EasyChair Preprint

№ 4975

Building A Secure Internet Banking Environment for the Bank

Nashwan Ghaleb Al-Thobhani and Naser Al-Maweri

February 5, 2021

Building A Secure Internet Banking Environment for the Bank

dr.Nashwan Saeed M.G. Al-Thobhani, UMS & Sana'a Community College, nashwansg@gmail.com;
dr. Naser Ahmed O. Al-Maweri, Nasa202006@gmail.com, Sana'a Community College, Yemen;

Abstract—This study was developed for the Bank and implemented on a real test environment and the study aims to build a secure Internet Banking Environment for the Bank which provides a high level of security and availability and effective management and control of a network environment. The researchers used the interview and questionnaire as tools to collect data for the primary and final study. By analyzing the interview questions and the questionnaire, the researchers concluded that the bank needs to build an online banking environment with a high level of security and availability to save time and effort for customers and the bank, reduce congestion on the bank, gain customer satisfaction, get more customers and meet their requirements At the end of the study, the researchers made a plan for implementing the appropriate proposed solutions.

Keywords: *Internet, Banking, Service, Security, Intelligent devices, Environment and Cryptography*

1. INTRODUCTION

TToday's world is one with increasing online access to services. One part of this which is growing rapidly is Internet Banking. "Internet Banking" is the new technology in banking environment, which allows the bank customers to do banking activities at any time and from any place. The Bank began using the Internet to operate their business and interact with the markets, Internet Banking one of the major Internet services which provided by bank.

2. Problem Background

The Bank began using the Internet Banking service to operate their business and interact with the markets, "Internet Banking" refers to systems that enable bank customers to access accounts and general information of bank products and services through a personal computer (PC) or other intelligent devices. Internet Banking allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society. Internet Banking is a new specific banking area, part of e-banking industry, which allows people to interact with their banking accounts virtually from anywhere in the world. Internet Banking addresses few emerging trends such as customer demand for anytime, anywhere services, product time to market essentials, and increasingly complex back-office integration challenges. One such challenge is the security of online financial transactions. In order for the industry to develop further, secure transactions with the trust of the customers are necessary aspects. Security of the transactions is a main concern for The Bank while the lack of security may result in serious actual loss. Examples of potential hazards of Internet Banking include online transactions, minting electronic currency, etc.

3. Problem Statement

Needs for providing a high-level security in a network environment of Internet Banking systems in The Bank.

4. Problem objectives

The main objective of this study is to build a Secure Internet Banking Environment for The Bank. the sub objectives of this study are the following:

- To provide high level of security in network environment.
- To provide high level of availability in network environment.
- Effective manage and control of network environment.
- Risk management for Internet Banking environment.
- Evaluate the network environment of Internet Banking system.

5. Problem contribution

It will contribute to set clear steps for implementing a secure environment for Internet Banking in The Bank in the best way possible

6. Problem hypothesis

The Bank needs to provide a high-level security in a network environment of Internet Banking systems.

- **Methodology:** The first stage is to determine and define the problem and its background. In the second stage, searching about the information that are related to the subject of the study from resources as well as theoretical background on the topic of the study have been prepared. The third stage was to create the action plan, schedule and the current situation. At the fourth stage, the gathered data through the interview questions and the questionnaire were analyzed and discussed. Also, measuring the reliability and validation against the pilot study is discussed. In the fifth stage, the suggestions and the recommendations were offered, the implementation plan was created and the significance of these solutions were explained.

7. LITERATURES REVIEW

6.1. The Internet

This high level of connectivity encourages an unparalleled degree of communication, resource sharing, and information access. It is probably the most powerful and important technological advancement since the introduction of the desktop computer. In order to benefit from what the net has to offer, a basic understanding of what it is and how it works is helpful [1]. Some of the basic services available to Internet users are: Email, Telnet, FTP, WWW,

6.2. The Internet Banking

The delivery channels include direct dial-up connections, private networks, public networks etc, and the devices include telephone, personal computers (PC) including the Automated Teller Machines (ATM), etc. With the popularity of PCs, easy access to Internet and (WWW), Internet is increasingly used by banks as a channel for receiving instructions and delivering their products and services to their customers. This form of banking is generally referred to as Internet Banking, although the range of products and services offered by different banks vary widely both in their content and sophistication[6].

6.3. Definition of Internet Banking

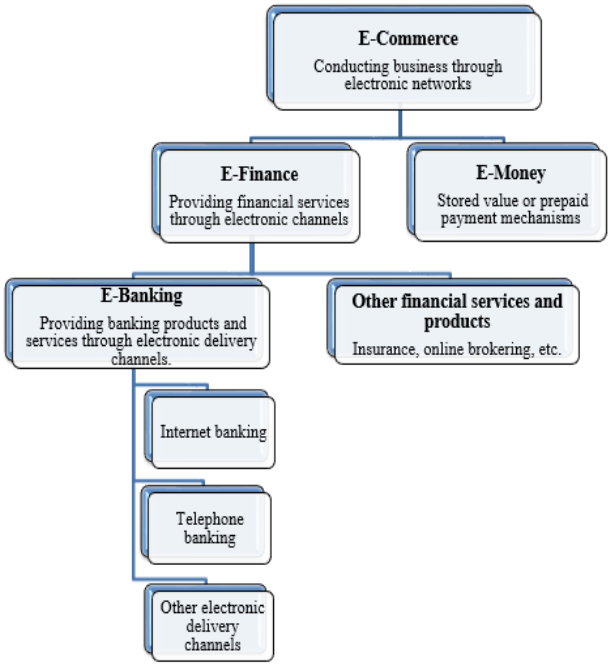

Fig.1: describes the definition of internet banking.

Internet banking also known as “Online Banking” refers to systems that enable bank customers to access accounts and general information on bank products and services through a (PC) or other intelligent device. Internet Banking lets many banking transactions handled via a PC. For instance, computer may be used to view an account balance, request transfers between accounts, and pay bills electronically[7].

Internet banking system and method in which a PC is connected by a network service provider directly to a host computer system of a bank such that customer service requests can be processed automatically without need for intervention by customer service representatives. The system is capable of distinguishing between those customer service requests which are capable of automated fulfillment and those requests which require handling by a customer service representative.

6.3. History of Internet Banking

Online services started in New York in 1981 when four of the city’s major banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) offered home banking services. First internet banking service started in the UK in 1983, Bank of Scotland offers Nottingham Building Society (NBS) known as “home link” connecting via a telephone and television to send transfers and pay bills. The first online banking service in

United States was introduced, in October 1994. The first online website was Stanford Federal Credit Union, which is a financial institution. In 2001, 19 million users started accessing bank accounts online. In 2005, Debit and credit was launched. In 2007, Apple launches I-phone and shifting of banking services via PC or Smartphone begins. Technology has enabled numerous advantages and overcome the traditional banking, offering the best of banking experience on fingertips[8].

6.4. Growth in Internet Banking

The challenge for national banks is to make sure the savings from Internet banking technology more than offset the costs and risks associated with conducting business in cyberspace. Marketing strategies will vary as national banks seek to expand their markets and employ lower cost delivery channels. Examiners will need to understand the strategies used and technologies employed on a bank-by-bank basis to assess the risk. Evaluating a bank's data on the use of their Web sites, may help examiners determine the bank's strategic objectives, how well the bank is meeting its Internet banking product plan, and whether the business is expected to be profitable. Some of the market factors that may drive a bank's strategy include the following: Competition ,Cost efficiencies, Geographical reach , Branding and Customer demographics

6.5. Types of Internet Banking

Understanding the various types of Internet Banking products will help examiners assess the risks involved. Currently, the following three basic kinds of Internet Banking are being employed in the marketplace:

6.5.1. Informational: This is the basic level of Internet Banking. Typically, the bank has marketing information about the bank's products and services on a stand-alone server.

6.5.2. Communicative: This type of Internet Banking system allows some interaction between the bank's systems and the customer. The interaction may be limited to electronic mail (e-mail), account inquiry, loan applications, or static file updates (name and address changes).

6.5.3. Transactional: This level of Internet Banking allows customers to execute transactions. Since a path typically exists between the server and the bank's or outsourcer's internal network, this is the highest risk architecture and must have the strongest controls. Customer transactions can include accessing accounts, paying bills, transferring funds, etc[7].

6.6. The advantages of Internet Banking can be summarized as follows:

- **Convenience**
  Unlike the corner bank, online banking sites never close; they're available 24 hours a day, seven days a week, and they're only a mouse click away.
- **Ubiquity**
  If moving out of state or even out of the country when a money problem arises, it's possible to be logged on instantly to the online bank and take care of business, 24/7.
- **Transaction speed**
  Online bank sites generally execute and confirm transactions at or quicker than ATM processing speeds.
- **Efficiency**
  Accessing and managing personal bank accounts is available, including IRAs, CDs, even securities from one secure site.
- **Effectiveness**
  Many online banking sites now offer sophisticated tools, including account aggregation, stock quotes, rate alerts and portfolio managing programs to help managing all of assets more effectively. Most are also compatible with money managing programs such as Quicken and Microsoft Money

- **The disadvantages of Internet Banking can be summarized as follows:**
- **Start-up may take time**
  In order to register for the bank's online program, would probably be required to provide ID and sign a form at a bank branch
- **Learning curve**
  Banking sites can be difficult to navigate at first. Plan to invest some time and/or read the tutorials in order to become comfortable in the virtual lobby.
- **Bank site changes**
  Even the largest banks periodically upgrade their online programs, adding new features in unfamiliar places. In some cases, re-enter account information may be required.

6.7. Types of risks associated with Internet banking: Operational risk, Security risk, System Architecture and Design, Reputational risk, Legal risk, Money laundering risk, Cross border risks,

Strategic Risk and Other risks (Credit risk, Liquidity Risk and Risk of unfair competition)

Thus, one can find that along with the benefits, Internet banking carries various risks for bank itself as well as banking system as a whole. The rapid pace of technological innovation is likely to keep changing the nature and scope of risks banks face. These risks must be balanced against the benefits. Supervisory and regulatory authorities are required to develop methods for identifying new risks, assessing risks, managing risks and controlling risk exposure. But authorities need to keep in consideration that the development and use of Internet banking are still in their early stages, and policies that hamper useful innovation and experimentation should be avoided. Thus authorities need to encourage banks to develop a risk management process rigorous and comprehensive enough to deal with known risks and flexible enough to accommodate changes in the type and intensity of the risks [9].

6.8. Technology and Security Standards for Internet Banking

6.8.1. Banking Products

The products accessible through Internet can be classified into three types based on the levels of access granted: Information only systems, Electronic Information Transfer System and Fully Transactional System.

6.8.2. Attacks and Compromises

When a bank's system is connected to the Internet, an attack could originate at anytime from anywhere. Some acceptable level of security must be established before business on the Internet can be reliably conducted. An attack could be any form.

6.8.3. Authentication Techniques

As mentioned earlier, authentication is a process to verify the claimed identity. There are various techniques available for authentication. Password is the most extensively used method. Most of the financial institutions use passwords along with PIN (Personal Identification Number) for authentication. Technologies such as tokens, smart cards and biometrics can be used to strengthen the security structure by requiring the user to possess something physical (Smart cards and Biometrics).

6.8.4. Firewalls: The connection between internal networks and the outside world must be watched and monitored carefully by a gatekeeper of sorts. Firewalls do this job. Broadly, there are three types of firewalls i.e. packet filtering firewalls, proxy servers and stateful inspection firewall.

6.8.5. Cryptography: Cryptography is the art and science of keeping messages secure. It uses a 'key' for encrypting or decrypting a message. Both the method of encryption and the size of key are important to ensure confidentiality of a message (Diffie-Hellman and RSA)

6.8.6. Digital Signature and Certification: To generate digital signature, the original, unencrypted message is processed through mathematical algorithms that generate a 'message digest' (a unique character representation of data). Certificate Authorities and Digital Certificates are emerging to further address the issues of authentication, non-repudiation, data privacy and cryptographic key management. A Certificate Authority (CA) is a trusted third party that verifies the identity of a party to a transaction. The diagram above shows flow of messages in SSL. The flow of authentication messages in SSL is shown in Fig.2.

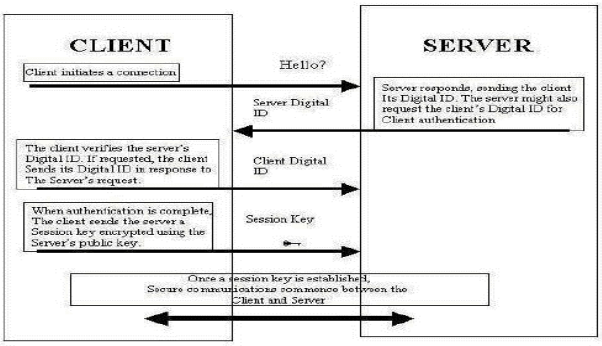

Fig.2.: Flow of messages in SSL-based security (at conceptual level)

Public Key Infrastructure (PKI): PKI consists of the following components:

Key Certificate, Certification Authority (CA), Registration Authority (RA), Certificate Repository, Certificate Revocation List (CRL), Certificate User, Confidentiality, PKI and Certificates and PKI Architectures.

6.8.7. Tools: Tools are extremely useful in monitoring and controlling networks, systems and users. Some of the system administration and network management tools are Scanners, Sniffers, Logging and Audit tools.

6.8.8. Physical Security: Physical Access can be secured through the following means: Bolting Door Locks and Combination Locks, Electronic Door Locks, Biometric Door Locks, Manual Logging, Electronic Logging, Photo Identification Badges, Video Cameras stationed at strategic points, Controlled Visitor Access. A bank should also have in place environmental

controls to manage exposures from fire, natural disasters, power failure, air-conditioning failure, water damage, bomb threat / attack etc. A few means of obtaining control over environmental exposure are:

- The server room and any other unattended equipment room should have water detector. Fire extinguishers should be placed at all strategic points, supplementing fire suppression systems with smoke detectors, use of fire-resistant materials in office materials including furniture, redundant power supply from two substations, electrical wiring placed in fire resistant panels and conduits and documented and tested evacuation plans.
- It is important to educate all 'stake-holders' (users, employees, etc) about the importance of physical security. This education should be carried out as part of 'social engineering'.

6.8.9. Security Policy: The information security policy is the systemization of approaches and policies related to the formulation of information security measures to be employed within the organization to assure security of information and information systems owned by it. The top management of the bank must express a commitment to security by manifestly approving and supporting formal security awareness and training. Security guidelines, policies and procedures affect the entire organization and as such, should have the support and suggestions of end users, executive management, security administration, IS personnel and legal counsel [6]. Figure 3 shows the latest Internet security and monitoring systems implementation. The following security measures are used to protect the privacy and the confidentiality of the communications between your Internet Browser and our Online Banking Servers:

6.8.10. To secure communications between your Internet Browser and the Bank's servers, Cryptography (encryption) is used to protect banking transactions from unauthorized access or tampering.

6.8.11. The protocol used to establish the secure session is called Secure Sockets Layer (SSL) Encryption. Once a secure session is established, keys (public and private) are exchanged between your browser and our Online Banking server.

6.8.12. The browser can tell whether is in a secure session mode by looking for the secured lock symbol at the bottom of the browser window. To provide the highest amount of security during online banking session, it is recommending to have an Internet browser with 128-bit encryption.

6.8.13. To obtain authorized access to the Bank's Online Banking system, it must to enter a password at the beginning of each online banking session. The password is verified at a secure data center. If entering a password incorrectly three (3) times during a Personal Online Banking session, or five (5) times during a Business Online Banking session, the online banking account will be locked until contact with the bank to unlock the banking account.

6.8.14. To provide additional security during the online banking session, the bank's online banking system provides a "timeout" feature. If the computer has been left or do not perform a transaction over a predefined time period, the online banking system will automatically be logged out of the secure session.

6.8.15. Both physical and automated security techniques are employed to protect against unauthorized access to the Bank's Online Banking Servers, computers storing customer account information and the Bank's website. The online banking server retrieves information from the Bank's computer containing customer account information through a proxy-based firewall server [10].

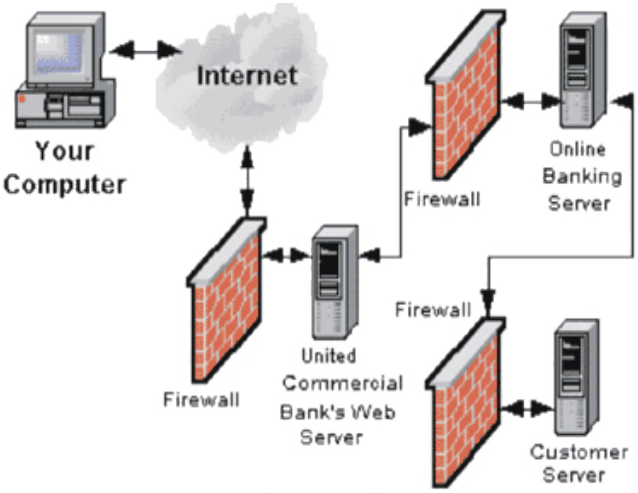

Figure 3. The latest Internet security and monitoring systems implementation.

6.8.16. Network Intrusion Detecion System (IDS): IDS can be set inline, attached to a spanning port of a switch, or make use of a hub in place of a switch. Network Intrusion Detection Systems (IDS) monitor system behavior and alert on potentially malicious network traffic (Baker, 2004). IDS can be set inline, attached to a spanning port of a switch, or make use of a hub in place of a switch. The idea here is to allow access to all packets you wish the IDS to monitor. When the system constantly gives false alarms, alerts tend to not be taken seriously. Fig.4. shows the IDS device.

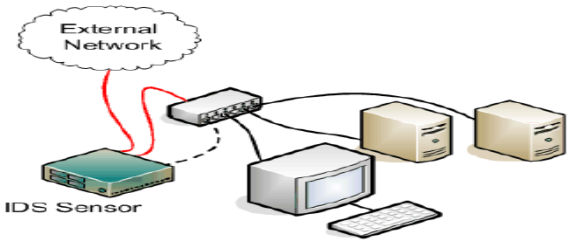

Fig. 4 Network Intrusion Detection Systems (IDS)

6.8.17. Network Intrusion Prevention System (IPS): An IPS is capable of monitoring the content deep inside the Web traffic. When the IPS discovers an event considered to be a true positive, the malicious connection is dropped and all subsequent matching packets are destined for the same outcome. Fig.5. shows the IPS device.

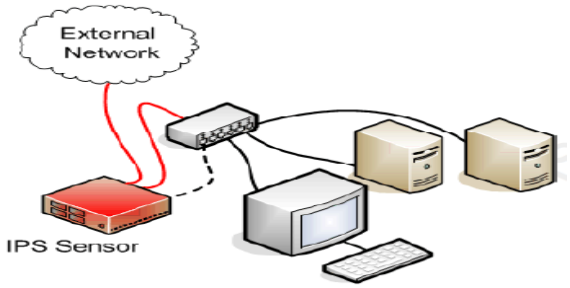

Fig. 5. Network Intrusion Prevention Systems (IDS)

6.8.18. Internet Banking Infrastructure

a) **Hardware** : Web servers, Aplication servers, Database aervers and Network equipmant.

b) **Software:** Systems software and Aplication software.

c) **Services:** Application integration with core banking, Scalability tests (desirable but optional), Web designing and Server sizing.

d) **Security:** Firewalls, Certification, Server level (mandatory), Client level (optional), Intrusion detection system and Subscribing to advisories.

e) **Hosting decision:** In-house vs IDC.

f) **Networking:** Isolation from the main network.

7. Current Situation of the Bank.

7.1. Organizational Structure of the Bank

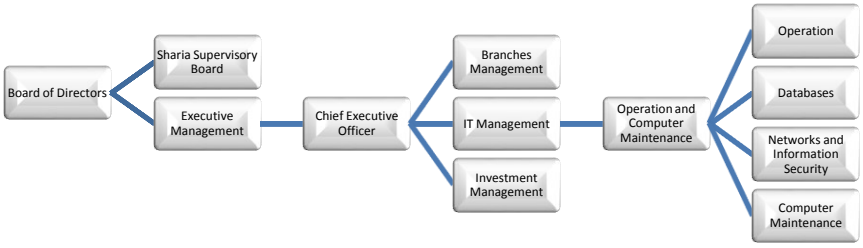

Fig. 6: Organizational structure of the Bank

7.2. The Bank Services

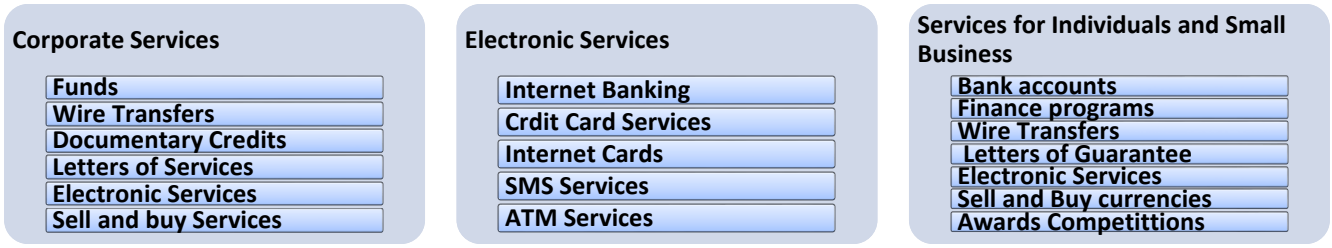

Fig. 7: The Bank services

7.3. IT Department in The Bank

IT Management is the most important management in the bank because it is responsible for the operation of the banking system from the beginning to the end. The management is responsible for daily backup and for any defect or malfunction in the system. Also, the most important and most dangerous tasks of the management are to maintain the confidentiality of the web site that works 24 hours a day, which contains Internet Banking services.

8. Data Analysis and discussion

The researchers here present the data collected for the research from the interview with the IT infrastructure manager and network security administrator in the Bank (the pilot study), and the questionnaire distributed to the IT department in Bank and customers of the Bank (the final study).

8.1. The Pilot Study

The data collected for the pilot study is shown by illustrating the answers of the interview's questions with the IT infrastructure manager and network security administrator in the Bank. The interview's questions and the obtained answers are shown in Table 1.

Table 1 The answers of the interview's questions

Question 1	**When have you started operating the Internet Banking services?**
Answer	We started in 2008.
Question 2	**What is the users' average that are using the Internet Banking services?**
Answer	Not a lot, because the Internet Banking was implemented just on the employees of the bank and two months ago the bank published the service on the branches and customers.
Question 3	**What are the available operations for users that are using the Internet Banking services?**
Answer	To query the account statement To query the current balance Profit operation To view the data of funds
Question 4	**What are the accounts logging in requirements of Internet Banking?**
Answer	First of all, customers should go to the bank and do the following requirements: having an account in the bank. filling the required information about the requested service user name, phone number, signature matching, account number … etc.
Question 5	**Do you have security policies related to the Internet Banking resources access?**
Answer	Physical security policy, by allowing some authorized persons to enter into the data center room with fingerprint and card systems. Logical security policy, by creating a user name and password, as well as, specifying the permissions for each user.
Question 6	**Are you using the digital certification?**
Answer	Yes, we are using the SSL certificate from "VeriSign".
Question 7	**Do you have special database for Internet Banking?**
Answer	Yes, we have a database server for this service. Also, the applications are at the same server (database and applications server).
Question 8	**Are there the verification users logging in?**
Answer	Yes, we send a message to the customer's email informing him by the logging in process.
Question 9	**Approximately, how many customers that log in to the Internet Banking at the same time (bottleneck)?**
Answer	Because of the little number of customers in this service, we don't have a bottleneck.
Question 10	**Are there any affect happens to the Internet Banking system at the bottleneck time?**
Answer	If the bottleneck happened, showing the old data for the customers will be the affected factor.

Question 11	**What is the Internet Banking infrastructure that is used?**
Answer	Application and database server for Internet Banking system. Web server for the website of the bank. Firewalls. Router with ADSL WIC.
Question 12	**Do you have traffic monitoring programs in Internet Banking network?**
Answer	Yes, we have a program from Microsoft.Net to monitor the traffic and logging in tries.
Question 13	**Do you have VPNs network that used in Internet Banking?**
Answer	Yes, we have.
Question 16	**Is there a responsible person for administrating and securing the Internet Banking resources? (if yes, mention the number of them).**
Answer	Yes, there are two persons the first is responsible for the system and the database of the Internet Banking, and the second is responsible for the network security.
Question 17	**Do you make a routine penetration testing?**
Answer	No, but the bank has applied for international companies in this field.
Question 18	**Are there problems in the Internet Banking network?**
Answer	No serious problems about the network, just some that need to restarting the system.
Question 19	**Do you have suggestions to develop the Internet Banking services?**
Answer	Make a modern technique about the security. Focusing on the communication between the bank and the customer. Make a backup connection for Internet .
Question 20	**Do you have any other information related to the Internet Banking?**
Answer	There are a lot of Internet Banking infrastructure scenarios with their advantages and disadvantages, so, search about that in the Internet.
Answer	No. we don't have a VPN in the Internet Banking, but we have VPNs to communicate between branches.
Question 14	**Do you use an international security standard in the Information Technology (IT) department?**
Answer	We don't have until now, but the bank will make an evaluating and penetration testing to start putting an international standard for the bank.
Question 15	**Do you have a disaster recovery plan?**

Question 21	**Is there any cost limitation for secure Internet Banking implementation?**
Answer	No, just make facility study and apply it for the management.

8.2. The Final Study

The data collected for the analyses and discusses the results of the final studies of the study for IT employees in Saba Islamic Bank and the bank's customers.

8.3. IT Employees

The data collected for the research's final study is shown by the percentages and a graphical illustration for the questionnaire, that was distributed to the IT department employees in The Bank. Figure (8) illustrate the questions' percentages of the IT questionnaire.

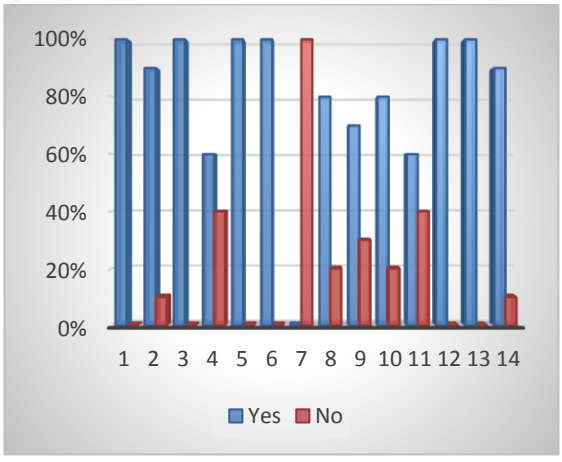

Figure (8) the questions' percentages of the IT questionnaire

8.3.1. Customers in the Bank

The data collected for the study's final study is shown by the percentages and a graphical illustration for the questionnaire, that was distributed to the customers of the Bank.

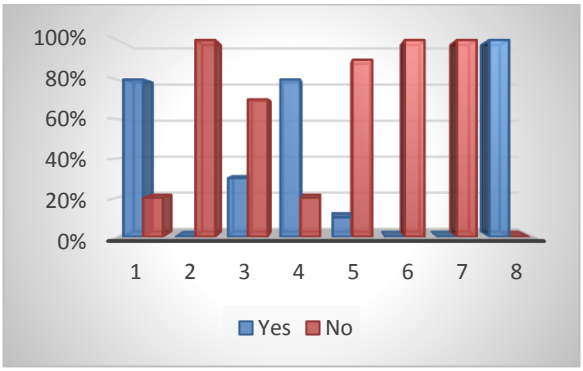

Figure (9) the questions' percentages of the customer questionnaire

9. Hypothesis Validation

The Hypothesis that was put at beginning of the study says “The Bank needs for provide a high-level security in network environment of Internet Banking systems”. This part will validate the correctness of this hypothesis. By returning to the questionnaires results of IT employees, the question number 3 This question has 100% percentage “Yes”. So, the money transfer process over the Internet needs to a high level of security in the bank. Also, the question number 5. This question has 100% percentage “Yes”. This points to that the all IT department employees proving that the Internet Banking infrastructure needs to a high level of security. As well as, the question number 10. This question has 80% percentage “Yes”. This refer to that the most of IT department employees proving they need to update the security techniques continuously to prevent the continuous risks and threats of the Internet. On other hands, the question has 20% “No” which mean they do not think that.

Obviously, all these questions result (3,5 and 10) prove the validation and correctness of the hypothesis of the study

10. Comparison between the Research’s Pilot and Final Study *(Reliability)*

By Comparing between the results obtained from the study's pilot and final studies we noticed that when we entered the web site to the Internet Banking service, we can only query for the account, which shows that they have a fear to use all of the operations available in this service. This fear caused by the need for a high level of security and the provision of new technologies to protect Internet Banking service and secure communication between the customers and bank. As well as, the need to aware and train customers to use the service.

This is what has been deduced from the second question, fifth, ninth, tenth, thirteenth, fourteenth, seventeenth, eighteenth and twenty of interview questions. As well as, from the first question, second, third, fifth, sixth, seventh, eighth, ninth, tenth, twelfth and thirteenth of the questionnaire, where the answered questions from the interview questions are compatible with the questionnaire.

11. Recommendations and Suggestions.

11.1. Identify Suggested Solution

The Suggested Solution was specified depending on The Bank requirements.

The Bank requirements:

a) High level of security in the environment of the internet banking system.
b) To manage and control internet banking network easily.
c) To implement risk management to develop the security policies that used in the internet banking.
d) To implement redundancy for network environment.
e) Use new security techniques related to internet banking.

11.2. Topology Network Design

Figure 9. Shows the Topology Network Design.

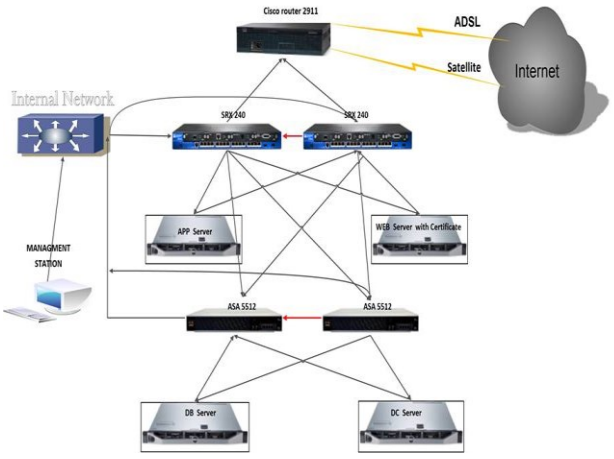

Figure 10 Topology network design.

11.3. Logical Network Design

Figure 11. Shows the Logical Network Design with IP Addressing.

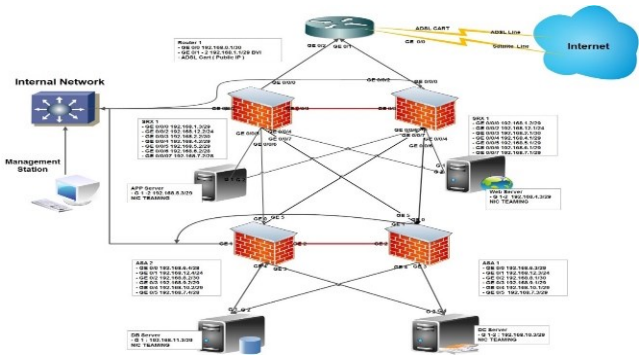

Figure 11. Logical network design

11.4. Network Test

The research was implemented and tested in Engineering Computer Center depending on specific topology as shown in figure 11 below.

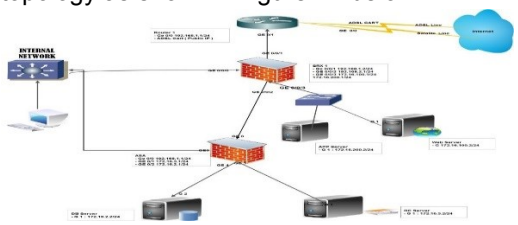

Figure 11 Network test

11.5. Conclusion

The goal of this study is to Build a Secure Internet Banking Environment for the Bank which provides a high level of security and availability and effectively manage and control of network environment.

The final findings of the research can be summarized as, the Bank needs high level of security in the environment of the Internet Banking system, high availability in the network environment, manage and control Internet Banking network easily, implement risk management to develop the security policies that used in the Internet Banking and to use new security techniques related to Internet Banking. The study was mentioned future recommendations to implement which help to increase the quality of the Internet Banking system, these recommendations can be summarized as: use Token-ring technology and RSA server to guarantee a perfect level of validation, make a study to compare with Islamic CAC bank the use Internet Banking system, perform a penetration testing by organization that is specialized with penetration testing, perform security risk management regularly to maximize use of finite organizational assets based on measurable risks, implement the ISO-27001 information security standard and conduct new study that aims to improve Internet Banking security.

The study will contribute to save time and effort for customers and the Bank, the customers can access to their account at any time, any place, reduce congestion on the bank, gain customers satisfaction, have more quantity of customers and meet their requirements, precedence in providing this service in Yemen, provide high secure between the bank and customers and provide high viability

In addition, this study contributes to provide information to those who wish to do future studies as well as the benefit of this study will be for other banks which want to implement the Internet Banking system in the best secure way.

References

[1] http://my.safaribooksonline.com/9788131760291/ch17#X2ludGVybmFsX0h0bWxWaWV3P3htbGlkPTk3ODgxMzE3NjAyOTElMkZjaDAxNzAwMiZxdWVyeT0=

[2] http://ar.scribd.com/doc/28572119/Internet-Banking

[3] http://www.roseburg.k12.or.us/depts/tech/StaffDev/Int4Ed/Resources/www7.html

[4] http://www.tutorialspoint.com/web_developers_guide/web_basic_concepts.htm

[5] www.ibm.com/eg/pdf/me/redp4004.pdf

[6] Internet Banking, Comptroller's Handbook, October 2009.

[7] IT For Managers on Internet Banking, Sunil Chichra, 2010.

[8] http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=243

[9] http://www.lokstuff.com/UCB/ucb/security.html

[10] http://www.cisco.com/

[11] http://www.juniper.net/uk/en/

[12] http://www.dell.com/