



Sudan University for Science and Technology
Faculty of Graduate Studies

Development of Secure Internet Banking System Framework using Special Browser Interface

**تطوير إطار أمن للمعلومات البنكية عبر الانترنت باستخدام
واجهة متصفح خاص**

**Thesis submitted in partial fulfillment of the academic requirements for
the degree of M.Sc. in Computer Science**

By:
Abid Omer Ali Ahmed

Supervisor:
Dr.Abuagla Babiker Mohamed

March 2016

تعديل العنوان: [AOA1] Comment

Acknowledgements

In the name of Allah, the Beneficent, the Merciful.

قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ
الْحَكِيمُ

They said, "Exalted are You; we have no knowledge except what You have taught us.

Indeed, it is You who is the Knowing, the Wise."

Quran (Surat Al Baqarah) – verse 32

First and foremost, all praise is for Allah, Who enlightened us with faith and knowledge, and Who is sufficient for us and has sheltered us.

To my mother, thanks and may Allah bless you and give you health and long life.

To my father, thanks and may Allah bless your soul.

My supervisor, Dr. Abu agla, thanks for trust, time, and patience.

My family, brothers and sisters, you were special people, thanks for everything.

My friends: Gazi mohammed and Mazin Karar, thanks to you all for the support and help.

To The one that help Me a lot Mohammed elser May God grant him mercy and soul rest in eternal peace

May Allah grant you a bright future and everlasting success.

ABSTRACT

After the wide spread of computers, and its inclusion in all aspects, and the expansion of computer networks significantly, people became dependent on this network for processing their financial transactions, which differs from the traditional transactions in the method of the process and the media used; due to their ambiguity for the user and the increasing of the electronic hacking which led to the weakness of trust between the clients and the banks in processing this type of transactions. This research addresses the online banking services and some of its problems and the methods used to solve these problems the research presented a propose Framework to reduce this problems, using third party to provide authentication, encryption as a method for Confidentiality and hash functions to maintain data integrity using a secure web browser, that is to enable the users to practice their transactions in a secure way that prevent the access of any unauthorized party. The Framework provided the reliability threw secure browser interface which is represented in helping the client make sure that the page in front of him is the bank actual page, authentication, data integrity, the ease and flexibility for the access of the bank service and secure transactions. And to improve this effort, I recommend the use of a number of symmetric and asymmetric encryption algorithms; to provide more security and insurance, and developing the browser used in the research.

Comment [AOA2]: Change abstract

المستخلص

بعد الإنتشار الواسع للحاسب الآلي ودخوله في كل المجالات ، وإتساع رقعة الشبكة العنكبوتية بصورة كبيرة ، أصبح الناس يعتمدون على هذه الشبكة في إجراء معاملاتهم المالية والتي تختلف عن المعاملات التقليدية في طريقة إجراء المعاملة والوسط المستخدم؛ ونسبة لإنهما مجهولان للمستخدم وإزدیاد عمليات الإختراق الإلكتروني أدى ذلك إلى ضعف الثقة بين العملاء والمصارف في إجراء معاملات من هذا النوع.

يتناول هذا البحث الخدمات المصرفية عبر الإنترنت وبعض مشاكلها والطرق المستخدمة لحل هذه المشاكل. قدم البحث حلاً مقترحاً للحد من هذه المشاكل مستخدماً طرف ثالث لتوفير التحقق والتشفير كوسيلة لحفظ الخصوصية وكذلك دوال الهاش لحفظ تكاملية البيانات بإستخدام متصفح آمن وذلك لتمكين المستخدمين من ممارسة معاملاتهم بشكل آمن يمنع تدخل أي طرف آخر غير مصرح له. وفر الحل الموثوقية عن طريق واجهة متصفح سريه والتي تتمثل في مساعدة العميل من التأكد من أن الصفحة التي أمامه هي صفحة البنك الفعلية ، التحقق، تكاملية البيانات، السهولة والمرونة في الوصول للخدمة المصرفية بالإضافة لسريه هذه المعاملات.

ولتحسين هذا الجهد أوصي بإستخدام عدد من الخوازميات في نوعي التشفير المتماثل وغير المتماثل لتوفير المزيد من السرية والتأمين ، تطوير المتصفح المستخدم في المشروع.

Table of Contents

Acknowledgements	1
CHAPTER 1	9
INTRODUCTION	9
1.1 Background of the Problem	9
1.2 Problem Statement	10
1.3 Objectives of the Study	11
1.4 State of the Art:	11
1.5 Scope of the Study	11
1.6 Significance of the Study	12
1.7 Proposed Solutions	13
1.8 Structure of the Thesis	13
CHAPTER 2	14
LITERATURE REVIEW	14
2.1 Online Banking Processes	14
2.2 Architecture of Online Banking	15
2.3 Threat in Online Banking	16
2.4 Attack's in Online Banking	22
2.5 Possible Solutions	25
2.6 Related Works	29
2.7 Summary	31
CHAPTER 3	32
PROPOSED FRAMEWORK AND TECHNIQUES	32
3.1 Introduction	32
3.2 Authentication Procedure	32
3.4 Proposed Framework Assumptions	35
3.5 Techniques	35
3.5.1 Programming Techniques	35
3.5.2 Cryptography Techniques:	36
3.5.3 Integrity Techniques	36
3.5.4 Authentication Techniques	37

CHAPTER 4.....	38
SYSTEM PROCEDURE AND ANALYSIS	38
4.1 Introduction	38
4.2 System procedure	38
4.2.1 Running of the Authentication Application.....	38
4.2.2 Authentication between the User and the Bank.....	38
4.2.3 Transactions with the Bank	39
4.3 System Analysis	40
CHAPTER 5.....	54
RESULTS and DISCUSSION	54
5.1 Results	54
5.2 Proposed System evaluation and validation:	62
CHAPTER 6.....	65
CONCLUSION AND FUTURE WORK	65
6.1 Conclusion	65
6.2 Future work and Recommendations	65
Reference.....	67

List of Figures

Figure 1.1: Cost per transaction for each banking channel ^[2]	13
Figure 2.1: Online Banking Transaction ^[3]	14
Figure 2.2: Architecture of Online Banking Application	15
Figure 2.3: Threat can pervade every stage of the transaction ^[3]	17
Figure 2.4: PS/2 keyboard input transaction and the threat thereof. ^[3]	18
Figure 2.5: Counterfeit log-in Web page through HTML Injection. ^[3]	19
Figure 2.6: Secure SSL Session ^[3]	20
Figure 2.7: Internet Explorer's Security Alert ^[3]	21
Figure 2.8: SSL Man-in-the Middle attack ^[3]	22
Figure 2.9: Phishing attack via e-mail	23
Figure 2.10: Most-Targeted Industry Sectors – 1st Quarter 2013 ^[4]	23
Figure 2.11: DNS spoofing attack. ^[5]	24
Figure 2.12: Authentication Protocol using Mobile Phones ^[6]	28
Figure 2.13: Demonstrates the CAPTCHA system. ^[14]	30
Figure 2.14: Demonstrates QR system and install it into the mobile phone.	31
Figure 3.1: The Authentication Procedure between System Components.	32
Figure 3.2: The Connection Procedure between User and Bank Server.	34
Figure 4.1: Use Cases Diagram: User Application View	40
Figure 4.2: Use Cases Diagram: Client View	41
Figure 4.3: Use Cases Diagram: Third Party View.	42
Figure 4.4: Use Cases Diagram: Bank Application View.	43
Figure 4.5: System Use Cases Diagram	44
Figure 4.6: System Activity Diagram	45
Figure 4.7: System Class Package Diagram.	46
Figure 4.8: Sequence Diagram: Exchange Authentication Numbers	48
Figure 4.9: Sequence Diagram: Get Server IP Address.	49
Figure 4.10: Sequence Diagram: Get Bank Web Page	50
Figure 4.11: Sequence Diagram: User Login.	51
Figure 4.12: Sequence Diagram: Verification System Components.	52
Figure 4.13: Sequence Diagram: Bank Web Site Login	53
Figure 5.1: Login Form.	55
Figure 5.2: Main Form.	56

Figure 5.3: Options From	57
Figure 5.4: Log Form.	58
Figure 5.5: Bank Login Page.....	59
Figure 5.6: Bank Home Page.....	60
Figure 5.7: Show Balance Page.....	61
Figure 5.8: Transfer Page.	62
Figure 5.9: Wireshark Snapshot.	63
Figure 5.10: Bank Server Snapshot.	64

Abbreviations

<i>Abbreviation</i>	<i>Meaning</i>
AES	Advanced Encryption Standard
APWG	Anti-Phishing Working Group
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
DNS	Domain Name System
DSN	Device Serial Number
ECIS	Extended CAPTCHA Input System
FTP	File Transfer Protocol
JAR	Java Archive
JDBC	Java Database Connectivity
MITB	Man in The Browser
MITM	Man In The Middle
ODBC	Open Database Connectivity
OTP	One Time Password
PKI	Public Key Infrastructure
RSA	Rivets, Shamir and Adelman
RT-MITM	Real Time Man-In-The-Middle
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UML	Unified Modeling Language
USB	Universal Serial Bus

CHAPTER 1

INTRODUCTION

This chapter introduces the current research with background problem after that statement of the problem, objectives of the study, scope of the study, significance of the study and structure of the thesis.

1.1 Background of the Problem

Web become the most used way for an increasing most of business and other sensitive transactions for online banking. Almost all browsers and servers deploy SSL/TLS protocols to address concerns about security although , the usage of SSL/TLS by browsers still allows Web spoofing, that is, misleading users by impersonation or misrepresentation of identity or of credentials^[1].

There are different types of risks associated with online banking. Security for user credentials has become much more important than anything. Indeed, there is an alarming increase in the amount of real-life Web-spoofing attacks, usually using simple techniques. Often, the attackers fraudulently redirect the user to spoofed Web site by sending her spoofed^[5]E-mail messages that link to the spoofed Web sites; this is often called phishing attack. The goal of the attacker is often to obtain user-IDs, passwords/PINs, and other personal and financial information. Some of the risks associated with online banking are as following:

- Web Spoofing and Phishing Attacks.
- DNS Cache Poisoning (Pharming).
- Malware: Trojan-horses, backdoors, root-kits, key-loggers.
- Credential stealing attacks.

There are different authentication methods used for online banking security involve different authentication factors like password, PIN, pass phrase. Most banks conduct two-factor authentication one of which being based on the knowledge of some data (i.e. something the user knows). The actual implementations may vary, still username-password combination, pass phrases or PIN numbers are the most commonly applied^[1]In

order to increase security, most banks employ a second authentication factor – a token that user possesses. The implementations of the authentication factor can be classified as follows^[1]:

- One-time password approach: Tokens in form of one-time passwords are very popular in Scandinavian countries. Main advantage of one-time passwords is the fact, that they can be used only once and become invalid afterwards.
- Certificate based approach: Certificates are software tokens that require (public key infrastructure). In the case of certificate based approach a certificate is used as the second authentication factor. They can be stored either on the hard drive or another storage device e.g. USB stick, smart card. Usually banks employ the combination of a certificate together with username-password, pass phrase or PIN number.
- Timer based (short) password approach: Timer based one-time-password is generated using hardware generators (e.g. Secure-ID). Additionally, a PIN or password is used together with one-time-password. Once the password is generated, it is valid only for some specific time interval. This approach is not only used by banks, but also employed by providers of other services like PayPal or eBay.
- Certificate - smart card based approach: In online-banking smart cards can be used to store certificates or as devices for generating one-time-passwords. When using smart cards, card reader is essential. Most of solution depend on PKI (Public-key infrastructure)

1.2 Problem Statement

Security is the most important and main issue in online banking .Trust can be developed through secure transition between bank and the customer's online banking. Proper identification of the authorized user is lagging in current mechanism. On the other hand customer wants to make sure that the page they are accessing is an actual bank page not fake page.

On the other hand the problem statement can be stated in the following Research question:

“How to provide secured online banking transaction between bank and customers without depend on PKI?”

1.3 Objectives of the Study

The main goal of this study is to develop a secured online banking system which satisfies most of the important security requirements while achieving the concept of ease of use. The detailed objectives are:

- Design new protocol to grantee keys exchange between client and banks servers threw Third Party.
- Develop special browser software interface to provide more secure transactions.
- Create encrypted channel between client (browser Interface) and Bank server to control security and integrity of data.
- Integrity: the system can detect any modification in data throw transmutation .
- Create a banking system that is easily accessible by customers from the comfort of their homes, offices etc.

1.4 State of the Art:

The E-Banking Field has many researches and different solutions to keep pace with the rapid development of technology. Some of it requires hardware devices like mobiles and tokens and the others only on user's credentials.

The PKI solution considered the base of the most online banking transactions.

1.5 Scope of the Study

The focus of this Study is to achieve the confidentiality of information and integrity online banking transactions to ensure its accuracy and protect them from any

modification without using PKI solution, so the solution rely on encryption to achieve those objectives and focus on securing client third-party connection and then connected to the bank because he is the weakest in security connection between bank and third-party always secured.

1.6 Significance of the Study

Many incentives make online banking an essential service for banks and customers. Here follows a list of incentives that banks would consider when deciding to offer online banking services:

- I. Accuracy: humans directly affect the reliability of transactions, especially when the transactions occur in a face-to-face manner. There is always a possibility of errors originating from either the employees or customers.
- II. Service: the Web offers equal opportunities to all competitors. Banks do not have to worry about approaching customers in different geographical areas but rather have only to concentrate on providing a central web presence approachable from everywhere. This gives the bank focused management as well as zero-delay service quality to offer to customers.
- III. Profit: is among the most attractive incentives for any commercial organization. For banks, online banking has emerged as one of the most profitable products over the past decade^[1]. This is likely a direct result of cost reduction in labor, building construction and maintenance, and service and transaction provision. For example, Figure 1.1 shows that online banking has a transaction cost of almost 1 cent compared to \$1.07 for transaction carried out on-site^[2].



Figure 1.1: Cost per transaction for each banking channel^[2].

- IV. Transaction speed: customers are sometimes involved in long queues in bank branches to request transactions. Online banking has eliminated the need for the delay and customers are able to process their transactions as soon as they click on the confirmation button.

In the developing countries like our country, the people need online banking service but the main problem is that PKI could not be founded for many reasons related to economy and political policies, so we need to develop alternative solution to gain this service securely. The new solution should consider the restriction of PKI in most of developing countries.

1.7 Proposed Solutions

The Proposed solution is to create simple protocol based on PKI theory that used third party to manage communication between clients and banks. The third party guarantees secure line to delivers keys to clients and banks to open secure channel that use to make transactions.

1.8 Structure of the Thesis

The research report was organized into five chapters: Chapter one focuses on the Background Problem, problem statement, objectives and justification of the study. In chapter two, a range of literatures review were captured there to gather relevant information concerning online banking security. In chapter three, detail of methodology followed to achieve results was outlined. It includes the study design, sampling, sampling technique and analysis. Chapter four contained results and discussion from the study supported with findings from other research works. Chapter five focuses on main findings and results .Chapter six contained future work and conclusions of the study

CHAPTER 2

LITERATURE REVIEW

This chapter describes the preliminary concepts and presents current approaches for secure online banking. The chapter begins with the definition and some background of online banking, Online Banking Processes and classification of online banking Threats and attacks, finally presents the related works of online banking security solution.

2.1 Online Banking Processes

Online banking is a series of processes in which a bank client logs on to the Website of the bank through the Web-browser installed on the PC and carries out various transactions such as account transfers^[3]. Online banking is carried out in four major stages illustrated below in Figure 2.1.

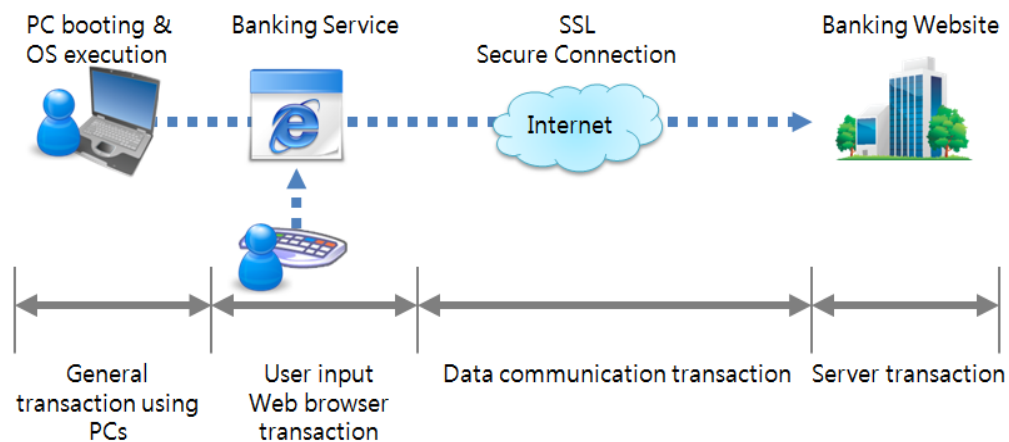


Figure 2.1: Online Banking Transaction^[3]

In the upper figure [2.1] first user turns on the PC and boots the OS, then open the web browser and access bank's Website and enters the ID or Personal Identifying Number (PIN) and the password by using the keyboard.

After that the data input is encrypted by SSL (Secure Socket Layer) and transmitted to the bank's server, from the other side the bank's server decrypts the

transmitted information and processes the user's authentication, account inquiry, account transfer, etc.

2.2 Architecture of Online Banking

The Online Banking Application is based on 3-tiered model the most popular in Online banking environment. The Enterprise architecture for Online Banking Application is shown below

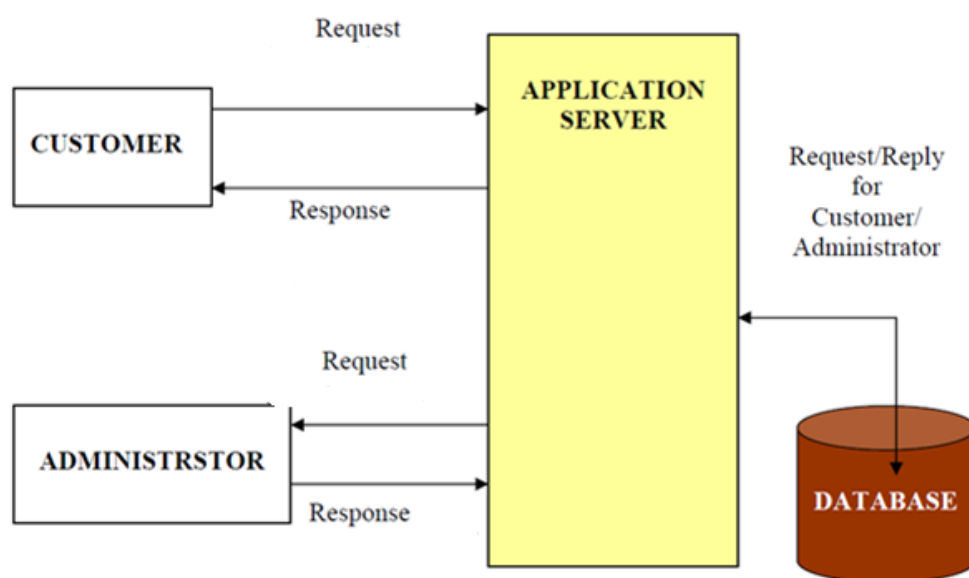


Figure 2.2: Architecture of Online Banking Application

The 3-tiered architecture shown above has the following major components:

Client: There will be two clients for the application. One will be a web-based user-friendly client called bank customers. The other will be for administration purposes.

Application Server: It takes care of the server script, takes care of JDBC-ODBC driver, and checks for the ODBC connectivity for mapping to the database in order to fulfill client and administrator's request.

Database: Database Servers will store customer's and bank data. Simply stated, the application works based on a request/response protocol. A client initiates a request to the server. The server responds by executing the business logic hosted inside the JSP

program and if required, communicates with the Database Server to fulfill a client's request.

2.3 Threat in Online Banking

The PC environment is exposed to many types of threats because of unsafe web surfing and installation and/or use of a variety of unverified programs. If a user carries out an online banking transaction in an environment exposed to various threats, there is no way to guarantee safety for that online banking transaction.

Most of the recent hacking tools are circulated throughout the Web, and they are downloaded and executed in the user's PC while the user is simply Web surfing or opening an e-mail^[3]. These hacking tools can easily capture the password, account number, and personal data which the user is inputting. Not only that! They are even capable of replacing the input screen that the user is watching with a counterfeit Website of the bank which the hacker had installed in advance. The user's input data are not transmitted to the bank because these hacking tools redirect the user's input data to the hacker's server instead for illegal account transfers. Thus hackers and hacking tools can attack us using many tricks in a number of different ways during the online banking process as shown in Figure 2.3^[3]

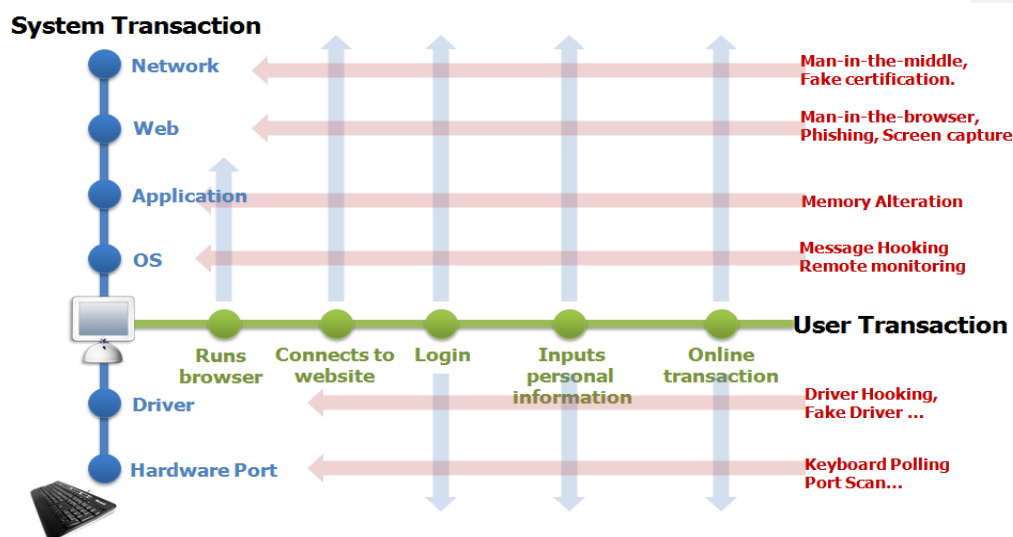


Figure 2.3: Threat can pervade every stage of the transaction^[3]

Threat to Using PCs

End users enjoy all sorts of games, Web surfing, and E-mail using their PCs, but many potential threats exist in the use of the ordinary PC and the Internet. Although Anti-virus and Anti-Malware programs are installed in the PC to protect against these threats, these programs are unable to counter the exponentially increasing new breed of malicious code shown in Figure 3 because the Anti-Malware technology is signature base which only detects known threats. For example, the hacking tool for online banking called, Zeus, contains a technology that detects and avoids the Anti- Malware software, and is constantly spreading new breeds or variants of Zeus mostly through famous Web sites, fake Web sites, phishing sites, e-mail, etc. In short, having no proper protective measures as in the examples above, a considerable number of PCs may be using the Internet banking even now, completely unaware that they are infected with a variety of hacking tools or malicious codes.

Threat to Personal Data Input

An end user accesses the online banking service through the web browser and inputs a value for personal identity authentication such as ID, PIN, and password. When the user presses the keyboard, the input signals are transmitted through the port connected to the keyboard, a number of other devices, and the keyboard driver to reach the program. In other words, the process of logging on to the online banking web site involves inputting personal data through the keyboard strokes, showing the input information on the screen, and transmitting the data by clicking the “log in” or “submit” button. Figure 2.4 illustrates possible attacks that the hacking tools can make during this process.

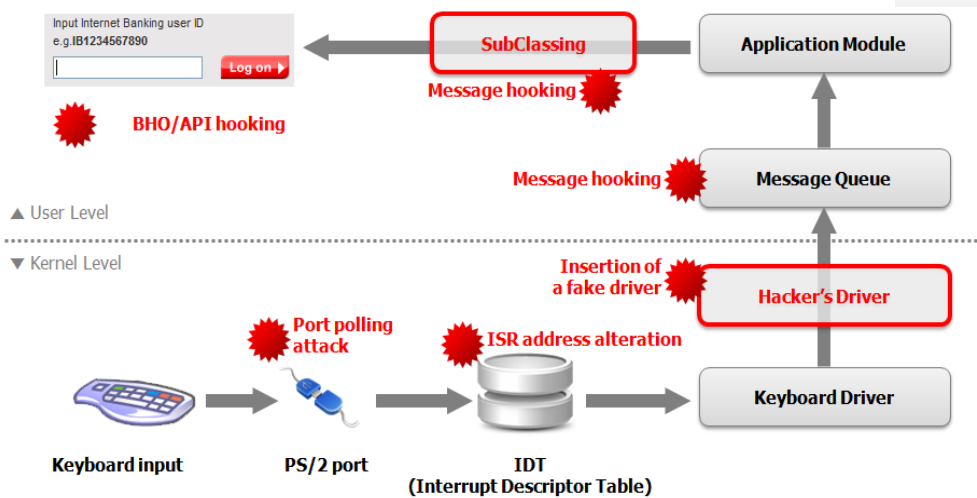


Figure 2.4: PS/2 keyboard input transaction and the threat thereof.^[3]

The key logging hacking technique that had previously been confined to the user's level has expanded to every stage of the entire process including the kernel level since 2006. Of late, polling and hooking methods are frequently used in attacks on the port level. Figure 4 shows the diagram of a PS/2 type of keyboard, but even the USB keyboard or Bluetooth keyboard are vulnerable to these types of attacks. The account information stolen from every stage of the entire online banking process is transmitted to the hacker's server through FTP along with the screen image that has also been captured. This is the main attack vector that is threatening the safety of Internet banking.

Threat to Web Browser (MITB: Man-in-the- Browser)

Man-in-the-Browser Attacks redirect the end user to counterfeit sites with the intention of stealing the end user credentials. Most banks offer One-Time Password (OTP) to protect the static password that the end user inputs on the keyboard. This is a technology that disables the attack by having the user input a new password generated by the OTP device every time the user logs in so that the hacker cannot use the password captured by using the key logging hacking tool. However, the hacker can incapacitate the OTP function with a simple attack. With the hacking tool that has been installed in the user's PC in advance, the hacker can show a fake online banking web site he made by modifying the user's hosts file

[3], or he can also intercept the user's online banking session and steal user credentials by covering the user's web site through HTML Injection with a counterfeit site to be filled with account information, the next figure 2.4 shows example of web fake html login page.

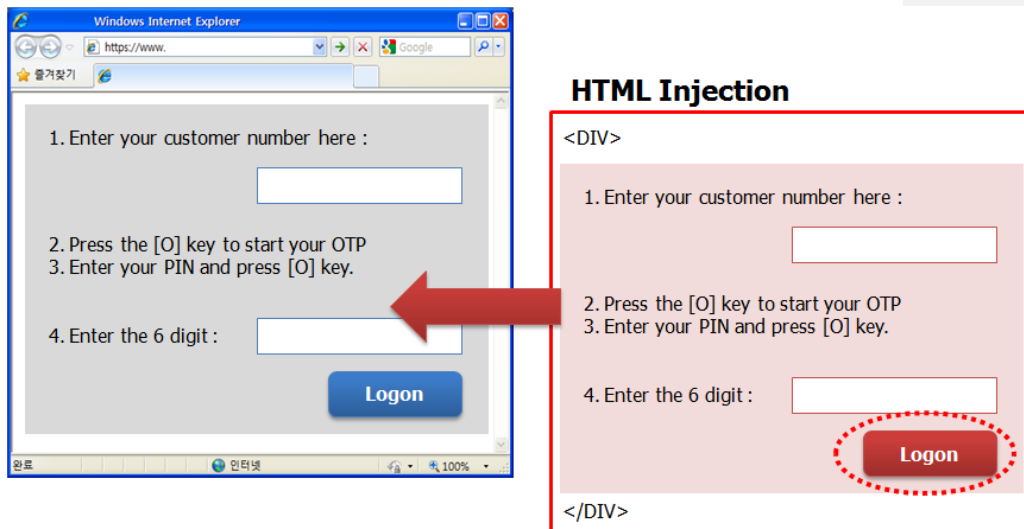


Figure 2.5: Counterfeit log-in Web page through HTML Injection. [3]

In the end, the user inputs account or financial transaction information on the counterfeit web page, and the information thus inputted is transferred to the account - both counterfeit web page and account is arbitrarily made by the hacker - and then is transmitted to the bank web site. When the illegal account transfer is completed as intended by the hacker, the hacker even shows the page describing the normally completed result to the user. Thus the user is unable to even perceive that his internet banking has been tampered with Man-in-the-Browser Attacks come in many flavors, and the hacking may even be targeted at the customers of a specific bank. Man-in-the-Browser Attacks can hold a session with the bank by using the account and password information including OTP that are stolen from the user's PC, and they can show a screen page with an error message and induce the user to input the latest OTP and then complete their illegal transfers. These multi-faceted online banking Trojans can inflict great amounts of financial losses that are big enough to drive the targeted enterprises into bankruptcy.

Threat to SSL Communications (SSL Man-in-the Middle)

With the latest advances in wireless internet, it is now possible to use the Internet in coffee shops or shopping malls through Wi-Fi Hotspot, and online banking or online shopping can be done through these hotspot networks. Of course, almost all the online banking web sites use SSL (128 bit or higher) encrypted communications for the security of the web browser, and they are known to be safe against the Man-in-the-middle (MITM) attacks by sniffing. However, it is difficult to say that SSL communication can guarantee safety in the wireless Internet (Wi-Fi) environment. The next figure 2.6 shows example of MITM attack.

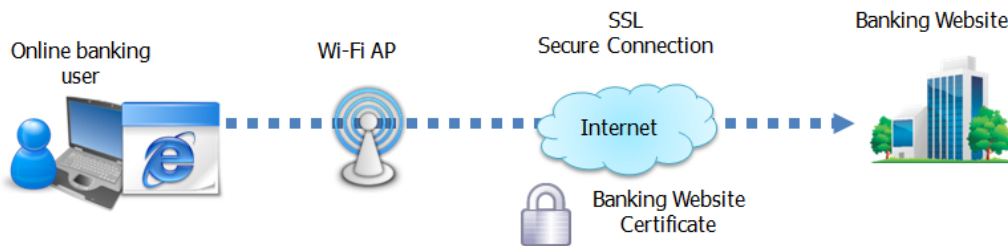


Figure 2.6: Secure SSL Session^[3]

The form of an SSL MITM attack through Wi-Fi can proceed with the following scenario.

- a. An end user starts online banking through Wi-Fi.
- b. A hacker connects to the same Wi-Fi network and starts SSL MITM attack through ARP spoofing and DNS spoofing as we shows in figure 2.8.
- c. The hacker offers a fake online banking web site and a fake certificate to the user.
- d. The web-browser goes on connecting to a session with no questions asked if the certificate is safe & doesn't fabricate, but if not; the warning message in Figure 2.7 is given. However, because most users do not have the expert knowledge about this kind of hacking, they will select "yes" by habit without thinking. In other words, the criminals socially engineer the users to accept an abnormal certificate which is secretly created.



Figure 2.7: Internet Explorer's Security Alert³¹

- e. Although SSL communication is being protected by 128 bit encryption, the attacker intercepts the SSL packet with a packet sniffing tool, such as Ethereal.
- f. The hacker uses a fake certificate and SSL Dump tool to decode the stolen coded packet and reveals the user's account and financial information.
- g. The hacker now logs on to the valid online banking website and completes the illegal account transfer.

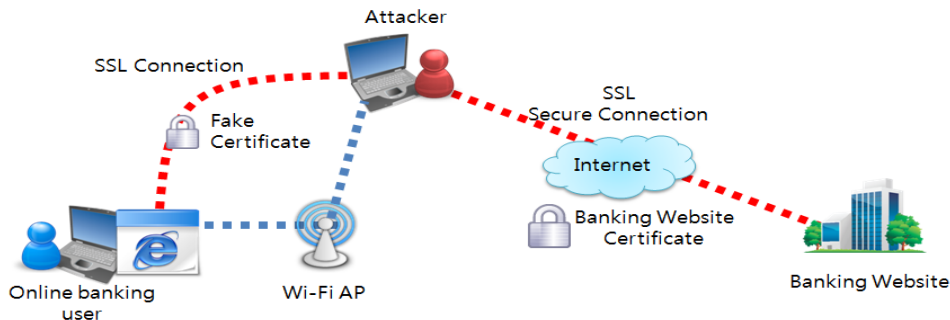


Figure 2.8: SSL Man-in-the Middle attack^[3]

2.4 Attack's in Online Banking

Social engineering attacks usually aim at stealing authentication factors by fooling the access credential holders. This type of attacks takes two forms: technical and nontechnical.

The credential holders may be the customers who are the account holders or even the support help desk people. Non-technical social engineering attacks aim at deceiving users by means of convincing and trust building. For example, an attacker introduces himself/herself to the user as a banker or a technician and requests the user's credentials for help and support purposes.

Another attacker calls the help Centre, impersonates a legitimate user, and requests a password reset to the account. This kind of conversation takes place through a call or email most of the time, as it is very hard or dangerous for the attacker to impersonate someone else and deceives a user or a help desk face-to-face. Who have administrative privileges to access and reset customer credentials.

Technical social engineering, on the other hand, involves other types of attacks such as phishing (see Figure 2.9) and pharming. These require the attacker to have technical or web development skills, usually to masquerade the OSP's web presence to capture users' access credentials.

- **Phishing**

Phishing is an example of technical, social engineering where the attacker designs and hosts a fake page or website, which has the same look and feel of a legitimate website.

Then the attacker invites people to submit log-in credentials using e-mails or instant messaging (IM) that claim to be from a legitimate source but contain links to the fake spoofed page or website^[16]. Figure 2.9 displays an example phishing e-mail message which introduces itself as if it comes from a legitimate HSBC source and asking the client to identify him/herself to the bank website using a misleading web link. That link displays a real valid link to hsbc.co.uk but the source (which is usually hidden) directs the client to a fake website hosted by another domain name.

Comment [AOA3]:



Figure 2.9: Phishing attack via e-mail

According to an Anti-Phishing Working Group (APWG), financial and payment services are the industry sectors most targeted by phishing attacks with almost 70% of

total attacks in the 1th quarter of the year 2013^[4] as shows in figure 2.10

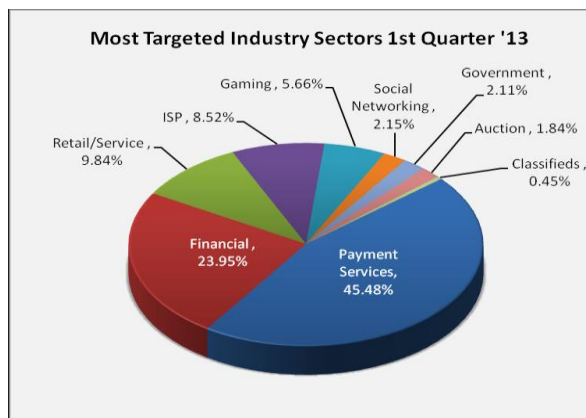


Figure 2.10: Most-Targeted Industry Sectors – 1st Quarter 2013^[4].

- Pharming

Pharming is yet another social engineering attack that targets end-users. Pharming and phishing implement the same techniques to capture end-users' access credentials [5].

However, they use different strategies to complete this task. Unlike phishing, pharming attacks first compromise the user's machine to alter the host's file before the user is deceived and taken to a fake website. The host's file is a file residing in personal computers and used to speed up domain name resolution [5]. When a user tries to access a domain name, if that domain name is not defined in the host's file, the machine will try to contact a domain name server (DNS) to resolve the IP address associated with the domain name. If it is defined in the local machine host's file, then there is no need to contact a DNS server.

This is more sophisticated than phishing techniques as it involves the altering of a file in the user's machine. It has a better impact than phishing as users will probably not notice that they are visiting a counterfeit website; the user is not required to click on a misleading link received by e-mail or found in a website because, whenever the user tries to access the actual website using its domain, the local hosts file will redirect the user to the fake website automatically.

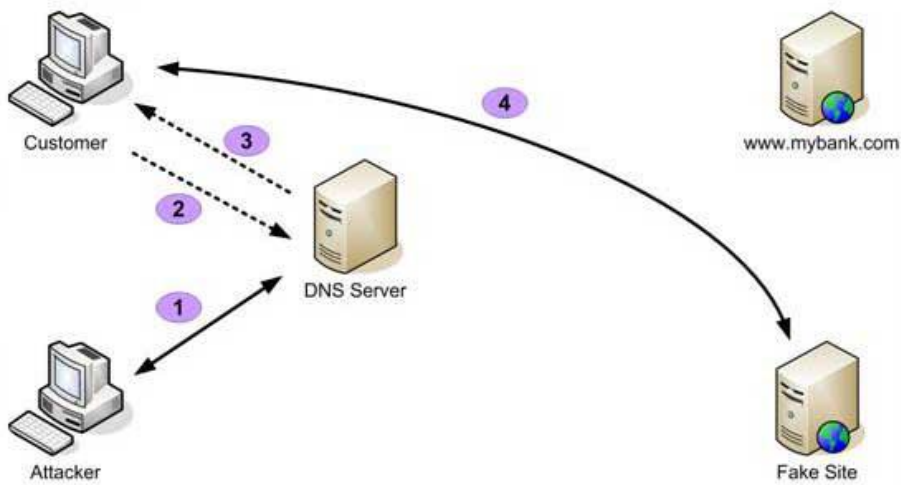


Figure 2.11: DNS spoofing attack. [5]

More sophisticated and dangerous pharming techniques exist at network or communication channel (CC) levels. This happens when DNS tables of routers and

servers are attacked and altered so they will redirect DNS resolution requests on a mass scale. This is known as DNS spoofing and is illustrated as showed in figure 2.11.

In figure 2.11, the attacker first attacks a DNS server and alters or adds an entry for www.mybank.com website so it will point to the different IP address of the attacker's fake website. Any customer requests for DNS resolution of www.mybank.com from the attacked DNS server will be redirected to the fake website rather than to the actual www.mybank.com site.

- **Click jacking:**

Click jacking, also known as user-interface (UI) redressing, is an attack technique based on

HTML codes being used to hide a layer on top of the displayed contents to perform unexpected actions after the user clicks on it. This exploit was officially released to the public in 2008 but it has existed for many years. It can be used in different ways. For example, an attacker can send an e-mail to a victim with an embedded video clip. The video clip has a play button, which, if clicked, installs malicious software into the user's machine (i.e., malware infection attack). This is achieved by placing an invisible layer on top of that button to run such an unexpected action.

A click jacking attack has the ability to allow an attacker to completely control the victim's desktop; thus, it hijacks the victim's active sessions or captures the authentication factors exchanged with other sites.

2.5 Possible Solutions

The potential value to an attacker of hacking Internet banking applications means that they may go to extraordinary lengths in order to do so. Most of the banking applications are using simple passwords as the primary form of authentication. The following are possible solutions:

1. **Digital Certificate Based Approach:**

Digital certificates are electronic files that act like a kind of online passport. They are issued by a trusted third party (i.e. VeriSign), a certificate authority (CA), which verifies the identity of the certificate's holder. They are tamper-proof and cannot be forged. Digital certificates do two things: Authenticate that their holders - people, web sites, and even network resources such as routers - are truly who or what they claim to be. Protect data exchanged online from theft or tampering, but there are many issues related to digital certificates mainly depend on PKI which can't be available in all countries, Also Certificate Renewing, Revocation and Private Key may Compromise.

2. One-Time Passwords

In one-time password systems, the password entered is only valid for a single login, and then changes in a secure way. The benefit of such a system is that monitoring by an attacker is useless, as the information available to them cannot be reused. However the disadvantages of this scheme are that administration is complex, and the user has to store a list of keys on a sheet of paper, creating the potential for theft and misuse. For these reasons, it is unlikely that a bank would adopt such a scheme, or that the public would accept it, even if it were implemented.

This approach is very costly and not easy to use for all users

Token based systems provide authentication of a user by requiring them to demonstrate the possession of a physical object or token which is unique to that user.

There are basically three types of tokens. Memory tokens - These tokens do not contain any processing capacity, but contain authentication data stored in magnetic, electronic or optical form. Second one is Microprocessor tokens - These tokens contain a microprocessor in addition to memory. Such tokens may implement cryptographic algorithms for encryption on the card. Microprocessor tokens are commonly referred to as smart cards. Many smart cards have properties that make them resistant to tampering.

Third one is Hand held password generators - This class of items includes both hardware calculators for the one-time password mechanisms as described above, and challenge response calculators that allow a user to enter a challenge from the server and calculate the appropriate response. Unfortunately, all these schemes require the purchase of extra hardware, making them unattractive to both banks and their customers.

Again This approach is depend on PKI which is not be available in all countries, the Token can susceptible to loss, damage ,stolen and reused.

3. Authentication Using Mobile Phones

The idea of using mobile devices in the verification process as a third party is far from cyberspace scenario^[6], it can be describe as follows: The customer open bank's website, and then enter his username and password, then the system will send a special code to the customer mobile number, which is registered in the bank database, through SMS, bank system should make sure the SMS arrived to the customer, and then customer enters the code and thus now client and the Bank can perform banking transactions. There is a few point should be considered here:

- i. Depend on external third party: this dependency may cause many problems like availability of service.
- ii. Attacker's exposure to Mobile messages.

The Systems based on SMS text messaging so sending the password will use instant communications networks like GSM mobile phones which recently came under attack and the attackers managed to capture all SMS text messages and decrypt them^[15].

Mobile phone networks use several encryption algorithms to achieve security, such as encryption algorithms A5 / 1 and A5 / 2 used to ensure confidentiality of the sound waves transmitted over the air has been announced for a number of attacks targeting these algorithms. Some algorithms require a long period of preparatory treatment after the attack

Comment [AOA4]:

can encrypt and humorous in just a few seconds. There are at least four commercial tools allow decrypts Telecom mobile networks. These tools price ranges between \$ 100,000 and \$ 250,000 depending on the speed at which you want to work with the program.

In the below figure 2.12 approach enhances performance and robustness against various attacks by using mobile phones to store digital certificate for clients and assume that client's mobile phone has TPM embedded and connected with a personal computer via a USB cable or Bluetooth^[6]

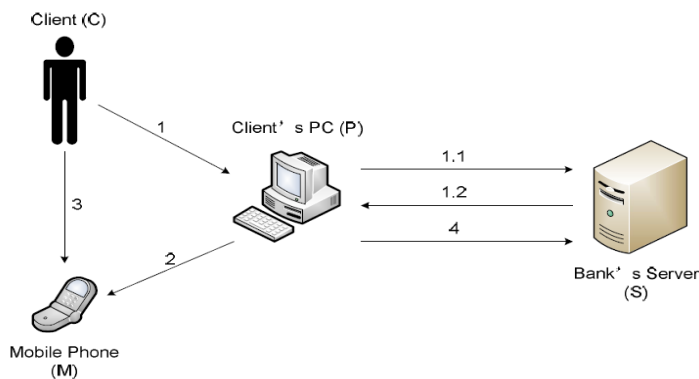


Figure 2.12: Authentication Protocol using Mobile Phones^[6]

1-A client starts a HTTPS connection with the bank by visiting the bank's login web page. The detail of HTTPS connection is described as follows:

- a. P says 'Hello' to S: As the beginning step, cipher configuration that documents the available cipher algorithms on P as well as a random generated number RC are sent to S.
 - b. S says 'Hello' to P: S reviews the configuration and sends back its cipher choices together with the bank's certificate, a RS, and a client digital certificate request.
2. Based upon a successful verification of bank's certificate, M displays a message prompting C to input the PIN, which is used to prove the current holder of M is the real C.
3. C types the PIN using M's keyboard.

4. C's certificate combined with PKC, a C's signature, and a pre-master piece, which is encrypted by PKB, are sent to S after the right PIN is provided. C's signature is in the pattern: $\{H(RC, RS)\} PVC$.

5. S first verifies C's certificate, then validates its signature through decrypting it using PKC and comparing the hash result. At last, S calculates a symmetric key, SK, for further usage. The SK is generated based on the knowledge of RC, RS, and the pre-master piece.

6. P generates a same SK and the further communication between P and S will be encrypted by SK. At this point, authentication process is successfully finished.

2.6 Related Works

In study by Han, Jae-Suk Lee and others researchers used the two-channel authentication method to serve online banking environment, The research assumes the existence of a software that should be installed on a mobile phone, Which receives a user name and personal identification number from the user and then extracts the password that you used once without the need to store the user name and personal definition number, as well as This suggested solution features by low of cost, usability and the lack of the place constrained. And then after comparing it with other methods still in use, the staff recommended by adopting it as the best way among the current available solutions.

In other study^[14] researchers used CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart") as shows in figure 2.13 which is simply enable the program watch any response comes from the customer is not from any computer program this is a human being.



Figure 2.13: Demonstrates the CAPTCHA system.^[14]

Chun-Ming Leung undertakes a study^[14] to reduce the Phishing by developing a model of CAPTCHA known by Extended CAPTCHA Input System (ECIS) with OTP. This system is mainly to resist Real Time Man-In-The-Middle Attack (RT-MITM) by integrating (ECIS) system with OTP system (the system of passwords entry) and determine a certain time constraints on it. The study was being able to reduce the attack of passes client information (auto-relaying of information).

In their proposed solution^[14] they provides software system that does not need to install, which it helps dramatically in publishing this software according to its cost against comparing it within these current available solutions. The system reuses the devices passwords (OTP) Instead of redesigning it as long, which is causes the Cost increases; the proposed solution provides a special browser integrated with the system.

Also there's a study had been done by each of Xing Fang and Justin Zhan^[6] for using the mobile phone in banking authentication operations over the internet.

This research based on To store digital certificate sin the customer's mobile phone which helps in improving the efficiency of the banking Authentication system over the internet.

The research realized that, using the mobile phone in authentication process presents spare feature in reducing the cost which that too expensive among the other systems used The (OTP) Devices.

Which is a new generation of ((2D Barcode) Quick Response) in 2008 (shows in figure 2.14) the QR code Used for Online Banking Authentication. A special encoding to convert data into symbols lines and boxes in such length and width, and there are three squares on its corners as coding determinants which make the data reachable.



Figure 2.14: Demonstrates QR system and install it into the mobile phone.

Both of Young Sil Lee and others have done a research which that study uses Mobile-OTP devices within (QR-code). The users enter their usernames and passwords and send it to the Bank then the Bank responses by the own customer QR symbol , then the customer uses his own mobile device to read it and extract the password , and write this code on the site and therefore we achieved the binary authentication concept over the contact ends .

The research realized that, the proposed system provides the necessary authentication to conduct the secure banking operations.

2.7 Summary

From the previous studies we noticed that the online banking world has many and different types of sophisticated problems and attacks, some of them based on technology and the other on the user himself.

The possible solutions have some vulnerabilities based on the environment that the solution applied on, e.g we can't use the mobile authentication solution with users never use Mobile phones and so on.

CHAPTER 3

PROPOSED FRAMEWORK AND TECHNIQUES

3.1 Introduction

This chapter shows the proposed solution from technical view, the relation between components and the technologies used in solution.

The Propose framework used third party to provide secure channel between the user and the bank over internet; this third party provide the needed authentication and privacy for sensitive data aiming to secure this transaction from Attackers.

3.2 Authentication Procedure

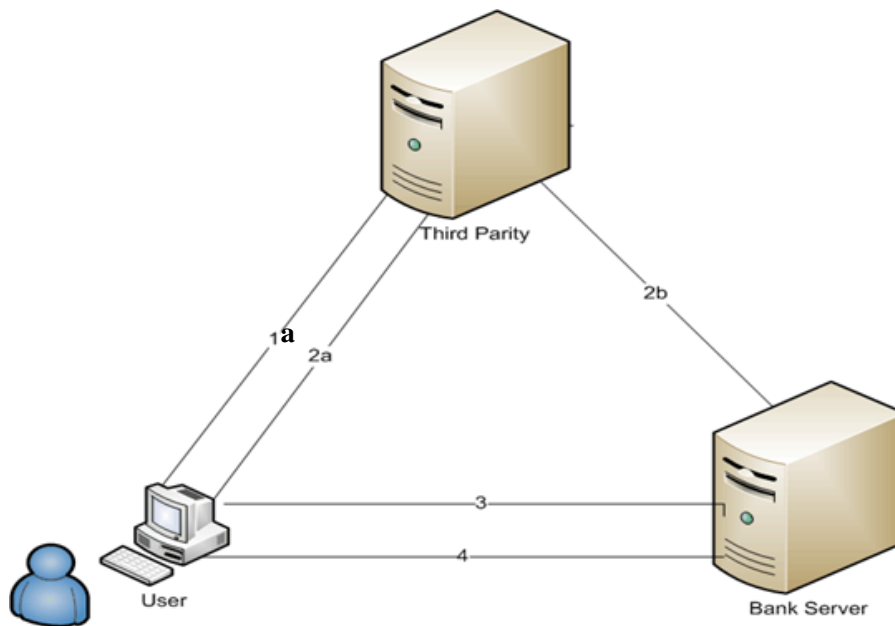


Figure3.1: The Authentication Procedure between System Components.

As can be seen from the above figure

Step 1: The Client application establishment connection to third party in this step and user select the bank. The client application send encrypted request to the third party using third party public key, the request contains:

- Bank Identification.
- Device Serial Number.
- Public Key Client to Third Parity.
- Pair Authentication Numbers N1 and N2.

Then The Third party reserve Encrypted request and Decrepit it using your privet key.

Step 2: In this step the third party send encrypt request to client application using client's application public key. This request contains:

- Bank IP address and Port Number.
- Bank Public Key.
- Result of Multiplied $N1 * \text{Constant value}$.
- Time stamp T1.
- Different Pair Authentication Numbers using for authentication between bank and client.
- Hash value for all request content using to integrity of data.

After that the third party send encrypt request to bank application using bank application public key. This request contains:

- Client Public Key.
- Device Serial Number (DSN).
- Time stamp T1.
- Pair Authentication Numbers using for authentication between bank and client.

Step 3: In this step the client applications after received request from third party decrypt the request using the privet key and recalculate hash value and matching with received hash value to insure data integrity. Then client send a request to bank contains one encrypted pair authentication numbers using bank public key and device serial number (DSN).

Step 4: In this step bank receive client request and decrypt it using your private key. After that send Encrypt request using client public key this request content:

- Second Authentication Numbers.
- Key session used to Encrypt requests between client and bank server.
- Time stamp T2.
- Hash value for all request content used to integrity of data this hash value signed by bank private key.

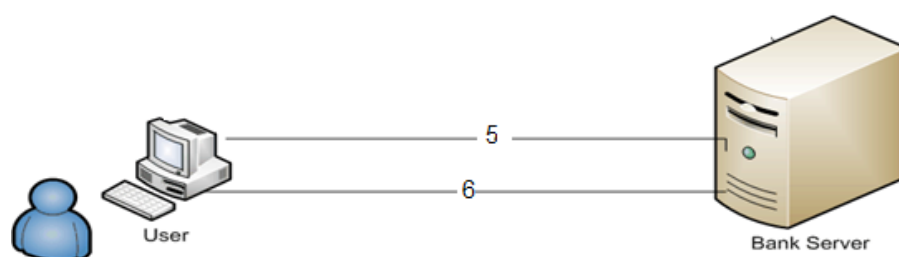


Figure 3.2: The Connection Procedure between User and Bank Server.

Step 5: In this step after client decrypt previous request and get the session key. Client send another request to bank encrypt using session key. This request content:

- Real Request between client and bank.
- Device Serial Number (DSN) and counter this counter auto increment for any request from this DSN to avoid Replay Attack.
- Hash value for all request content used to integrity of data.

Step 6: In this step bank send a response to the client request and hash value for this response encrypted using session key between bank and client.

1. $C \rightarrow TP: E_{K_{UTP}}[ID_B || DSN || KU_{CTP} || KU_C || N]$.

2.

2a- $TP \rightarrow C: E_{K_{UC}} [[IP_B + Port || KU_B || T_1 || N * const || N_1 || N_2 || H[IP_B + Port || KU_B || T_1 || N * const || DSN || N_1 || N_2]]$.

2b- $TP \rightarrow B: E_{K_{UB}} [KU_C || DSN || T_1 || N_1 || N_2]$.

3. $C \rightarrow B: KU_B [N_1 || DSN]$.

4. $B \rightarrow C: KU_C[[N_2||Ks// T_2] || E_{KR_B}[H[Ks// T_2]]]$
5. $C \rightarrow B: Ks [[Request || DSN+counter] || H[Request || DSN+counter]]$
6. $B \rightarrow C: Ks [[Reponses] || H [Reponses]]$

ID_B : Bank Identification

N_1, N_2 : Pair Authentication Numbers.

KU_{CTP} : Public Key Client to Third Parity.

DSN : Device Serial Number.

IP_B+Port : Bank IP Address and Port Number.

KU_C : Client Public Key.

KU_B : Bank Public Key.

KR_B : Bank Privet Key

KR_C : Client Privet Key.

Ks : Session Key.

T_1, T_2 : Time stamp.

3.4 Proposed Framework Assumptions

- 1- The third party in the proposed Framework must be a central bank in the country.
And have secure connection to all banks
- 2- The user Devise not secure.
- 3- The propose framework Consider the Confidentiality of Data transmission higher than performance of the network because high sensitivity of the information exchanged in banking transactions

3.5 Techniques

3.5.1 Programming Techniques

Java language

Java is a full-featured, general-purpose programming language that is capable of developing robust mission-critical applications. Today, it is used not only for Web programming, but also for developing standalone applications

across platforms on servers, desktops, and mobile devices. It was used to develop the code to communicate with and control the robotic rover that rolled on Mars.

Java has a virtual machine (VM) which is a software application that simulates a computer, but hides the underlying operating system and hardware from the programs that interact with the VM. If the same VM is implemented on many computer platforms, applications that it executes can be used on all those platforms^[8]

3.5.2 Cryptography Techniques:

3.5.2.1 RSA Algorithm (Rivets, Shamir and Adelman)

RSA is a block cipher in which the plaintext and cipher text are integers between 0 and $n - 1$ for some n .

Encryption and decryption are of the following form period for some plaintext block M and cipher text block C :

$$C = M^e \bmod n$$
$$M = c^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the values of n and e , and only the receiver knows the value of d . This is a public-key encryption algorithm with a public key of $KU \{e, n\}$ and a private key of $KR \{d, n\}$ with 64bits long^[9]

3.5.2.2 Advanced Encryption Standard (AES)

The Advanced Encryption standard (AES) is a symmetric-key block cipher published by the national institute of standard and technology (NIST) in December 2001.

AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12 or 14 rounds. The key size, which can be 128, 192 or 256 bits, depends on the number of rounds depends of the number of round^[10]

3.5.3 Integrity Techniques

Secure Hash Algorithm (SHA-1)

Is the most widely used hash function, SHA is based on the hash function MD4, and its design closely models MD4. SHA-1 produces a hash value of 160 bits. In 2002, NIST produced a revised version of the standard, FIPS 180-2, that defined three new versions of SHA with hash value lengths of 256, 384, and 512 bits known as SHA-256, SHA-384, and SHA- 512, respectively. Collectively, these hash algorithms are known as SHA-2.^[9]

3.5.4 Authentication Techniques

Mutual authentication

Mutual authentication, or two-way authentication, is the technology in which both communicating parties in a communications phenomenon can authenticate each other. In a network environment, the client authenticates the server and vice-versa. This means that network users can be assured that they are doing business exclusively with lawful entities and servers can be certain that all users are authentic to gain access for legitimate purposes. Mutual authentication is accepted as a tool to minimize the risk of online cheat in e-commerce^[11]

CHAPTER 4

SYSTEM PROCEDURE AND ANALYSIS

4.1 Introduction

In this chapter we will discuss the procedure of the system at its various stages; the system has been modeled and analyzed by identifying its functions through clarifying the procedure of the system by identifying the interaction between the user and the system, also we will discuss the process of system modeling and system analyzing using Unified Modeling Language(UML).

4.2 System procedure

The interaction between the user and the system uses to explain the procedure of the system as mentioned in the introduction, the stages of this procedure are:

4.2.1 Running of the Authentication Application

- At this stage the user installed specified system's USB Flash Memory which contains the authentication application of the customer and system's browser in the device which wants to use it to conduct transactions with the specified bank.
- Then the user installs Java JDK program through which we can run Java program on the computer in use, that because the authentication application and the browser are programmed by Java Language. Existence of auxiliary folder for the user can help them easily install Java JDK program.
- If the computer already occupied by Java JDK program, the user should go to the next step directly.
- Then the user runs the customer's authentication application which is located in USB Flash Memory to contact the third part to know the logical address of the bank which wants to contact with.

4.2.2 Authentication between the User and the Bank

- After the completion of the previous phase successfully we move on to the authentication stage at where we do the exchange of authentication information to ensure the reliability between the bank and the customer.

- Then the application displays an interface to the user to enter their user name and password to be logged only in the authentication application not to the bank, and that to know whether this user authorized to use this application or not. This step is important because it helps in reducing the load on the network and that because of the application will contact the third party to retrieve the bank logical address immediately after this step, then the third party will inform the bank by the customer who wants to contact with. In case of cancellation of this step the application will ask from the bank address whether the user is authorized or not.
- After the user authentication, the application displays another interface in order to help the user choose the bank which wants to deal with.
- Then this application requests the bank logical address from the third party.
- After getting the logical address of the specified bank, the application contacts the bank to match between the bank and its logical address.
- If the previous step is done successfully, then the customer's authentication application will run the system's browser in order to display the page of the bank at where the user can log in to their accounts.

4.2.3 Transactions with the Bank

If the previous stages done successfully the browser displays a page of the bank transactions for the user to choose the treatment they want

4.3 System Analysis

As we can see from the above figure it is clearly shown how can bank deal with (client bank application) and third party.

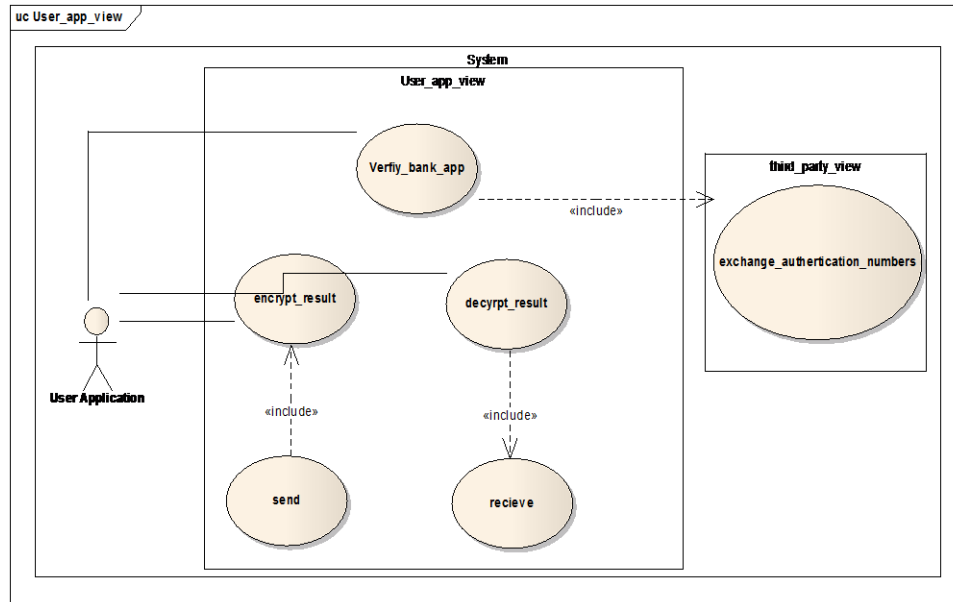


Figure 4.1: Use Cases Diagram: User Application View

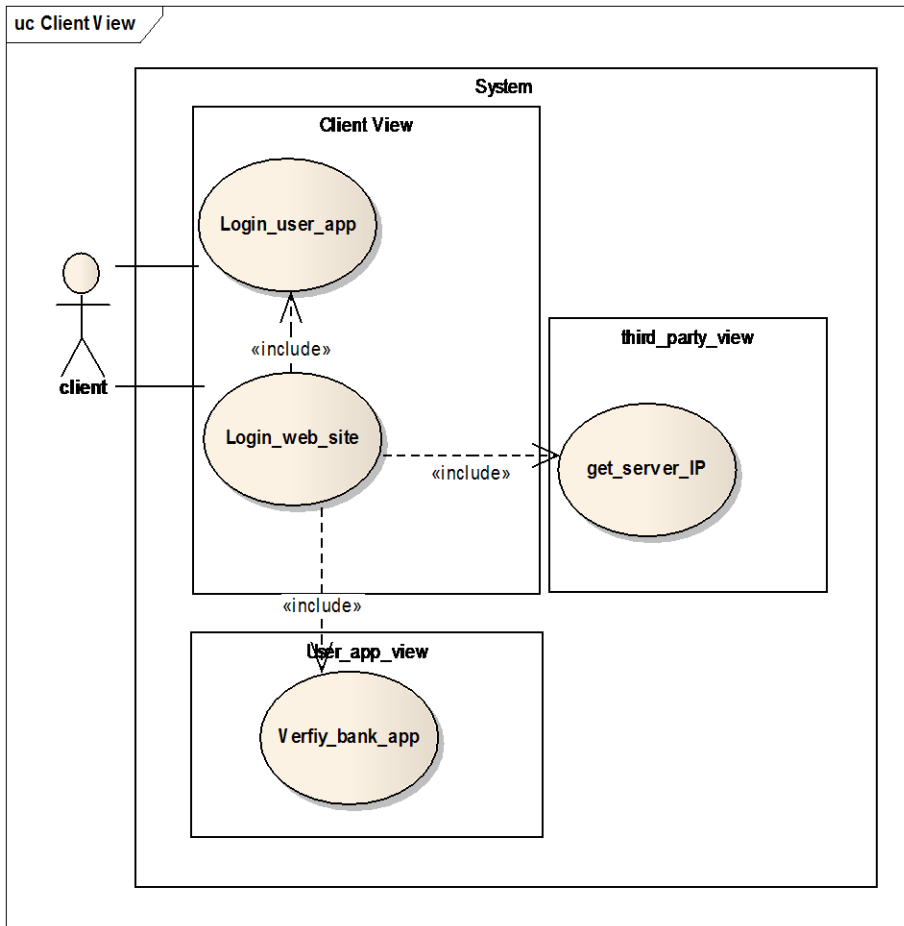


Figure 4.2: Use Cases Diagram: Client View.

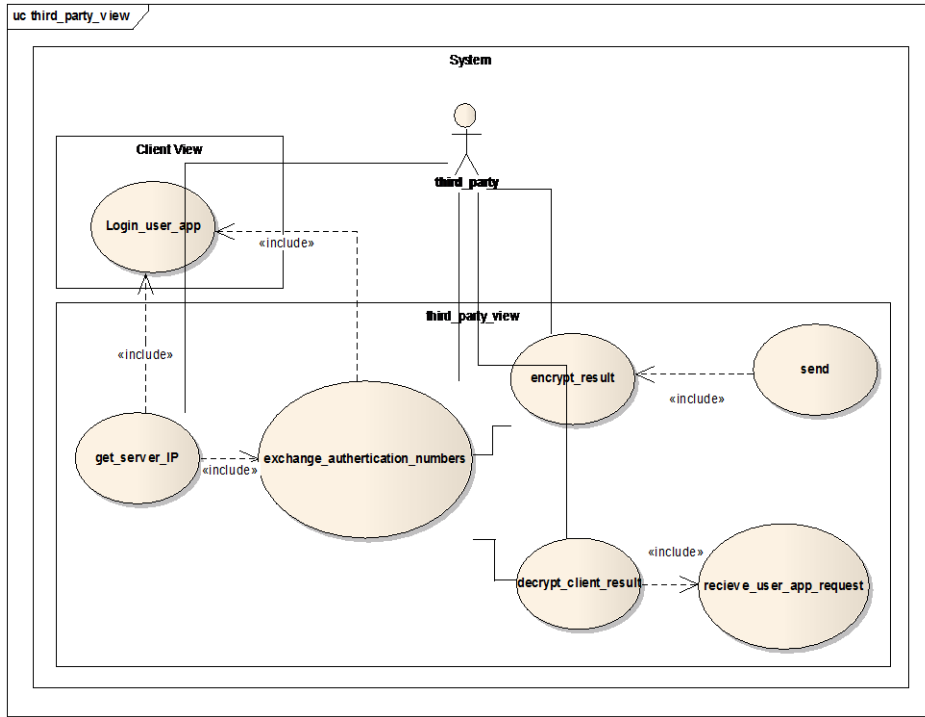


Figure 4.3: Use Cases Diagram: Third Party View.

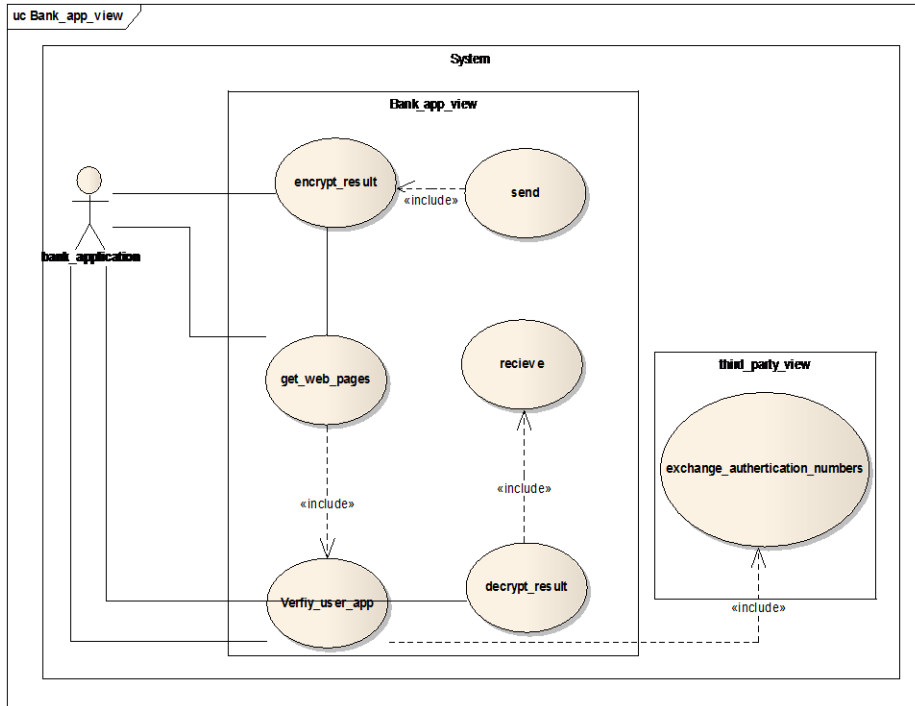


Figure 4.4: Use Cases Diagram: Bank Application View.

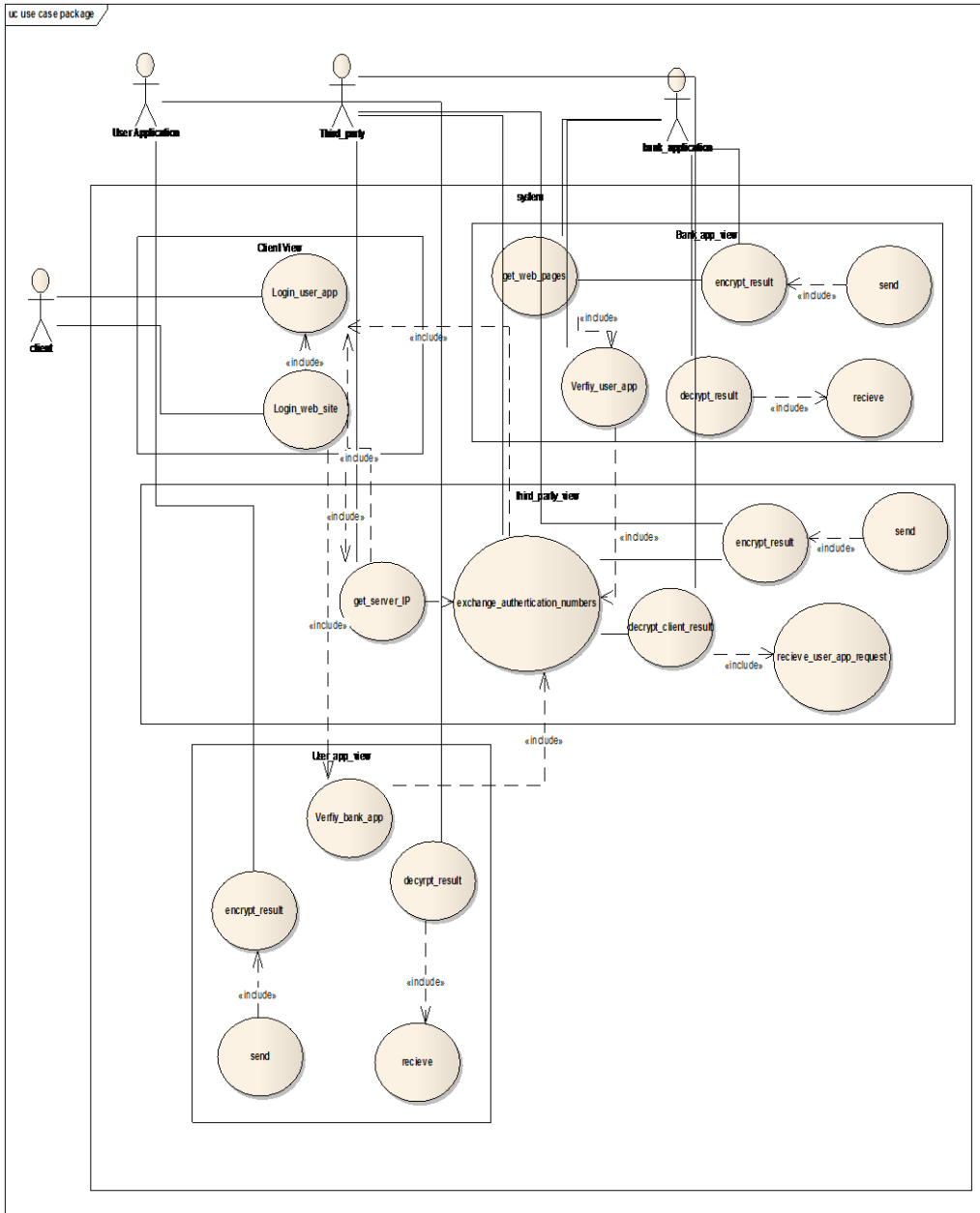


Figure 4.5: System Use Cases Diagram

The above figure represent the activities and process step by step starting by the client request to bank page until the bank response with decrypted result, and how the third party manage the process of authentication.

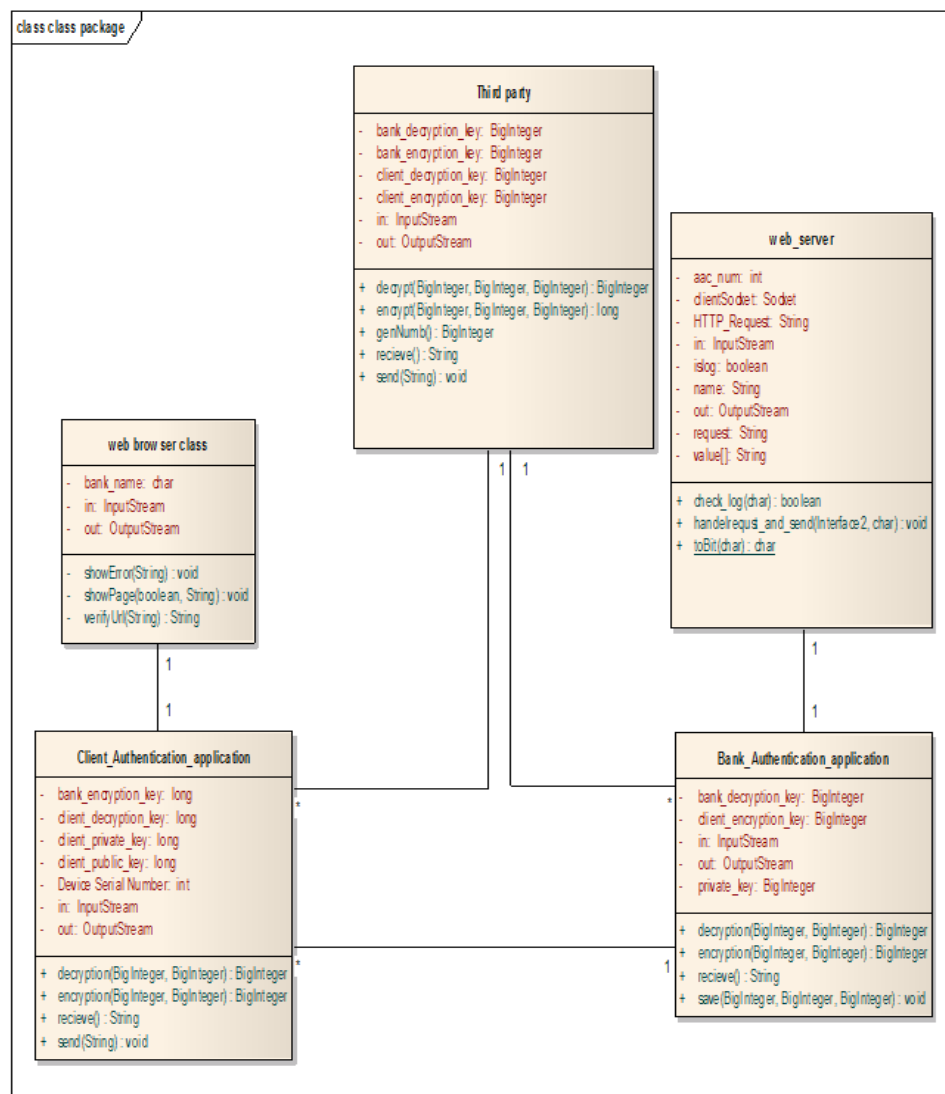


Figure 4.7: System Class Package Diagram.

The above figure represents the three entities of System in a technical view with the functions and the return parameters for each.

Bank_Authentication_application

Public Class:

Client_Authentication_application

Public Class:

Third party

Public Class:

Web Browser Class

Private Class:

Web Server

Private Class:

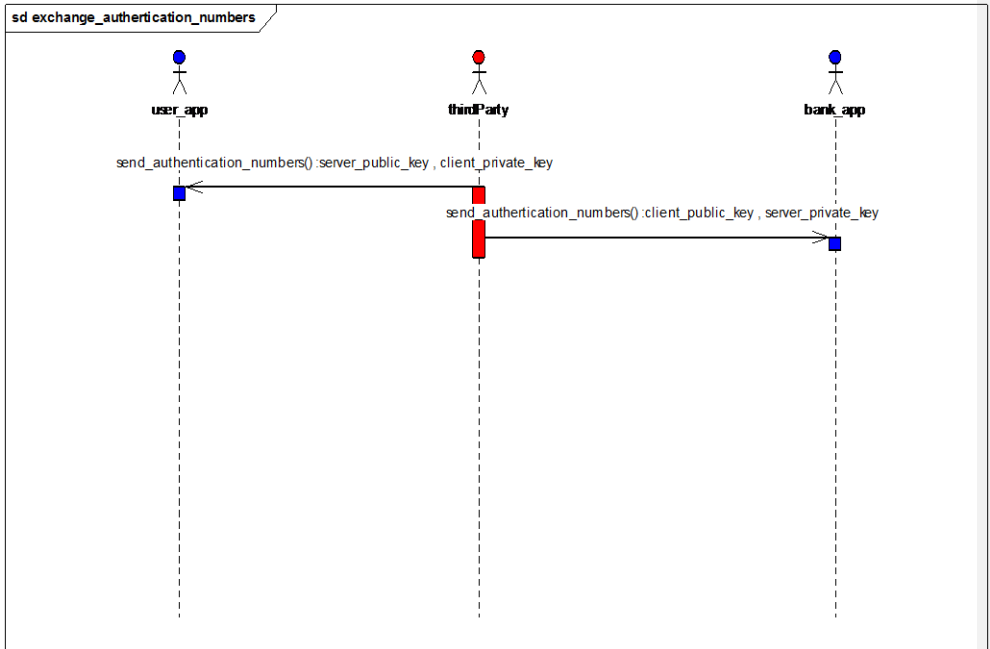


Figure 4.8: Sequence Diagram: Exchange Authentication Numbers

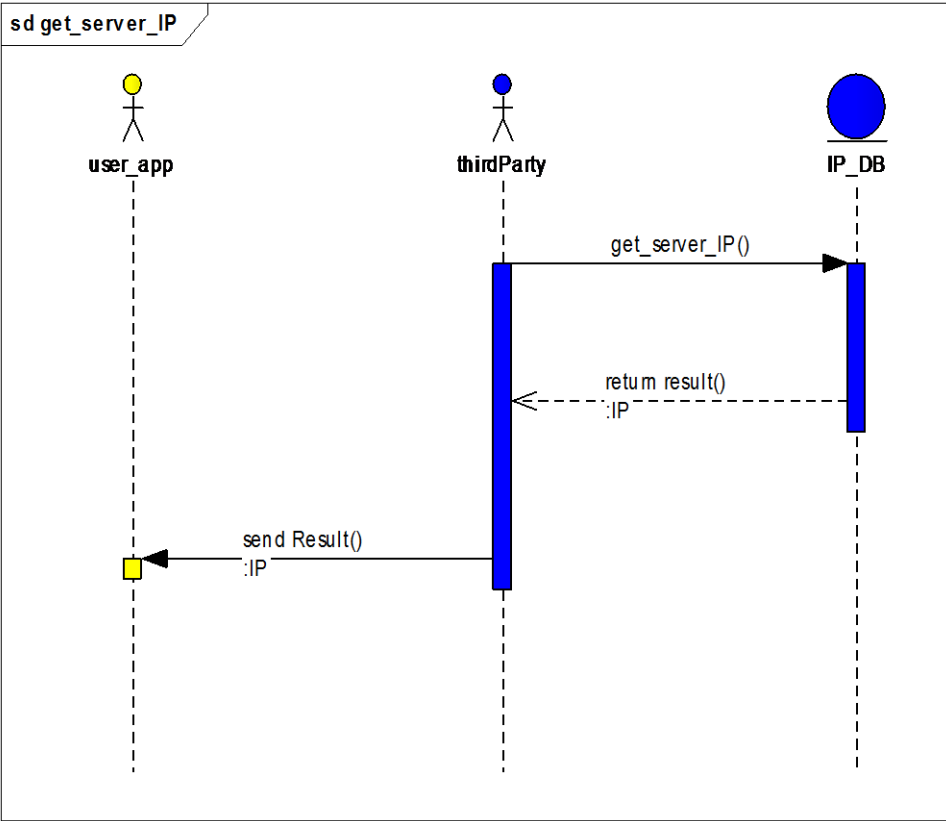


Figure 4.9: Sequence Diagram: Get Server IP Address.

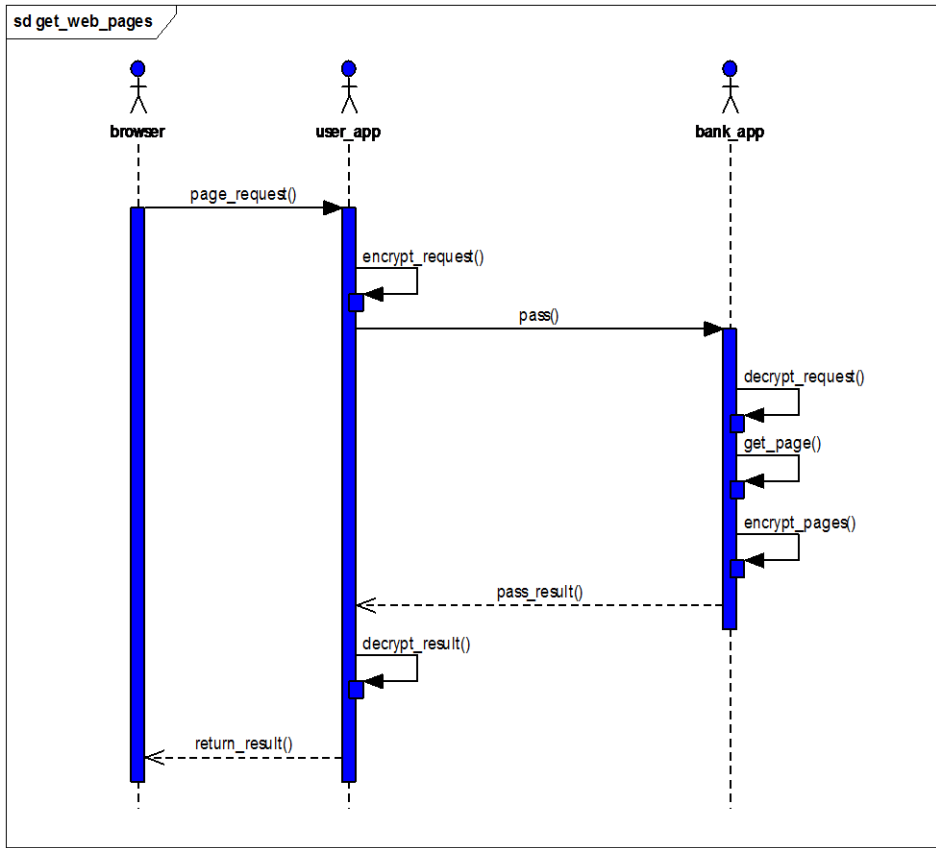


Figure 4.10: Sequence Diagram: Get Bank Web Page.

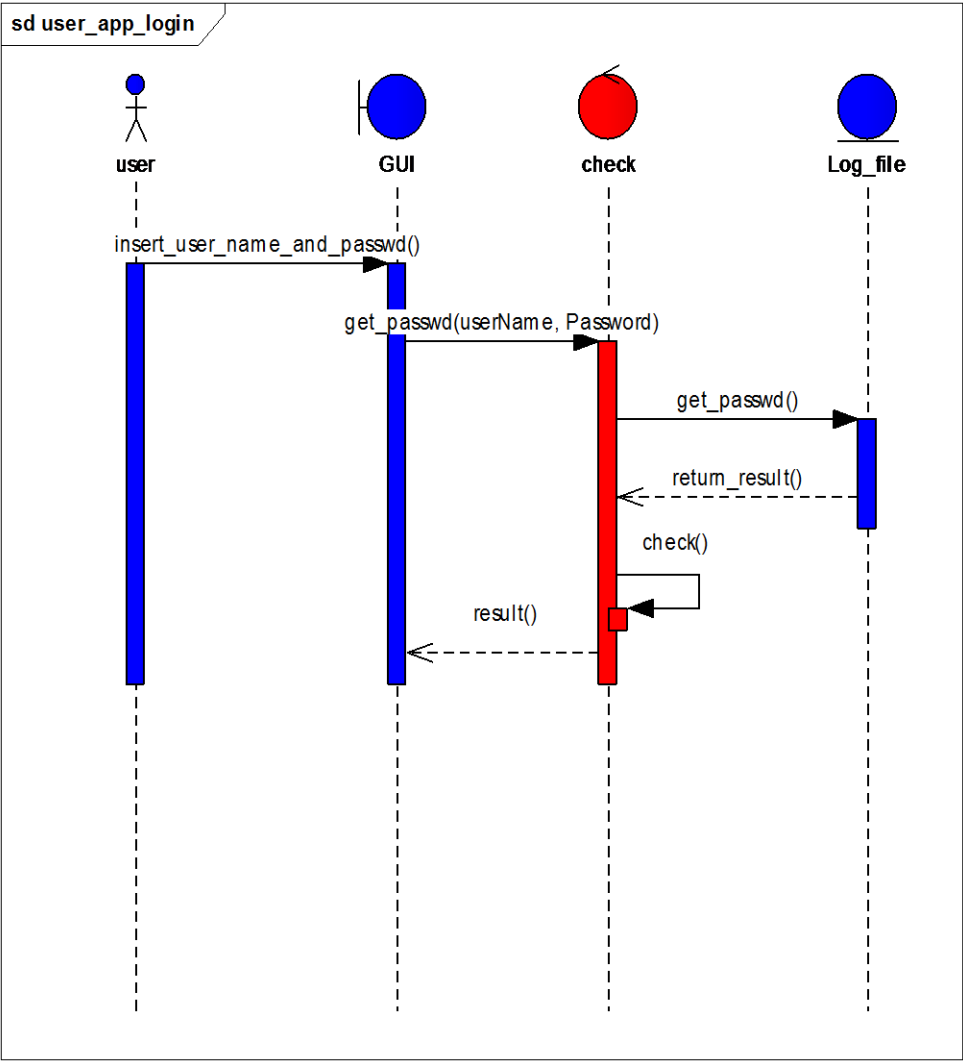


Figure 4.11: Sequence Diagram: User Login.

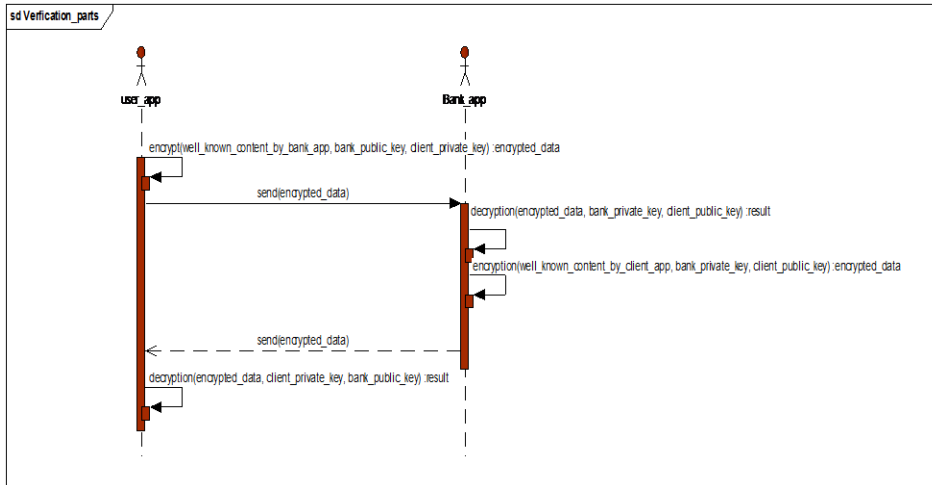


Figure 4.12: Sequence Diagram: Verification System Components.

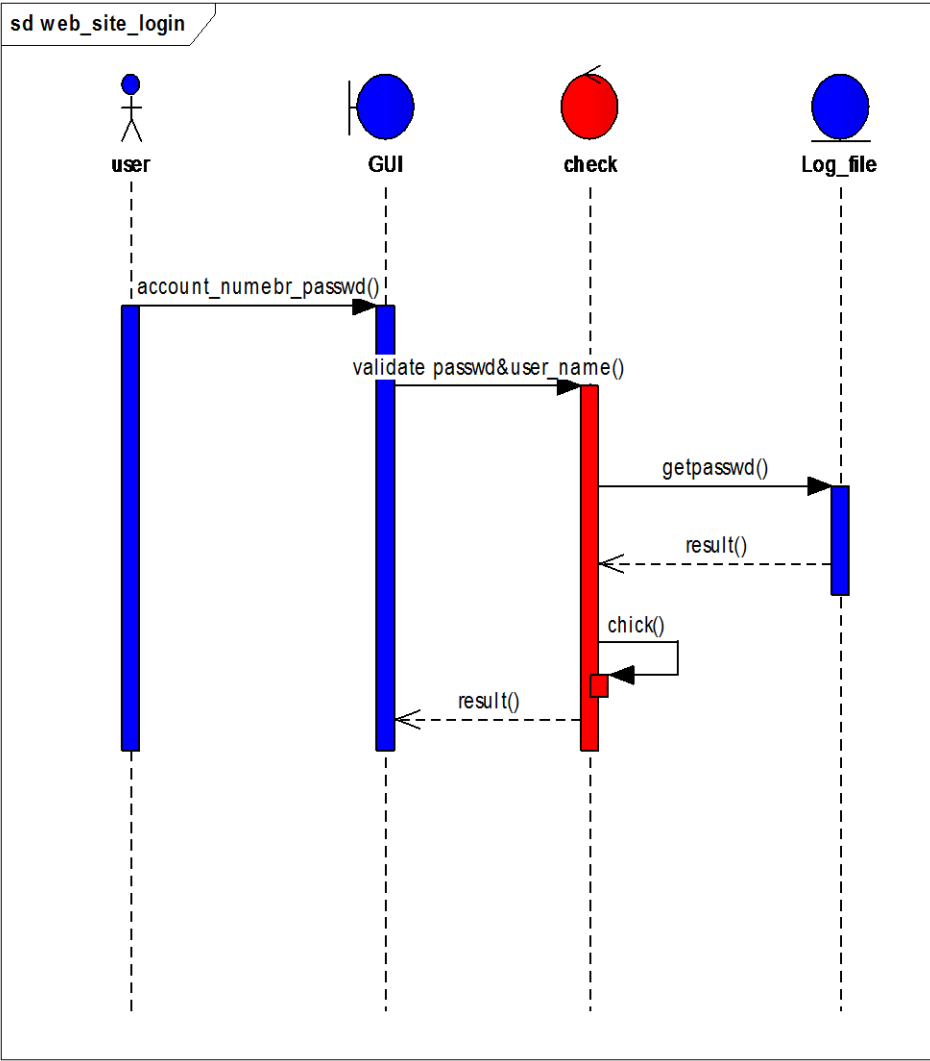


Figure 4.13: Sequence Diagram: Bank Web Site Login.

CHAPTER 5

RESULTS and DISCUSSION

5.1 Results

The final product was developed with a simple interface, server Side (Bank) and the third party that manage the communication between the banks and their clients as we proposed earlier in chapters.

The used protocol uses third party to deliver the needed information and keys between clients and banks in secure line to begin authentication process between them, then open secure channel to begin online transactions using a self-developed and secured browser.

The software designed to be portable (jar file) to work on different Operating Systems with same efficiency. The next (figures 5.1-5.4) show Snapshots from the client software.

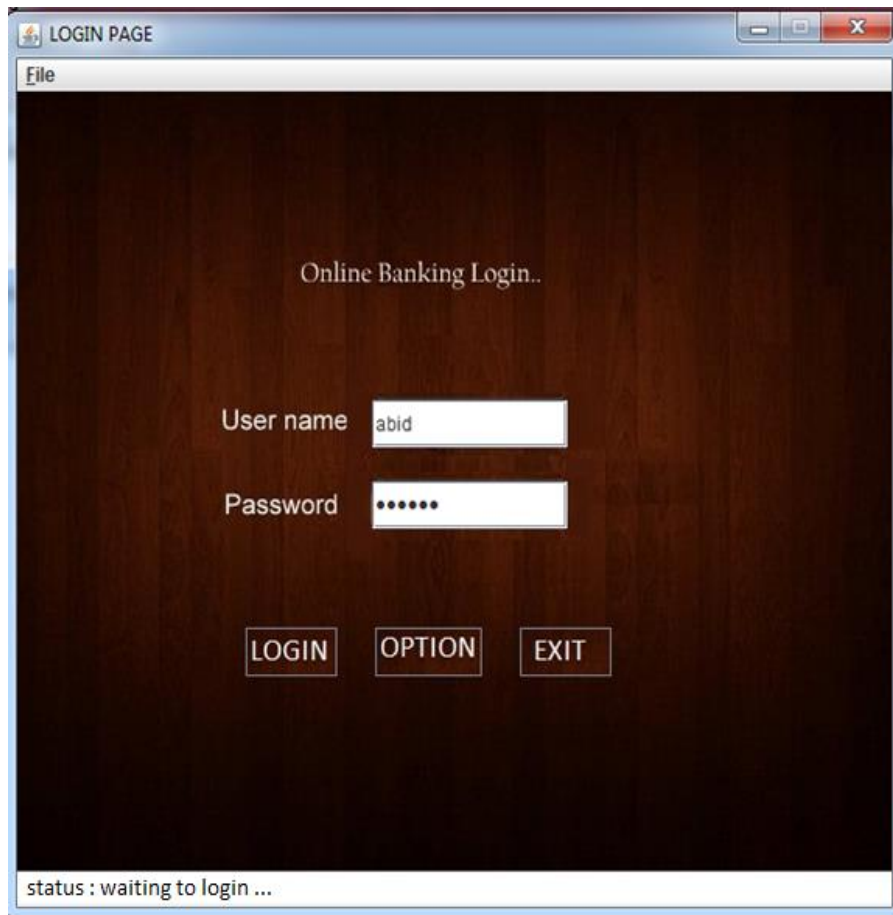


Figure 5.1: Login Form.

The Main Login interface software content two Fields username, password and three buttons:

- Login : to log on software after pass the authentication by user name and password
- Option :content may option
- Exit :Exit from system



Figure 5.2: Main Form.

The upper figure5.2 shows the main connection to online banking service content drop dawn menu user can select your bank then click the connect button and content many buttons:

- Logout : to log out from this logon user.
- Option: content many option
- Exit :Exit from system



Figure 5.3: Options From.

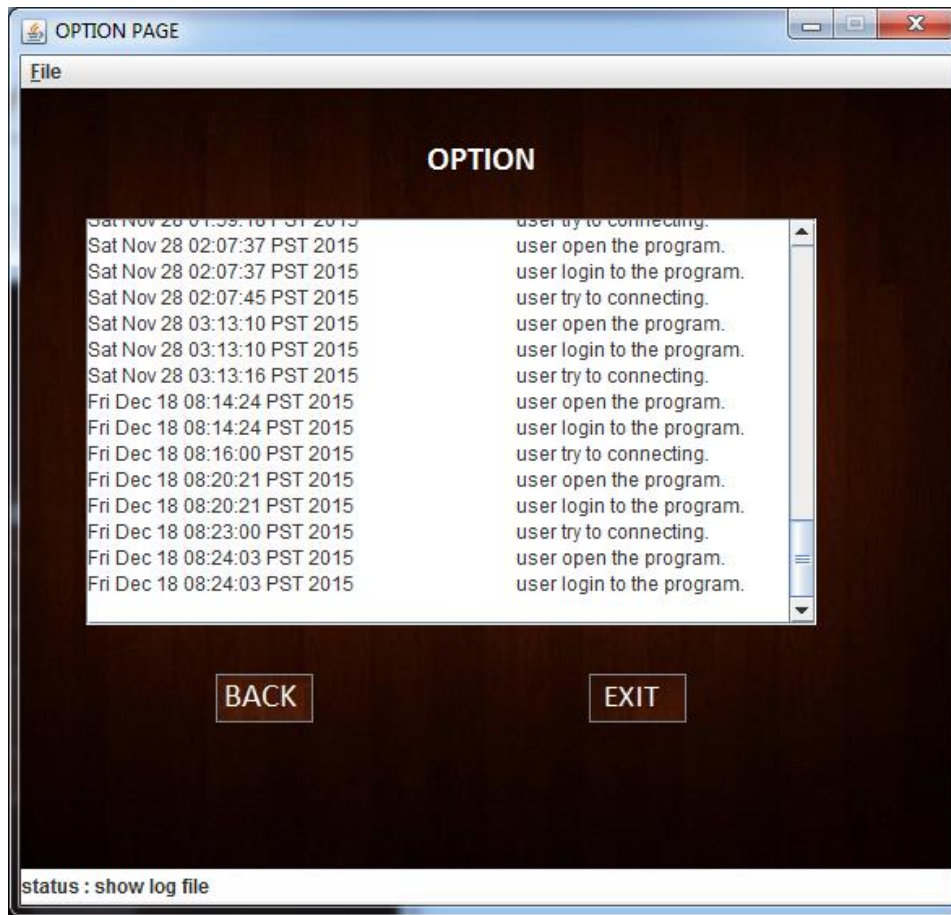


Figure 5.4: Log Form.

Browser Interfaces

The developed browser in this research considered important key of this solution, it designed to control communication between bank server and client by encrypt and decrypt the http socket after keys exchanged.

Also it solved the problem of view page source in the other browsers which leads to prevent the browsers' attacks like sql injections, writing scripts and even copy page contents.

The Banks pages designed to be simple and contain just the important components to speed the process of transferring data between client and bank server. The next figures [5.6-5.9] show the designed pages.

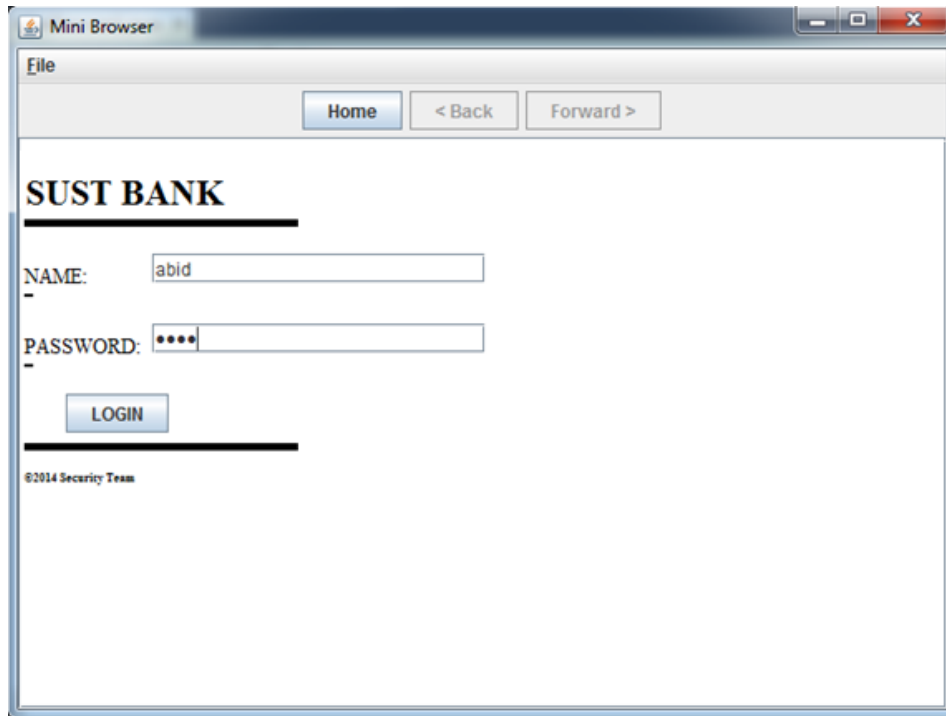


Figure 5.5: Bank Login Page.

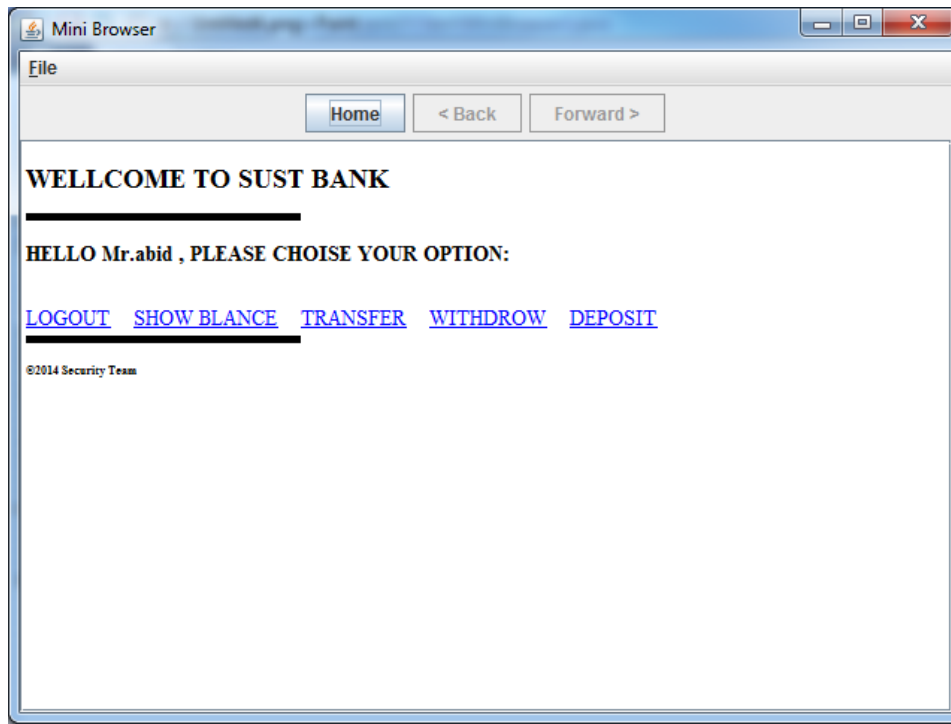


Figure 5.6: Bank Home Page.

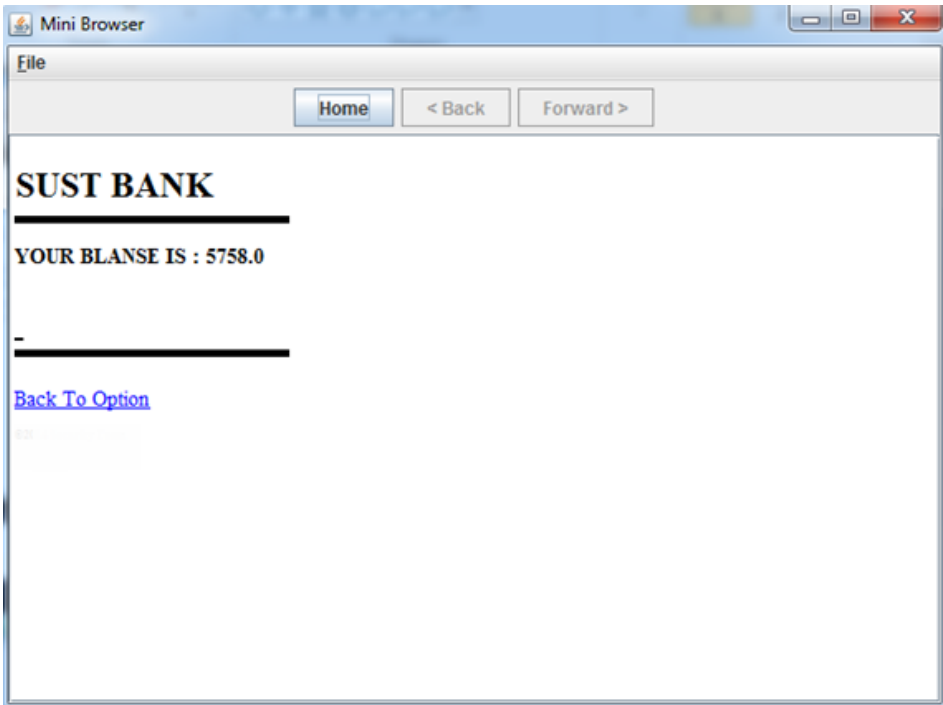


Figure 5.7: Show Balance Page.

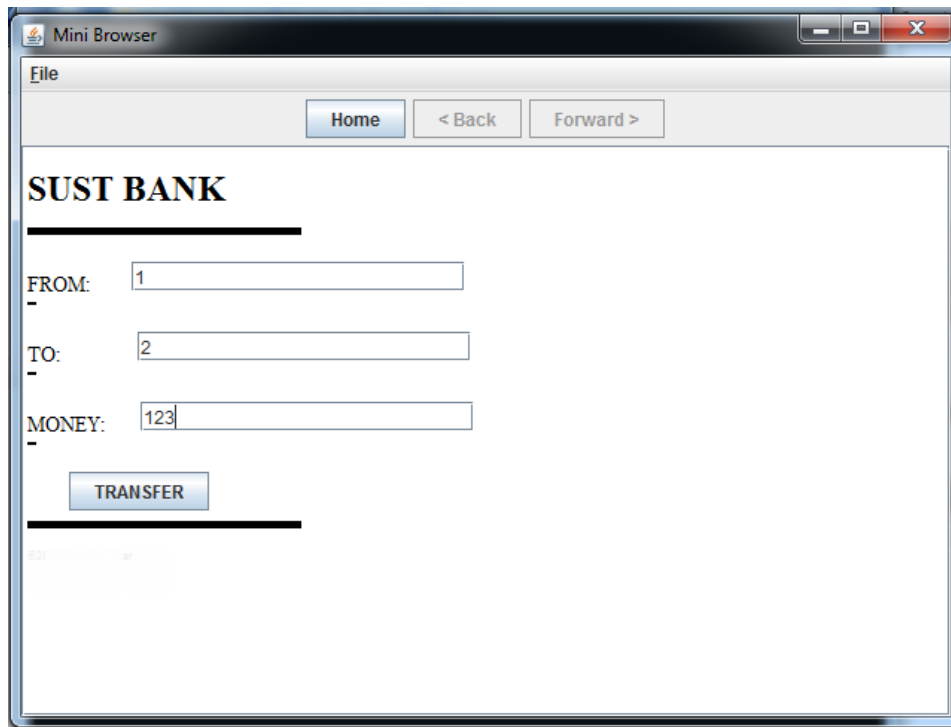


Figure 5.8: Transfer Page.

5.2 Proposed System evaluation and validation:

The system has been tested on a virtual environment consisting of 20 clients, 2 banks and third-party. All the clients accessed to the system at the same moment and the system has served all of them with some delaying in some operations due to the reasons that the specifications of the devices which used as servers are not compatible with standard specifications of the servers. After testing of the system, it has been concluded that the system is able to provide the following:

- Reliability: it appears in helping clients to make sure that the page they are dealing with is the actual page of the bank and not any other fake page using the

secure browser as we can show in the next figure 5.10 the data the exchange between client and bank it took by Wireshark tool

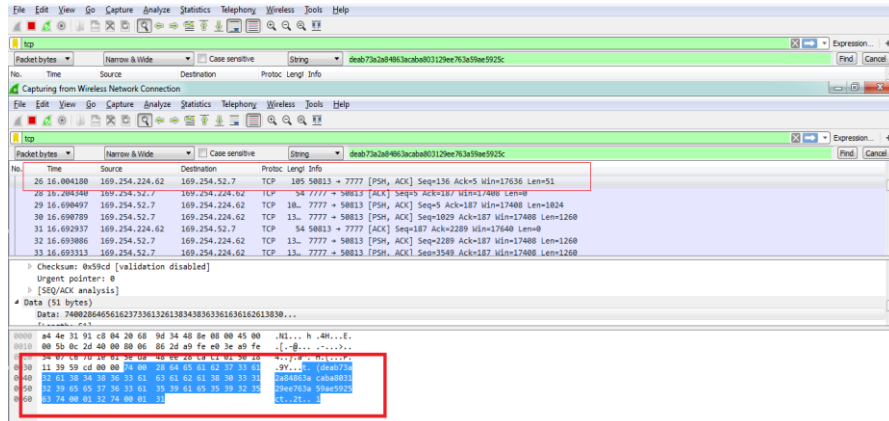
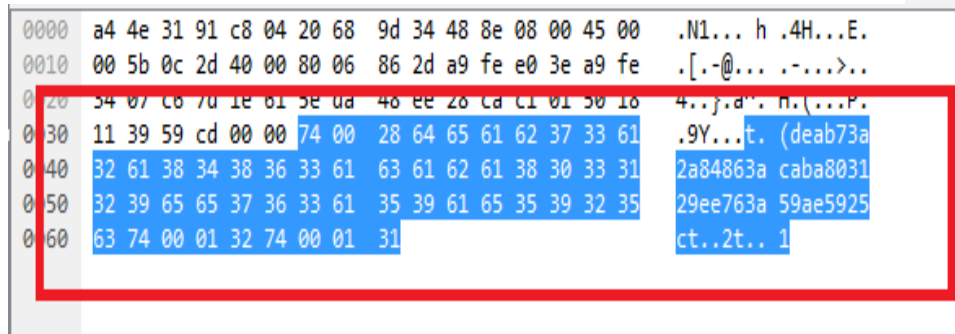
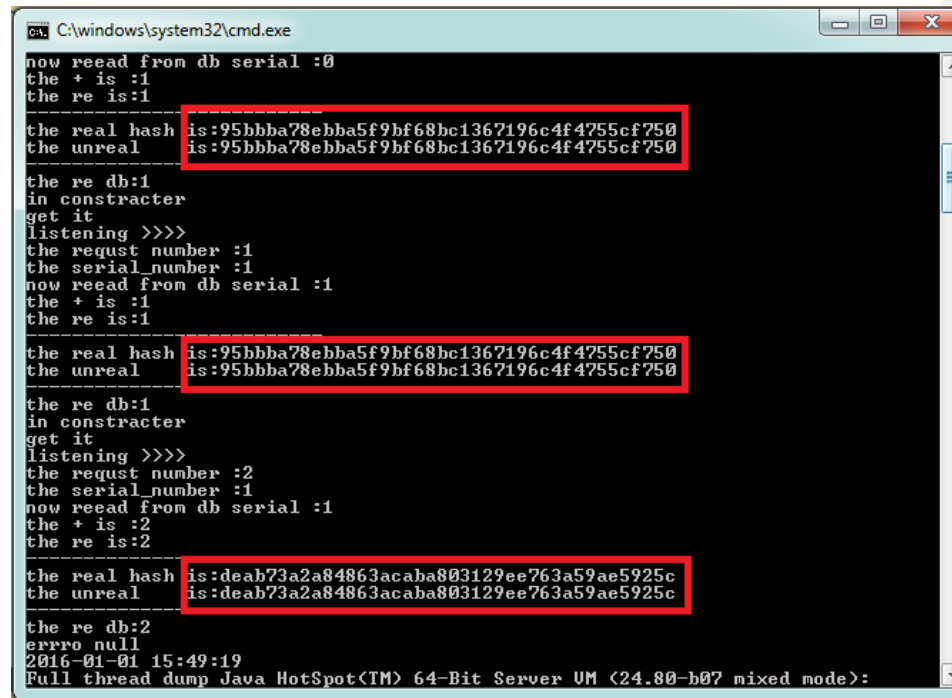


Figure 5.9: Wireshark screenshot.



- Authentication: is to verify that the customer is not impersonating by someone else, it will be on several levels:
 - First level: user's password which is exists in the user's computer.
 - Second level: typing of user name and password in the bank's website.
- Security and protection: where the exchange data is encrypted.
- Data Integrity: it is achieved by using SHA-1 which can figure out any data updates during the process of transmission by sending Hash value with the data and when the

reception process finished, the value of Hash will recount, if the new value of Hash remain as same as its first value that means the data is safe, the next figure show snapshot from bank server.



```
C:\windows\system32\cmd.exe
now read from db serial :0
the + is :1
the re is:1
the real hash is:95bbba78ebba5f9bf68bc1367196c4f4755cf750
the unreal is:95bbba78ebba5f9bf68bc1367196c4f4755cf750
the re db:1
in constracter
get it
listening >>>
the request number :1
the serial number :1
now read from db serial :1
the + is :1
the re is:1
the real hash is:95bbba78ebba5f9bf68bc1367196c4f4755cf750
the unreal is:95bbba78ebba5f9bf68bc1367196c4f4755cf750
the re db:1
in constracter
get it
listening >>>
the request number :2
the serial number :1
now read from db serial :1
the + is :2
the re is:2
the real hash is:deab73a2a84863acaba803129ee763a59ae5925c
the unreal is:deab73a2a84863acaba803129ee763a59ae5925c
the re db:2
errro null
2016-01-01 15:49:19
Full thread dump Java HotSpot(TM) 64-Bit Server VM (24.80-b07 mixed mode):
```

Figure 5.10: Bank Server Snapshot.

The real hash is from client and the unreal is generated by the Bank server after decrypt the data from client. We notice that the two hashes are identical.

- Simplicity and flexibility of banking service access.
- Mobility: the client to transfer between many devices and the proposed Framework enables the user to mobility and use it in more than one device.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

The presence of the e-banking system in Sudan via the third party (Central bank of Sudan) encourage the researchers to do this kind of secure online banking, which provides a great deal of comfort to users and the financial system in the country as a whole.

The developed solution considered a new addition in E-Banking solutions with simple usability, access and provide a level of confidentiality in all bank transactions by using very secure protocol to prevent many types of attacks. Moreover in this protocol, a newly proposed secure browser has been implemented to ensure more security and reliability.

At last this solution tried to accomplish something that can participate in developing of both the field and the country which I belong to, and there is no doubt establishment of such studies and projects like this can strongly support the country to be developed in the field of online banking service.

Finally I ask the Almighty Allah to benefit the mankind by this study and to teach us whatever we don't already know and to add this study to my good deeds, and It's my pleasure to end my study by sending blessings and salutations upon the one who has sent as a mercy to mankind Muhammad peace be upon him.

6.2 Future work and Recommendations

There is no doubt that the projects which are undertaken in the field of computer science encounter a lot of obstacles and problems, Whether that was the lack of time for the completion of these projects, or the accessibility of the tools for the completion of these projects and the lack of previous studies, and scarcity in a lot of cases. In addition to the lack of availability of specialized references of the subject of online banking or

electronic banking (especially the studies in Arab countries and specifically in Sudan), this project tried to accomplish the majority goals of the project but the actual fact that perfection doesn't exist so what we couldn't achieve completely. The recommendation scan is summarized as follows:

- Use several algorithms into two types of symmetric encryption and asymmetric to provide more confidentiality and insurance.
- Improve developing Browser used in the project.
- Dynamic contents pages Developing for the banks in order to be closer to the reality.
- Procedure tests on the system in terms of breaking the keys through statistical attack and Brute force attack. That needs special devices.
- Procedure test consider about the Agents Man-in-the Middle attack (MITMA) who receives the packages and re-sent it after the modification.
- Let the users be far more aware about the method of cheat and how to avoid it, because it the main reason of success in such this kind of cheating.

Reference

- [1]M.-C. Lee. (2009), *Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit,* " *Electronic Commerce Research and Applications*, vol. 8, pp. 130-141, 2009.
- [2] (2010) *Online Banking Fees: Look for the Lowest Rates*.
<http://www.msmonney.com/mm/banking/onlinebk/fees.htm>. Available in (2013, 2 Oct).
- [3] AhnLab, *White paper Online Banking: Threats and Countermeasures*, Seoul 150-869, Korea, <http://www.ahnlab.com> Release Date: June, 2011
- [4](2013)*Phishing Activity Trends Report: 1th Quarter 2013*, APWG2013
- [5]The Pharming Guide - Whitepapers.
<http://www.technicalinfo.net/papers/Pharming2.html>Available in: (2010, 20Oct)
- [6] Xing Fang, Justin Zhan. (2009), *Online Banking Authentication Using Mobile Phones*, June 2009.
- [7]M. A. Hossain, M. A. Tahir. (2012), *Intelligent phishing detection and protection scheme for online transactions*, SKIMA 2012 Conference
(<http://dl.acm.org/citation.cfm?id=2461550.2461819&coll=DL&dl=GUIDE&CFID=345940878&CFTOKEN=17330119>).
- [8]Liang, Y. Daniel.Introduction to Java programming: comprehensive version/Y. Daniel Liang, sixth edition.
- [9] W. Stalling, *Network Security Essentials, applications and standards: by prentice Hall, Fourth edition, 2010*
- [10]Behrouz A. Fourzan ,*Cryptography and network security*.
- [11]<http://searchfinancialsecurity.techtarget.com/definition/mutual-authentication>

[12]د. خالد بن عبدالرحمن الثغبر، م. سليمان عبدالعزيز الهيشة، الإصطياد الإلكتروني الأساليب والإجراءات المضادة، من إصدارات مركز التميز لأمن المعلومات جامعة الملك سعود، (2009م - 1429هـ) (ص 50-70).

[13] Mohamed Al-Fairuz and Karen Renaud. Multi-Channel, Multi-level Authentication for More Secure eBanking. ISSA 2010. Johannesburg, South Africa. 2-4 August, 2010.

[14] Leung, C.M., 2009, August. Depress phishing by CAPTCHA with OTP. In Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on (pp. 187-192). IEEE.

[15] Wu, M., Garfinkel, S. and Miller, R., 2004, July. Secure web authentication with mobile phones. In DIMACS workshop on usable privacy and security software (Vol. 2010).

[16] Wüest, C., 2006. Threats to online banking. White Paper: Symantec Security Response.

