# A Survey on Online Banking System Attacks and its Countermeasures

**Navjeet Kaur**
Rayat Bahra Group,Kharar, Punjab, India.

**Summary**
The major concern while using internet is the security of the transmitted and the stored data. The proposed system will provide a solution to the security and the problems of the centralized database system. To achieve this task, the concept of distributed database and cipher text will be used. In distributed database portions of the database are stored on multiple computers within a network. Users have access to the portion of the database at their location so that they can access the data relevant to their tasks without interfering with the work of others. Cipher text is encrypted text i.e. the original text is converted into unreadable text using some algorithms so that unauthorized user could not get access to the information. Most systems are based on the concept of centralized single database. The centralized database acts as the backbone of the whole system. If the centralized database gets failed, whole of the system crashes. Moreover the data stored in the database is stored as plain text. If anybody gets access to the centralized database, the information could be easily retrieved. Secured transmission of data is a wide area of research in networking as data is the most crucial element of any organization also the risk of getting the information leaked or hacked these days has also increased. The Paper is divided into five Section which include introduction in the first section , review of literature with several attacks explanation in second section, third section explain some countermeasures to overcome different problems. Finally, we end up our paper with a conclusion and future scope.

***Keywords***
*Cipher text, Data encryption, Distributed database, Enhancing security, Secured transmission.*

## 1. Introdution

Security in computer systems is strongly related to the aspect of dependability. A dependable computer system is one that we trust to deliver its services. Dependability includes availability, reliability, safety, and maintainability. However, if we are to put our trust in a computer system, then confidentiality and integrity should also be taken into account. Confidentiality refers to the property of a computer system whereby its information is disclosed only to authorize parties. Integrity is the characteristic that alterations to a system's assets can be made only in an authorized way. In other words, improper alterations in a secure computer system should be detectable and recoverable. Major assets of any computer system are its hardware, software, and data.

### 1.1 Online Banking System

Online Banking System is a service for customers to do financial transactions. Online banking implements software that allows customers to access information regardless of where the customer is located. A unique aspect of online banking software is that it is able to track different transactions (deposits, withdrawals, transfers, etc.) and when these transactions take place. By creating an online banking system, customers have unique access to utilize all of the unique features anywhere without having to physically go to the bank. In addition customers are able to receive a comprehensive over view of their finances and actively engage in various transactions such as transferring of funds.

### 1.2 Vulnerabilities in online banking system

Table 1 presents known vulnerabilities which affect each security mechanism developed by various organisations. The correct identification of the threats faced by the current Internet Banking Systems is essential for designing more efficient models which provide higher level of security.

Table 1: vulnerabilities in online banking systems [1]

| Security Mechanism | Vulnerabilities |
|---|---|
| Digital Certificates | It is possible to export A1 certificates and remotely utilize them; A3 certificates can be used by more than one user at the same time, allowing adversaries to use stolen certificates. |
| OTP Token | The generated password may be captured and used in real-time; The user may be lured into informing the password for unauthorized transactions through the use of social engineering. |
| OTP Card | Malware may collect passwords or lure the user into informing them. |
| Browser Protection | New malware remain active util they are identified by the model; Counterfeit online banking system web pages which prevent the protection from properly loading can be used to make the user input his sensitive data (such as passwords) in an unsafe environment. |
| Virtual Keyboard | Known tools such as Screenloggers or mouseloggers may capture sensitive information; Decryption techniques and attacks focused on flawed encryption algorithms can also be applied. |
| Device Registering | Characteristics thought to be unique to the user's device may be reproduced; Information regarding the device's register can also be reproduced. An attacker can apply social engineering to persuade the user to authorize and register a malicious device. |
| CAPTCHA | The methods applied to scramble the information in the image are too simple, making it possible to extract the desired information using OCR software. |
| Short Message Service | The attacker may alter the cellular phone number to which the authorization messages are sent. |
| Device Identification | Characteristics thought to be unique to the user's device may be reproduced. |
| Positive Identification | Information thought to be only known by the user may leak in the Internet and social engineering techniques may be used to discover such information. |

Manuscript received March 5, 2015
Manuscript revised March 20, 2015

## 2. Review of Literature

In online banking system customer's information is the most crucial element to be secured. The user is the most delicate link in the whole system to be attacked. As the whole system of online banking is provided with the highest security as even a small attack could bring the whole system down which could cost unexpected. In online banking system the bank's server is equipped with the highest security level techniques, so the bank server is less prone to attacks [1]. But the database of the bank is not kept on single server in the distributed database technique. The database is kept in parts over the network on different computers. So in case of distributed database the security concerns get increased as these are more vulnerable to the attacks. The user is the most delicate and often targeted link. User is the weakest link in the whole system as a layman user could never understand the security threats and attacks.

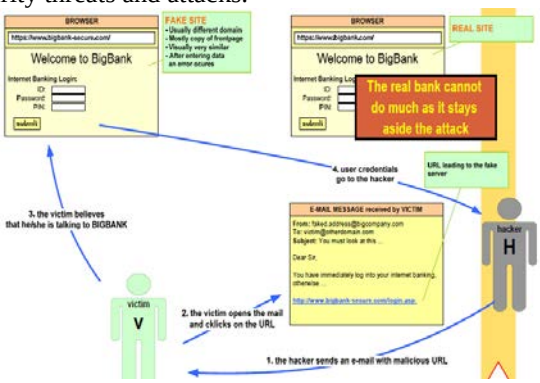


Figure 3: Online banking attack [2]

Attacks on the bank's server are mostly unsuccessful but the most common attack is Denial of Service attack. This attack refers to such a condition when the resources are not available to its intended users. It is done by flooding the network with requests. It can also simply refer to a resource, such as e-mail or a Web site that is not functioning as usual.

The user has the authentication information of his account which is the main target of the hacker. It can be hacked by using Credential theft, Social engineering, phishing, pharming and man in the middle. In credential theft the personal information of the user which is used for authentication of the account is stolen. The success of this kind of attack depends upon the type of authentication used [2]. The credential theft uses malicious software to steal the information from the users. The malicious software is used to disrupt the normal operations of client's computer and gather sensitive information. These are also known as malware. Malware can be in the form of code, scripts or software.

Social engineering is one of the mostly used methods to intrude the security [3]. In this kind of attack mostly layman users are targeted. It relies heavily on human interaction and tricking other people to break in the security. A person using social engineering to break in the security must try to gain the confidence of the user first. Social engineers rely on general helpfulness of the people also on their weaknesses. Another aspect of social engineering relies on people's inability to keep up with a culture that relies heavily on information technology. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it. Social engineers search dumpsters for valuable information, memorize access codes by looking over someone's shoulder or take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed. Social engineering requires less technical knowledge but require more tricks.

Phishing is a method of gaining access to user name, password, credit card number and other confidential information [3]. It is carried out by generally sending e-mails containing malwares. The user is lured into a fake website which looks like the original one and is told to login. When user login onto that fake website, the confidential information gets lost. Phishing uses a fake website, actually not whole website but only login page which is similar to the original website. The link to that webpage is provided with the email which is sent to the user. If user login into that fake webpage, the personal information gets hacked. Suppose you check your e-mail one day and find a message from your bank say BigBank [3],[4]. You've gotten e-mail from them before, but this one seems suspicious, especially since it threatens to close your account if you don't reply immediately. This message and others like it are examples of phishing, a method of online identity theft. In addition to stealing personal and financial data, phishers can infect computers with viruses.

The difference between fake site and original site is that the domain of the fake site is different and mostly after entering the information an error occurs. Pharming is similar to phishing but an advanced technique.

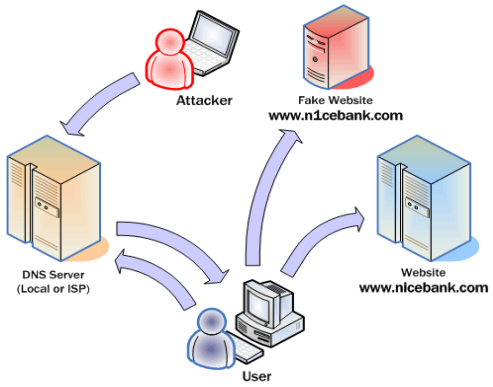


Figure 4: Example of Pharming[5]

In pharming DNS reconfiguration is used. For this purpose malicious software like Trojans and viruses are used. The user is lured into a fake website containing malicious code and Trojans. Man in the middle uses Trojan horse to be installed on the client's machine. It could be done by social engineering or phishing. Once the Trojan horse is installed on the client's machine the user when enters the URL of the original website Trojan does not allow to connect via a secured connection, the unsecured connection is followed and the confidential information gets hacked.

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. These hacking tools can easily capture the password, account number, and personal data which the user is inputting. 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 stages during the online banking process as shown in Figure 1.

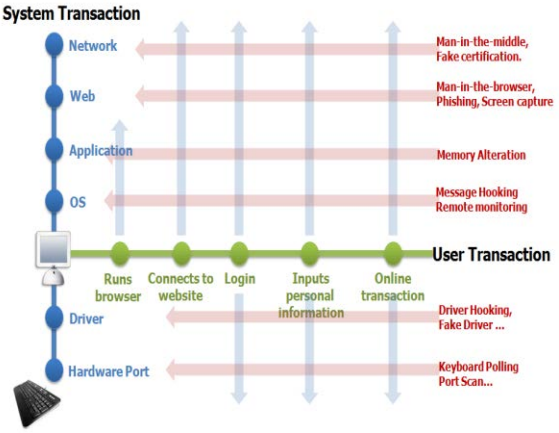


Figure 1: Spreading Threat through various stages of the transaction[7]

One of the examples is the Man-in-the-Browser Attacks that redirect the end user to fake 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 [8]. 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. 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 file3, 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.

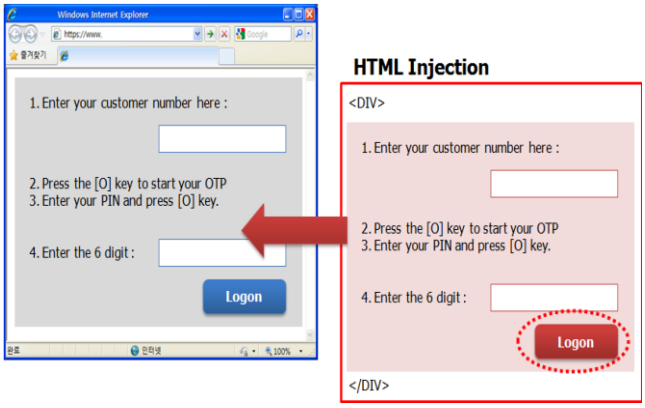


Figure 2: Fake log-in through HTML Injection [9]

Most of the attacks directed at online banking systems target the user (the weakest link in the chain), focusing on obtaining authentication and identification information through the use of social engineering and compromising the user's Internet banking access device in order to install malware which automatically performs banking transactions, apart from obtaining authentication data. This fact indicates that secure internet banking systems should provide security mechanisms as user independent as possible, mitigating the risk of user related information leaks and security issues affecting the system and leading to fraud.

In face of the current security issues and the growing number of attacks and consequent frauds, new internet banking systems should be designed as to provide better authentication and identification methods which are less dependent on the user. The basic characteristics of such methods are introduced based on the analysis the methods currently employed. A internet banking systems with those characteristics will render the presented attacks (and other attacks) ineffective, significantly decreasing the number of observed frauds.

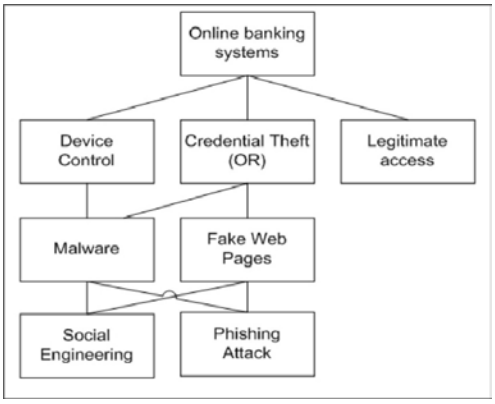

Figure 5: Attack Tree model[10]

The attack tree model for common attacks against online banking systems is presented in Figure 9. This model represents the main components of banking systems authorization and authentication mechanisms and efficient attacks against them. The attacks exploit vulnerabilities inherent in the people (engineering social and phishing) then to gain control of device (malware) and credential theft legitimate user (fake Web pages and malware).
The attacks description in this section is based on current trends observed in malware specifically focused on banking. It has been observed that such attacks are efficient against the authorization and authentication schemes currently adopted in online banking systems.

## 3. Countermeasures to Threats

Online banking is carried out through a series of transactions in various environments between the end user and the system, and these transactions are always vulnerable to complex, multi-faceted attacks from hackers. In the final analysis, a solution that does not understand the specific techniques involved in particular attacks as well as the entire process of online banking transactions cannot provide countermeasures to block the many faceted attacks from hackers. We must protect end users of online banking with a multi-faceted security solution that understands all the trends of hacking and combines all the technologies that can ensure security for end user's data input, security for web browsing, as well as security for the network used.

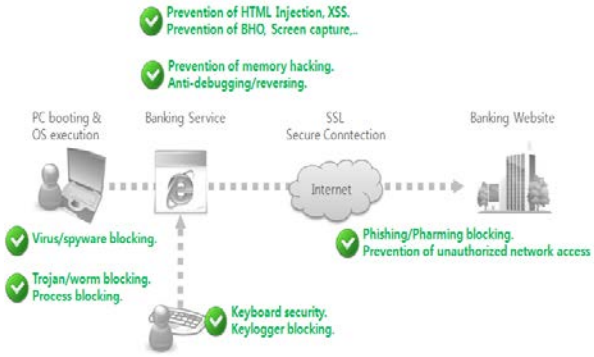


Figure 6: Secure technologies protecting every stage of the online banking transaction [8]

### 3.1 Anti-key logging Technology

To protect keyboard input values, each and every segment of the entire system must be protected, as illustrated in Figure 9, starting from the end user's keyboard input to what is saved in the memory of the web browser and what is finally reported on the screen. For keyboard security, the solution must be able to detect everything not only in the kernel level key logging but also in the user level key logging.

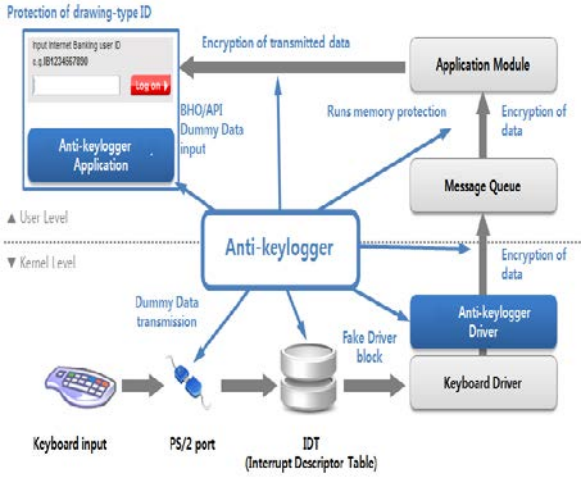


Figure 7: Anti-key logger protects every stage of the transaction carried out during keyboard input (PS/2 illustrated) [8]

At the kernel level, it is possible to protect the input values only when the input values from the port to IDT, from the port to Driver are encrypted. . At the user level, hooking should be detected in each stage of the process, and the memory must be protected. In addition, a sophisticated technology must be applied which can show only the dummy data that would be meaningless when it is captured through BHO6 or API of the browser

### 3.2 Anti-Hacking and Network Security Technology

A security technology that blocks threats to online banking in advance by blocking illegal intruders and outside hackers. This security solution must block intruders not only on the user's level but also on the kernel level, blocking or removing in real time the worms and trojans that are already known through the signature that is updated continuously. To cope with threats that are yet unknown, we must recompose the online banking environment and block illegal network communications through a particular program or processor.

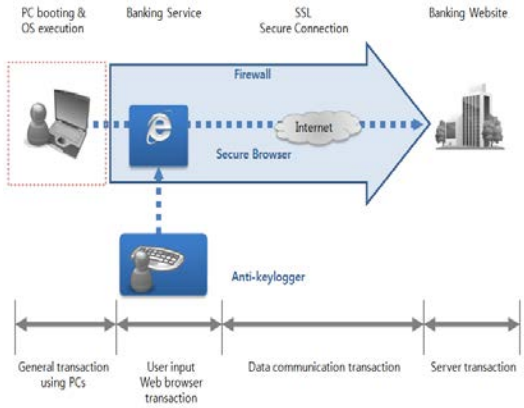

Figure 8: Secure, safe and reliable electronic financial transaction environment [10]

To sum up, the online banking service should always be ready to ward off the complex and organized hacking with a keyword inputting security technology, a web browser security technology, and a hacking tool blocking and network security technology.

## 4. CONCLUSION

With the explosive spread of the Internet, electronic financial transactions such as online banking have become a universally accepted common practice. Unfortunately, electronic financial transactions as such are offering a new revenue model to organized hackers. While innovations in security measures for electronic financial transactions are urgently called for, the conventional communication security measures through authentication like OTP and encryption using SSL are no longer satisfactory countermeasures for all transactions of online banking.

Because of these changes, a safe online financial transaction service has become an absolute requirement. Safe online security service is a new directive critical in the evaluation of the competitiveness of an online banking service. Accordingly, banks are obligated to provide safe online banking environments equipped with advanced and integrated online security. The general approach used these days for storing data of any organization is using a database server. This database is centralized database with some minimal distribution criteria. Every client who wishes to retrieve information has to communicate with the centralized database. The main problem that occurs with this system is that if the centralized database site fails or goes down whole of the system fails. So the centralized database acts as a backbone of the whole system. Secondly, cost of communication with the remote database server also increases if the central database server lies in remote area. Thirdly, with advent of technology, the risk of getting crucial data hacked has also increased. As data is the most important asset of any organization, so it is very important to secure the data while it is being transmitted over a network. As the data in the database is stored as plain text and there is generally one single file of every database which contains all the information, it could be easily hacked and data is retrieved.

## 5. FUTURE SCOPE

Our Future work will be based on designing an web application with distributed database. Use of Cipher text and its related algorithm like RSA, MD5, DES for encrypting database information. Designing and developing a application using advanced java features like session management, hibernate, generics etc to secure the input and output information. Further, implementing a system with three tier architecture to enhance security.

## REFERENCES

[1] Laerte Peotta, Marcelo D. Holtz, “A formal classification of internet banking attacks and vulnerabilities”, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 1. Feb 2011

[2] Prakash Kuppuswamy, “Enrichment of security through cryptographic public key algorithm based on block cipher”, ISSN : 0976-5166 Vol. 2 No. 3., 2011.

[3] Shiv Shakti Srivastava, Nitin Gupta,(2011) “A Novel Approach to Security using Extended Playfair Cipher”, International Journal of Computer Applications (0975 – 8887)volume 20– No.6, April 2011.

[4] Suhair Alshehri, Stanisław Radziszowski, and Rajendra K. Raj, “Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption,ACM Digital Library”, IJCS, 2011

[5] Anand K. Tripathi, Monika Tripathi, “A framework of ditributed database management systems in the modern enterprise and the uncertainties removal”,Volume 2, Issue 4, April 2012 ISSN: 2277

[6] Nikos Moshopoulos and Eleftherios Chaniotakis,” A Survey of Cryptography Algorithms – Trends and Products”, IJCS, 2010

[7] Thomas Hardjono nad Jennifer Seberry,” A Multilevel Encryption Scheme for Database Security, IJCSI,2009.

[8] Fuad Al-Yarimi, Sonajharia Minz,” Multilevel Privacy Preserving in Distributed Environment using Cryptographic Technique”, WCE 2012.

[9] Masashi Une and Masayuki Kanda,” Year 2010 Issues on Cryptographic Algorithms”, 2011.

[10] G. Dalton, R. Mills, J. Colombi, and R. Raines, "Analyzing Attack Trees using Generalized Stochastic Petri Nets," 2006 IEEE Information Assurance Workshop, 2006, pp. 116-123.

**Navjeet Kaur** currently working as an Assistant Professor in Rayat Bahra Institute of Engineering and Biotechnology Kharar Punjab. She received her B.Tech degree from Shaheed Udham Singh College of Engg and Tech, Tangori (Mohali) and M.Tech degree from Indo Global College of Engg and Tech, Abhipur (Mohali). Her research interests include parallel computing, security system, high performance computing etc.