql = sprintf("UPDATE tbl_user SET login_count = '$lc1',
last_login_date = '$date' WHERE username='%s'", $user) ;
        $result = mysql_query($sql);
    }
```

```
        functiondelete_app_user($user,$id)
        {
                require('security.class.php');
                $sec = new security();
                $user = $sec->filter($user);
                $id = $sec->filter($id);
          $sql = sprintf("SELECT * FROM tbl_user WHERE username = '%s' AND aid
= '%d'", $user, $id);
                $result = mysql_query($sql);
                if (mysql_num_rows($result) > 0)
                {
                        $query = sprintf("DELETE FROM tbl_user  WHERE username =
'%s' AND aid = '%d'", $user,$id);
                        $res = mysql_query($query);
                        $q = sprintf("SELECT * FROM tbl_user WHERE username = '%s'
AND aid = '%d'",  $user,$id);
                        $r = mysql_query($q);
                        if (mysql_num_rows($r) > 0)
                        {

                                return 2;
                        }
                        else
                        {
                                //require('log.class.php');
                                //$log = new log_file();
                                //$log->write_log($_SESSION['sta_sys_un'], "Delete
User", "$user", "process");
                                return 0;
                        }

                }
                else
                {
                        return 1;
                }
        }

        functiondisable_app_user($user, $id)
        {
                require('security.class.php');
                $sec = new security();
                $user = $sec->filter($user);
                $id = $sec->filter($id);
                $sql = sprintf("SELECT * FROM tbl_user WHERE username = '%s'
AND aid = '%d'", $user, $id);

                $result = mysql_query($sql);

                if (mysql_num_rows($result) > 0)
                {
                        $query = sprintf("UPDATE tbl_user SET active = 'N' WHERE
username = '%s' AND aid = '%d'", $user, $id);
                        $res = mysql_query($query);
                        $q = sprintf("SELECT * FROM tbl_user WHERE username = '%s'
AND aid = '%d' AND active = 'N'", $user, $id);
                        $r = mysql_query($q);
                        if (mysql_num_rows($r) > 0)
                        {
                                //require('log.class.php');
                                //$log = new log_file();
                                //$log->write_log($_SESSION['sta_sys_un'], "Disable
User", "$user", "process");
                                return 0;
                        }
                        else
                        {
                                return 2;
                        }
                }
                else
                {
                        return 1;
                }
                //return 0;
        }

        functionenable_app_user($user,$id)
        {
                require('security.class.php');
                $sec = new security();
                $user = $sec->filter($user);
                $id = $sec->filter($id);

                $sql = sprintf("SELECT * FROM tbl_user WHERE username = '%s'
AND aid = '%d'", $user, $id);
                $result = mysql_query($sql);
                if (mysql_num_rows($result) > 0)
                {
                        $query = sprintf("UPDATE tbl_user SET active = 'Y' WHERE
username = '%s' AND aid = '%d'", $user, $id);
                        $res = mysql_query($query);
                        $q = sprintf("SELECT * FROM tbl_user WHERE username = '%s'
AND aid = '%d' AND active = 'Y'", $user, $id);
                        $r = mysql_query($q);
                        if (mysql_num_rows($r) > 0)
                        {
                                //require('log.class.php');
                                //$log = new log_file();
                                //$log->write_log($_SESSION['sta_sys_un'], "Enable
User", "$user", "process");
                                return 0;
                        }
                        else
                        {
                                return 2;
                        }
                }
                else
                {
                        return 1;
                }
        }

                functiongeneratePassword ($length = 8)
        {
                $password = "";
                $possible =
"0123456789abcdfghjkmnpqrstvwxyz!#&@%*ABCDEFGHIJKLMNOPQRSTUVWXY
Z!#&@%*0123456789";
                $i = 0;
                while ($i< $length)
                {
                        $char = substr($possible, mt_rand(0,strlen($possible)-1), 1);
                        if (!strstr($password, $char))
                        {
                                $password .= $char;
                                $i++;
                        }
                }
                return $password;
        }
```

```
    functionchange_password($user, $old_pass, $new_pass)
    {
        require('security.class.php');
        include("database.php");
        $sec = new security();
        $user = $sec->filter($user);
        $old_pass_enc = sha1($sec->filter($old_pass));
        $new_pass_enc = sha1($sec->filter($new_pass));

        $sql = sprintf("SELECT * FROM tbl_user WHERE username = '%s'
AND password = '%s' AND  active= 'Y'", $user, $old_pass_enc);
        $result = mysql_query($sql);
        echomysql_num_rows($result);
        $act_date = date("Y-m-d") . " " . date("H:i:s");
        if (mysql_num_rows($result) > 0)
        {
            $sql01 = sprintf("UPDATE tbl_user SET password =
'%s',flag='%s' WHERE username='%s'", $new_pass_enc,'A', $user);
            $result01 = mysql_query($sql01);
            $sql02 = sprintf("SELECT * FROM users WHERE tbl_user = '%s'
AND password = '%s' AND  active = 'Y'", $user, $new_pass_enc);
            $result02 = mysql_query($sql02);

            if (mysql_num_rows($result02) > 0)
            {
                //require('log.class.php');
                //$log_fil = new log_file();
                //$log_fil->write_log($user, "Password Changed", "",
"Asset Management System");
                return 0;
            }
            else
            {
                return 1;
            }
        }
        else
        {
            return 2;
        }
    }

}
?>
```

security.class.php

```
<?php
class security
{
        function filter($content)
        {
$check_list = array(";", "GRANT", "Grant", "grant", "INSERT", "Insert", "insert",
"DELETE", "Delete", "delete","REVOKE", "Revoke", "revoke", "UPDATE", "Update",
"update", "=", "DROP", "Drop", "drop", "--", "UNION", "Union", "union", "OFFSET",
"Offset", "offset");
                $content = str_ireplace("'", "", $content);
                $content = str_ireplace($check_list, "", $content, $count);
                if ($count > 0)
                {
                        return '';
                }
                else
                {
                        return $content;
                }

        }

        functionfilter_for_mssql($content)
        {
$check_list = array(";", "GRANT", "Grant", "grant", "INSERT", "Insert", "insert",
"DELETE", "Delete", "delete","REVOKE", "Revoke", "revoke", "UPDATE", "Update",
"update", "=", "DROP", "Drop", "drop", "--", "UNION", "Union", "union", "OFFSET",
"Offset", "offset");
                $content = str_ireplace("'", "", $content);
                $content = str_ireplace($check_list, "", $content, $count);
                if ($count > 0)
                {
                        return 'Error';
                }
                else
                {
                        return $content;
                }

        }
        functionlite_filter($content)
        {
                $check_list = array("'", "--");
                $content = str_replace($check_list, "", $content);
                return $content;

        }}?>
```

log.class.php

```
<?php
classlog_file
{

        functionwrite_log($user, $desc, $refNo, $type)
        {
                //$log_date = date("Y-m-d");
                $log_date = date("Y-m-d") . " " . date("H:i:s");
                $log_user = $user;
                $log_desc = $desc;
                $refNo = $refNo;
                $log_type = $type; //process,
                $q_log = "INSERT INTO tbl_log (log_user, log_date, description,
refNo,type) VALUES('$log_user','$log_date','$log_desc','$refNo','$log_type')";
                mysql_query($q_log);
                if ($desc == 'Login')
                {
                        $this->write_to_user_log($user,2);
                }
        }
}
?>
```

The windows scrip file use to execute the Secure Token Generating Application

```
@echo off
call "C:\Program Files (x86)\Microsoft Visual Studio 10.0\VC\vcvarsall.bat" x86
cd C:\Users\Sahan.Walpitagamage\Documents\Visual Studio 2010\Projects\saferPay
msbuild saferPay.sln
echo build complete
```

PHPcode used run the scrip

```
exec("vc.bat");
```

payment_finsh.php

```
<?php
session_start();
require("database.php");
$match_code=0;
$status="";
$transaction_cid="";
if(isset($_POST['Verify']) && $_POST['Verify'] == "Verify")
{
          $match_code=0;
          $token_id=0;
          $app_code = $_POST['txt_token'];
          $password = $_POST['txt_password'];
          $username=$_SESSION['username'];
          $tr_number=$_SESSION['tr_number'];
          $bank_code="";
          $sql="SELECT* FROM tbl_user where username='$username'";
          $result = mysql_query($sql);
                              while($roow = mysql_fetch_array($result))
                              {
                                        $token_id = $roow['token_id'];
                              }

          $match_code=($token_id-1)*($tr_number-1);
          require('user.class.php');
          $user_cls = new user();
          $log_num = $user_cls->transaction_login($username,$password);//pass UN and
PW
          $user_id = $user_cls->user_id;

          if($match_code==$app_code&& $log_num=='0')
          {    $sql001="SELECT* FROM tbl_user_banks where user_id ='$user_id'";
               $result01 = mysql_query($sql001);
                              while($roow = mysql_fetch_array($result01))
                              {
                                        $bank_code = $roow['br_id'];
                              }
                    $today = date("Y-m-d H:i:s");
               $username= $_SESSION['username'];
```

```
        $m_code="M1";
        $amount=$_SESSION['amount'];
        $description="Payment for Goods";
        $status="Success";
        $temp_id= date('Ymd');
        $temp_id = "T".trim($temp_id);


        $sql01 = "SELECT MAX(transaction_id) AS maxn From
tbl_transaction_details WHERE transaction_id LIKE '$temp_id%'";
        //echo $sql01;
        $res01 = mysql_query($sql01);
        while ($row01 = mysql_fetch_array($res01))
        {
            if (is_null($row01['maxn']) || $row01['maxn'] == NULL ||
$row01['maxn'] == "")
            {
                $maxnum01 = "001";
                $maxnum01 = $temp_id.$maxnum01;
                $transaction_id = $maxnum01;
$sql002="INSERT INTO
tbl_transaction_details(transaction_id,user_id,amount,date_time,bank_id,m_id,descriptio
n,status)VALUES('$transaction_id','$user_id','$amount','$today','$bank_code','$m_code','
$description','$status')";
        mysql_query($sql002,$conn);
                    if (mysql_affected_rows($conn) > 0)
                    {
                        $status="Success";
                    }
            }
            else
            {
                $tempmax01 = $row01['maxn'];
                $tempmax01 = substr($tempmax01, -3);
                $tempmax01 = $tempmax01 + 1;
                //echo "<br>".$tempmax01."<br>";
                $transaction_id = $tempmax01;
                if ($tempmax01 <= 999)
                {
                    if ($tempmax01 < 10)
                    {
                        $tempmax01 = "00".$tempmax01;
                    }
                    else if ($tempmax01 < 100)
                    {
```

```
                                                        $tempmax01= "0".$tempmax01;
                                                }
                                                else if ($tempmax01 < 1000)
                                                {
                                                        $tempmax01 =$tempmax01;
                                                }
                                                $tempmax01 = $temp_id.$tempmax01;
                                                $transaction_id = $tempmax01;


                                                                $sql002="INSERT INTO
tbl_transaction_details(transaction_id,user_id,amount,date_time,bank_id,m_id,descriptio
n,status)VALUES('$transaction_id','$user_id','$amount','$today','$bank_code','$m_code','
$description','$status')";
                                                mysql_query($sql002,$conn);
                                                if (mysql_affected_rows($conn) > 0)
                                                {
                                                        $status="Success";
                                                        $sql03 = "SELECT MAX(transaction_id)
AS tmaxn From tbl_transaction_details";
                                $res03 = mysql_query($sql03);
                                                        while($roow3 = mysql_fetch_array($res03))
                                                                {
                                                                        $transaction_cid =
$roow3['tmaxn'];
                                                                }
                                                }



                                }   }
                        }
                }
                else
                {
                        $status="Fialed";
                }
}
?>
```

User Acceptance Test Questionnaire

Objective

To find out that the system meets the user requirements.

	Agreed	**Natural**	**Not Agreed**
This system has user friendly interface and can easily learn			
The system has quick response time			
The procedures were simple and required minimum number of steps			
The system can provide good security against the security threads towards on line electronic payment transfer			
Compare with existing electronic payment systems, I feel secure and comfortable when I am using the system			