Research Journal of Applied Sciences, Engineering and Technology 7(19): 4056-4063, 2014
DOI:10.19026/rjaset.7.766
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: November 20, 2013 Accepted: December 13, 2013 Published: May 15, 2014

Research Article

E-banking: Online Transactions and Security Measures

Hameed Ullah Khan
Department of Information Systems, College of Computer and Information Sciences,
King Saud University, Kingdom of Saudi Arabia

Abstract: This study presents the technology involved in the more important payment systems currently available to internet users. As the field is undergoing a major upheaval by changing the traditional banking services, e-commerce is facilitating change in recent years. These programs in-returns have shown lucrative growth in internet businesses and capital generation. Transactions on an international scale are the mark of highly demanding businesses with a global consumer base. Banks around the world provide their banking services online though electronic channels, one of the most widely used is the internet channel. Many people avail internet banking services which is convenient in this day and age. On-line banking platforms allow consumers to manage their accounts globally and at their convenience. The internet banking services have to be at top level of security and risk free in order to be trusted by customers. In this study the attack models have been explained and the top risks factors that the internet banking services come to face and applications have been discussed. This study deals with experimental models that can be applied to curb cybercrime attacks and make the internet banking applications more secure to the consumer strata.

Keywords: Internet banking, internet banking risks, internet banking services

INTRODUCTION

Online banking allows customers to make financial transactions on a secure website operated through their bank. On-line banking solutions have many features and capabilities in common, but traditionally also have specific applications. Almost all the banks in the world are providing the online facility that ranges from day to day transactions to account opening, issuing credit cards, paying and getting the loans and debts and providing customers facilities to shop online. Some banks are also providing the facilities to draw cash from their bank accounts online and they can pay their bills online (Asli, 2011).

The term “Internet Banking” or “e-banking” refers to the use of the Internet as a remote delivery channel for banking services. In other words and according to some resources, internet banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting bank branches. Such systems should enable banks’ customers to access their accounts, obtain information on financial products, transfer money and utilize other offerings (Humphreys, 2008).

“The advent and expansion of globalization and the development of new technologies forced the banks to launch new channels to gain a competitive advantage, reduce their costs, improve the quality of their financial services, increase their customer base, progress their financial positions through innovative products and boost their general customer loyalty”. For such reasons, banks should provide internet banking applications that facilitate their customers’ businesses at high level of trust, one major indication of trust is security, as banking matters are all based on security (Booz and Hamilton, 1996).

With the use of online banking, the user feels secure and can do it from their home/office and no need to go to bank time to time in physical. Just log in to the website of concern bank and enter your account number and make the payments. One can get access to all the services provided by the banks to perform the desire task. The services offered by the online bank are the same for a customer who is provided in physically interactions and on many occasions banks offer more in the online. Online banking feature seems best for performing their monetary action that they require. So the online service solves the customer's problems and save time for the customers. More people are using their services through the online banking because it is easy to access and save time for not waiting in queues to receive service. In fact, the customer can make transactions by simply clicking on the buttons of his computer. That is why the concept of online banking is getting better and better day by day as the demand and supply involves (Hiltgen *et al*., 2006).

The idea of paying for goods and services electronically is not a new concept. All around evidence of transactions taking place where at least part of the process is carried on electronically. Variety of schemes has been proposed to allow payment to be effected across a computer network. Few of these schemes got beyond the design stage since the schemes were of little use to those who were not connected to a network. With the arrival of the Internet has removed this obstacle to progress. This networks has grown dramatically from its inception today's truly global medium. It is not known how many people make regular use of the Internet (Hole *et al*., 2006).

In the early stages of the Internet evolution, it was common to make the assumption that each of these machines was used by around 10 people. This would mean that some 930 million people have Internet access worldwide. Most commentators would agree that this figure is much too high and have used a variety of other estimating techniques to arrive at a better answer. Internet survey takes an average of such estimates and concludes that just over 4000 million people were online around the world. Much of this growth has been driven by the availability of World Wide Web (WWW) technology that allows information located on machines around the world to be accessed as a single multimedia-linked document with simple point-and-click interactions. Surveys of Internet users suggest that the profile is changing from the original university-centered user base to a more broadly based residential population with a high spending power. These facts are not lost on commercial organizations wishing to offer goods and services for sale to a global consumer audience. Initially the focus of electronic commerce (e-commerce) was on selling goods to consumers. The most popular categories included computer goods and software, books, travel and music CDs. This so-called Business-to-Consumer (B2C) e-commerce grew spectacularly. It was estimated at $7.7 billion in 1998, $10.3 billion in 1999, $13 billion in 2000 to $47 billion in 2011 and $1 trillion in 2012 (US Retail Ecommerce Holiday Season Sales, 2011).

The industry focus began to shift to the trade that companies do with each other. By building on-line electronic marketplaces, it became possible to bring together businesses such as car manufacturers and their component suppliers, or fruit wholesalers with primary producers. This Business-to-Business (B2B) e-commerce is thought to have the potential to become considerably larger than the B2C sector and indeed some early estimates suggest that B2B e-commerce reached $226 billion worldwide in 2000 and is projected to reach $12.4 trillion by 2012. In both the B2C and B2B sectors, the Web was first used simply as a means of discovering products and services, with the payment being carried out off-line by some conventional payment method. In the case of B2C consumer purchases, merchants found they could capture credit card details from Web forms allowing the completion of the transaction off-line, albeit with a complete absence of security measures (Ecommerce Sales Topped $1 Trillion, 2012; E-marketer, 2001; Ismail, 2013).

A huge variety of different payment methods has been developed by researchers for commercial uses. Some of these were launched on the market and failed to reach a critical mass. Early market leaders such as First Virtual Inc., CyberCash Inc. and Digicash launched payment systems that achieved quite extensive deployment but failed to generate an economic return. The advent of B2B payments with their different requirements will give a greater impetus to payment methods that can cope with bank-mediated large-value transfers. A totally new market has also developed for people to make payments with the assistance of their mobile phone or hand held wireless device. Mobile commerce (m-commerce) has the potential to become a very large industry and many payment technology providers have appeared to fill this gap (Furst *et al*., 2000; Open Web Application Security Project, 2011).

LITERATURE REVIEW

Internet is bringing so much changing in peoples life that they can get whatever they think by sitting at home and without making any efforts. This is the benefit of using internet. We can see everything from home accessories to services, consultants, gaming to online selling are done through internet. You only need to type the key word which you require and get the results at glance. The same case is with banking. All the international banks and local banks have the online websites that provides services for their customers to get their banks from their homes. The customer can get online forms and you have to fill the form and submit all required information to open new account in the bank. When the customer has an online account with his bank, he deals with your other matters and using the available services to solve his problems (Open Web Application Security Project, 2011).

The online service solves customer's problems and he does not have to go the branch of the bank. The banks offer many services for customers as pay services bills as water and electricity. These features are useful for both the customer and the companies because it save a lot of time and reduce the number of the required employee to complete these transactions (Internet Host Count Maintained by the Internet Software Consortium, 2011).

The bank has great benefits from the online banking; the bank can reduce the number of employees and the number of opened branches to offer services to customers. The customer use the online banking to request service from the bank and the bank employee receive and process the customer's requests (Nua Internet Surveys, 2001).

Advantages of online banking: Following are advantages for online banking: comfortability; where you can end your transactions remotely and quickly at any time, they are available 24 h a day, seven days a week. Second advantage is availability; if you are outside the country, you can work all your transactions, you can log in to the system as it is available 24 h. Third advantage is high speed processing; e-bank sites on the Internet provide the speed and confirm the termination of the transaction, faster than ATM. Fourth advantage is effectiveness; e-banking sites provide all the services, checking accounts, money transfers, bill payments and other services. Fifth advantage is reliability; a user or customer is doing all transactions with confidence (Pitkow, 1997).

Disadvantages of online banking: Following are disadvantages for online banking: negotiation time; need to take the consent of the bank and fill out the forms and signed and on-site registration this process is time consuming. Second disadvantage is confidence; some people do not want to use electronic transactions, as they believe that the use of papers is more authentic. Second disadvantage is application software are not friendly user; some customers, especially the older have problems in using software (Koskosas, 2011).

INTERNET BANKING ATTACKER MODELLING

Internet banking applications can be attacked with different intensity, skill and persistence and these elements are usually correlated with the profile of the human behind the attack. The bank should decide which types of attacker it expects to be more likely than others and focus on defending against these types. Attempting to defend against all categories of attackers may well lead to unnecessary expenditure.

Opportunistic attacker/malware: This type of attack agent attempts to carry out preprogrammed attacks and is limited by the level of intelligence that can be implemented into software at the present date. It is thorough, quick and precise, but can't cope often with unfamiliar circumstances and does not apply intuition or ingenuity to the attack. It targets an entire population of online targets and swiftly moves from one target to the next should the attacks not succeed. It will typically focus on stealing credentials and credit card numbers; and will often try to hijack a system into joining a botnet, putting its network bandwidth and computing power in the service of the botnet controller. The botnet controller can then use it to send spam, launch distributed Denial of Service attacks (DoS) or break cipher text or passwords using brute force attack. The motivation is usually either financial or the creation of mayhem (Open Web Application Security Project, 2011).

Organized crime: Distinguished mainly by their motivation, these attackers are knowledgeable in security and adaptive to the point of creating custom tools for their attacks (including targeted malware). Security researchers may be motivated by the challenge of overcoming obstacles or by the desire to blow the whistle, while criminal elements are motivated by financial gain and supporting real-life criminal activities (organized crime). Their targets are typically singled out among their peers and the attackers persist in attacking them beyond any initial difficulties. Offline components such as bribes and social engineering can be part of the attack mix. A serious impact of criminal element attacks is corporate espionage, in which there is an agenda of specific information assets to be targeted (Mu, 2003).

Insiders/disgruntled employees: While they may not be highly skilled technically, this class of attackers has the advantage that they start "from the inside", with a certain level of privileges and prior knowledge. Their motivation is usually either greed or retaliation for perceived injustices. They tend to persist beyond initial setbacks. Disgruntled employees will often aim for leaking confidential information or for data destruction; two ways in which they can harm the organization's interests. Most of internets banking attacks are coming from this type (Schneier, 2005).

State-level attackers: With considerable resources and skills at their disposal and applying a planned, thorough and systemic approach with patience, this type of attacker is the most difficult to defend against. The attacks will blend as necessary offline components such as bribes, infiltration of the target organization, interrogation and military action. The actors carrying out the attacks usually benefit from political and legal protection. Unfortunately large numbers of this kind of attacks have been succeeded in targeting their targets (Schneier, 2005).

Denial of service: The Denial of Service (DoS) attack is focused on bringing down application, service or website for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may stop providing service to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources are used. Sometimes the attacker can inject and execute arbitrary code while performing a DoS attack in order to access critical information or execute commands on the server. Denial-of-service attacks significantly degrade service quality experienced by legitimate users. It introduces large response delays, excessive losses and service interruptions, resulting in direct impact on availability. For the internet baking, this model of attacks is being used widely in an organized crime way. This type of attacks model can be generated easily and internet banking applications exposed for such attack. Hence, such model of attack needs to be detected and resisted in a dynamic way (Open Web Application Security Project, 2011).

Phishing: Phishing is the process of acquiring sensitive information such as usernames, passwords, credit card details and sometimes, indirectly, money by masquerading as a trustworthy entity in an electronic communication. This type of attacks is the most spread one these days since it is has many way to capture the victim information. Each day coming, attackers invent new way of phishing attacks and then phishing become mercurial way of attack. Phishes are trying to capture the customer username and password in order to maliciously access customers' banking accounts. One way of phishing is to develop a site that looks like the original bank site in look and feel matter and ask the customer to login to his bank profile. Once the customer enters his username and password, the attacker's site stores them and displays an error message apologizing for being unable to access the profile. Hence the attacker succeeded in stealing victim's credentials (Schneier, 2005).

Internet banking risks: According to The Open Web Application Security Project (OWASP) organization, the security risks on the web applications have been rated according to successful attacks happened and hereunder the most risks announced in 2010, how attack might occurs. Following are the risk reported with little description of each given below (Open Web Application Security Project, 2011).

The first type of risk is: injection flaws; such as, SQL (Structured Query Language), OS and LDAP (Lightweight Directory Access Protocol) injection occur when un-trusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data. The second type of risk is: Cross-Site Scripting (XSS); occur whenever an application takes un-trusted data and sends it to a web browser without proper validation and escaping. The XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. The third type of risk is: Broken Authentication and Session Management (BA&SM); the application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities. The fourth type of risk is: Insecure Direct Object References (IDOR); direct object reference occurs when a developer exposes a reference to an internal implementation object, such as, a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data. The fifth type of risk is: Cross-Site Request Forgery (CSRF); a CSRF attack forces a logged on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim. The sixth type of risk is: Security Misconfiguration; good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server and platform. All these settings should be defined, implemented and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application. The seventh type of risk is: Insecure Cryptographic Storage (ICS); many web applications do not properly protect sensitive data, such as credit cards, SSNs and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes. The eight type of risk is: Failure to Restrict URL Access**;** many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway. The ninth type of risk is: Insufficient Transport Layer Protection (ITLP); applications frequently fail to authenticate, encrypt and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms; use expired or invalid certificates, or does not use them correctly. Lastly, the tenth type of risk is: Invalidated Redirects and Forwards; web applications frequently redirect and forward users to other pages and websites and use un-trusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages (Dean and Widrig, 2012).

SECURITY FOR ONLINE BANKING SITES

Before developers start writing code, the architects and designers establish the blueprints of the software. Already at this stage high level security flaws can be avoided or remedied and it is the stage at which course corrections are cheapest. The high-level decisions should be documented and made available to the other stages of building the product and they should be updated throughout the process. The following high-level security should be considered and applied throughout the lifecycle of a computer system, to help ensure that security flaws can be avoided.

Do not trust user inputs: The user interface should be considered as a key trust boundary because the end-user may be malicious, prone to errors, or manipulated by another malicious party. In the case of internet banking applications the user interface is often considered as between the web browser and the user, but from a security perspective the main trust boundary is between the web server and the network (e.g., internet). This is because it must be assumed that the end-user's browser or computer can be under control of an attacker, through any of a variety of technical methods (e.g., browser extensions, installing an intercepting web proxy between the browser and the Internet). Even if the user is honest, an attacker may have succeeded in inserting themselves into the communication channel and may be intercepting and changing traffic at will. The requests arriving to the web server need to be considered as malicious until proven innocent and the web application needs to be prepared to handle any request. Input validation must be used to confirm that any assumptions about the requests are indeed true (Harris and Laura, 2002).

Fix security issues correctly: When a security issue is brought to light it should be addressed at three levels: first; the software product level: the issue should be fixed in the locations where it was found. This will presumably make that instance of the software safe from that problem. Second; the development process level: since the issue has arisen in a product, the development process is not protected against it. The issue should be searched for and fixed everywhere in the code and safeguards should be placed in the development process to prevent this issue from reoccurring again in products. Third; the organization level: not only should this kind of issue never make it into a product, but it should never make it into the source code. Development guidelines should be updated to reflect the correct way to prevent the issue, the developers should be trained and third party suppliers should be evaluated by their susceptibility to introduce this kind of issue (Ivar, 2012).

Establish secure defaults: Software products are in general very versatile. Part of their value proposition is that they can be customized and optimized for each user's needs. However, this often requires an effort from the user to learn how to configure the software and an effort to determine the optimal configuration for them. Software with a high learning curve (or where the search for optimality is not easy) discourages users from spending that effort and so many settings remain unchanged from their default values. The consequence is that a large proportion of deployed software products are in their "out-of-the-box" state. Because of this reality it is important that the default settings should provide at least some basic commonly expected security requirements (e.g., not allowing everyone administrative access to the system, keeping credentials confidential, ensuring separation between users), so that users aren't unknowingly exposed to unnecessary security risks. Secure defaults may clash with the marketing of the software, as they often decrease the quality of the user experience. Developers need to make the software easy to use even in its secure state and marketers need to understand that attackers have access to the defaults simply by obtaining a copy of the product. They can then proceed to attack it until they succeed, assured that lots of other instances with the same configuration are deployed in the world (Mu, 2003).

Least privilege: At every granular level of an internet banking application (role, process, module, transaction) the entity that executes an action should have the necessary privileges to carry out that action, but little more. Less privilege than necessary and the application would have a functional defect because a legitimate action cannot be carried out. Often a security breach takes the form of a component being subverted into doing something else other than its normal function. If the component has no more privileges than necessary, even then an attacker manages to subvert it the attack will fail for lack of sufficient privileges (Robert *et al*., 2013).

Clean up production code: During development auxiliary code may mixed in with the application's code, either for debugging purposes or during exploratory programming. This code should be removed before the code goes into production because: first; if it is active code (as opposed to commented out, or on code branches that are never taken) then it was probably developed to a lower standard of security, which means it is more susceptible to attacks. Secondly; auxiliary code tends to take shortcuts, for which it is given more privileges than necessary. When active, if an attacker manages to subvert the auxiliary code, the attacker may be able to cause more damage. Thirdly; even inactive auxiliary code can find its way into a production environment. Not all compilers optimize dead code and comments out of the binary artifact. Interpreted languages tend to ship the auxiliary code together with the useful code. In these cases they may disclose useful information to the attacker through developer comments, deactivated links that allow for hidden files to be discovered, or other forms of internal information disclosure (Harris and Laura, 2002).

PROPOSED APPROACH

The proposed approach is divided into two sections. In the earlier section the data movement is explained through flow chart and in the later section its logical implication is given in detail.

System flow chart: In the proposed approach the data entered and passes through different authorization stages as shown in Fig. 1.

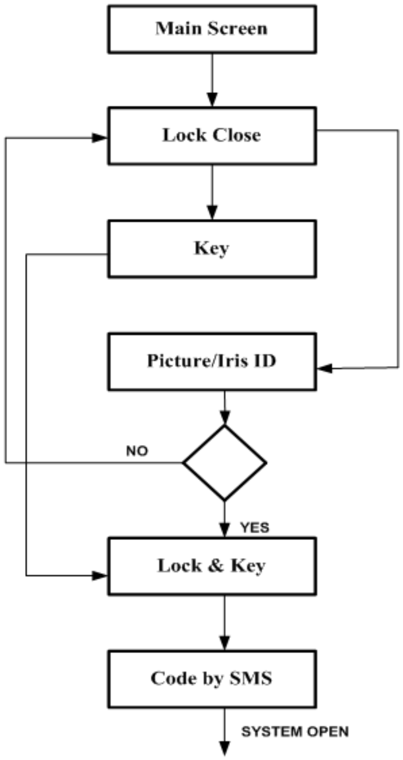


Fig. 1: Flow chart for proposed system

When the system is going to be operated the front page will appears as the main screen of the system. The second step is to feed user id to start process for lock close, which is followed by a password as a key for authentication. In the database the user already placed at the time of registration any mark of identification in the shape of either picture or iris for the purpose of matching. If the match is found correct then the combination of lock and key will confirm and the system will be allowed to open but not yet granted authorization until the six digit code is feed.

Design and implementation: This section presents the proposed approach by considering modern trends and technologies. The process of authentication of customer starts from the username and followed by password by putting each one in a separate page. The customer inserts his username first before his password as shown in Fig. 2.

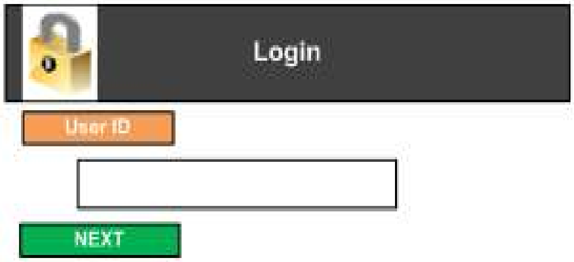


Fig. 2: First page that asking for username

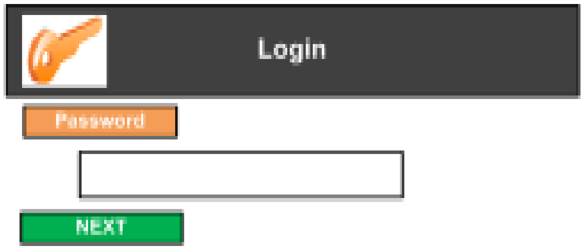
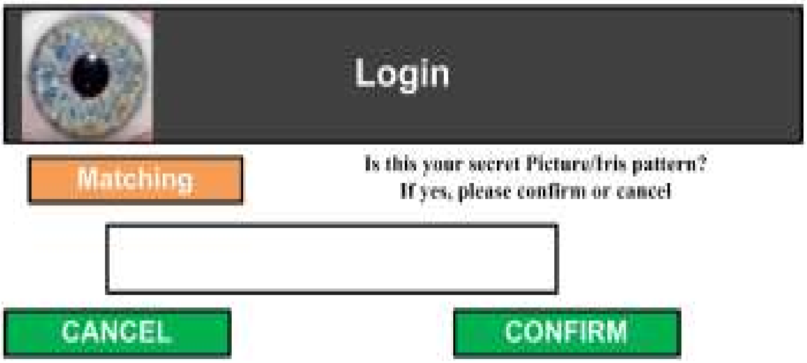


Fig. 3: Second page that asking for password

There is no use of card, as many problems are associated with cards, such as, lost, scratches, insertion, etc. The customer will enter his password as shown in Fig. 3.

After second step the internet banking application will ask the customer to proceed to third page by entering the secret picture/iris pattern, showing the matching process what the customer selected earlier during the time of his/her registration process, as shown in Fig. 4.

The customer will assure that the site is the bank site with sensitive data and will enter the combine the lock and key for the account to lock open, as shown in Fig. 5.



Is this your secret Picture/Iris pattern?
If yes, please confirm or cancel

Fig. 4: Third page that display the secret picture/iris pattern

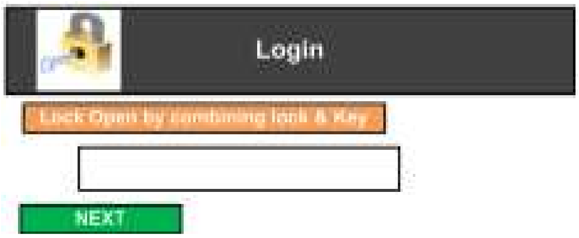
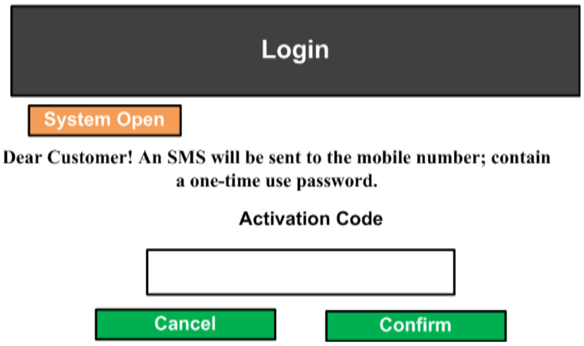


Fig. 5: Fourth page that combine lock with key



Dear Customer! An SMS will be sent to the mobile number; contain a one-time use password.

Fig. 6: Fifth page one-time password through SMS

To prevent phishing it is proposed to use second factor for authentication to ensure the customer entity. One common way is to send one-time password through SMS to the customer's mobile. The customer should enter this one-time password through the bank site to assure this is the real customer that has the same picture, password and physical mobile. This one-time password should be for one time use and should be valid for a short time, shown in Fig. 6.

It is notice that the picture/iris approval and followed by lock and key combination and by sending the one-time password, which might slow down the processing of the system. But here security is the prime concern not the time.

CONCLUSION

The proposed system will help the customers for using the internet for their business. The online banking helps every one for better services on the cost of security. The system allows customers to transfer money, account inquiry and get the balance sheet and many other services. Besides, the idea to get the cash money is also possible. In that case a portable ATM services which will help handicapped, VIP customer and those who are living in remote areas. They do not have access to branch of the bank can be facilitated by providing services. In contrast if customers hire specialized companies to transfer amount to beneficiaries, is not safe. Places are far from banking services; where bank can not cover remote population but through the mobile services and ATM, which permit customer cash withdrawals, etc.

In large transactions particularly at a distance, customer does not need to go to the bank. From the service point, the bank is going to charge certain amount for the services but will provide the facility. Since technology is undergoing a major upheaval, by using m-commerce. Further, such system is time consuming and extra cost for the bank especially if the bank has too many customers. But here the main concern is security to save customers from big disasters. Hence, the minor overhead can be ignored.

RECOMMENDATIONS

We hope that in future services to customer are going to be more enhance. This will be possible by making it easier and using smart phone. It's not only the reason that the use of smart phone is easier, but it keeps up with the new trends and technology. Also, the futuristic expectations are to develop more banking service to help community living in remote area, where the access to bank is not possible or the customer is old enough to reach their physically.

ACKNOWLEDGMENT

I am grateful to the Research Centre (RC), College of Computer and Information Sciences (CCIS), for extending me all support during this research study. I am also thankful to all those who contributed in any form to make this research successful.

REFERENCES

Asli, Y., 2011. Customer's perspectives and risk issues on e-banking. J. Internet Bank. Commer., 16: 1.

Booz, A. and I. Hamilton, 1996. Internet Banking: A Survey of Current and Future Development. Financial Services Group, New York.

Dean, L. and D. Widrig, 2012. Managing Software Requirements: A Use Case Approach. Addison-Wesley, Boston.

Ecommerce Sales Topped $1 Trillion, 2012. Retrieved form: http:/ /www.emarketer.com/ Article/ Ecommerce-Sales-Topped-1-Trillion-.

E-marketer, 2001. The E-Commerce: B2B Report. Retrieved form: http://www.emarketer.com.

Furst, K., W.W. Lang and D. Nolle, 2000. Internet banking: Developments and prospects. Office of the Comptroller of the Currency Economic and Policy Analysis Working Paper No. 2000-9.

Harris, L. and J.S. Laura, 2002. The ethics of e-banking. J. Electron. Commer. Res., 3(2): 59-66.

Hiltgen, A., T. Kramp and T. Weigold, 2006. Secure internet banking authentication. IEEE Secur. Priv., 4.2: 21-29.

Hole, K.J., V. Moen and T. Tjostheim, 2006. Case study: Online banking security. IEEE Secur. Priv., 4.2: 14-20.

Humphreys, E., 2008. Information security management standards: Compliance, governance and risk management. Information Security Technical Report, pp: 247-255.

Internet Host Count Maintained by the Internet Software Consortium, 2011. Retrieved from: http:// www.isc. org/.

Ismail, S., 2013. Factors affecting the adoption of B2B e-commerce technologies. Electron. Commer. Res., 13: 199-236.

Ivar, J., 2012. Object Oriented Software Engineering, Addison Wesley. Retrieved form: Designing Web Interfaces: Principles and Patterns for Rich Interactions.

Koskosas, I., 2011. The pros and cons of internet banking: A short review. Bus. Excellence Manage., 1: 49-58.

Mu, Y., 2003. E-banking: Status, Trends, Challenges and Policy Implications. Retrieved from: SSRN: http://ssrn.com/ abstract= 485343 or DOI: 10.2139/ssrn.485343.

Nua Internet Surveys, 2001. How Many Online? Retrieved form: http://www.nua.ie.

Open Web Application Security Project, 2011. Denial of Service. Retrieved form: https:// www. owasp. org/ index. php/ Denial_of_Service.

Pitkow, J., 1997. The WWW User Population: Emerging Trends, GUV Centre, Georgia Institute of Technology, Atlanta, GA.

Robert, M., D. Alan and H. Barbara, 2013. System Analysis and Design. 4th Edn., Wiley, Hoboken, NJ.

Schneier, B., 2005. Two-factor authentication: Too little, too late. Commun. ACM, 48(4): 136.

US Retail Ecommerce Holiday Season Sales, 2011. Retrieved form: http: //www-958.ibm.com/ software/analytics/manyeyes/datasets/us-retail.