Internet Security Impact on E-Banking Users

Mohammed Khodayer Hassan[a], Ali Hassan[b], Aymen Mohammed Khodayer[c], and Omer Mohammed Khodayer[d]

[a] *Al-Rafidan University, Department of Computer Science, Baghdad, Iraq*
[b] *Institutes for post graduate studies, Iraqi commission for Computers & Informatics, Baghdad, Iraq*
[c] *Al-Farhidai University, Head of the Department of Communication Engineering Baghdad, Iraq*
[d] *Polteckina University of Bucharest, the Department of Telecommunication Engineering, Bucharest, Romaine*

Abstract

Information technology has been used widely in different sectors in daily task to fulfill Customers and organization's needs. Banking business is one of the main trends that use information technology in wide range. Customers can deal with banks through Websites which E-banking or using a credit card at an ATM what it is called. One of the most important factors in the success of electronic banking services is security. A strong security system is critical for a safe banking system in order to prevent hacking of the client's banking account and any private information of the customers in the bank system's databases. Any of the tasks can only be performed by legal or authorized personnel. As a result, bank systems must ensure that their transactions run as they should, in a secure manner, and that no activities occur that could result in a loss to the bank organization and its clients or customers. Banking account hacking has resulted in millions of dollars in losses in the wild world due to security system vulnerabilities. That kind of paper discusses the attacks on the banking system, the importance of the robust security system and the security measures that have been taken to prevent a great lost to the financial institution. Recommendations have been made to prevent any intrusion in the future. This paper shows the security trends to word helping customer and banks in their works to get better performance in doing their jobs by using electronic banking system.

Keywords

E-banking systems, authentication, confidentiality, intrusions of banking system.

1. Introduction

Banking transaction can be done efficiently at nowadays technology and this will satisfy the needs for customers. Online banking has improved the services that are offered by the bank to their clients. Clients can conduct various electronic banking transactions via the internet at anytime and anywhere, no need to stand on queues to perform financial needs. On line banking has given different names, internet banking, electronic banking, tele-banking, web banking, and self-service banking. All these names have the same jobs and have on line access to the banking system. Customers can perform their paying bills, transferring money, withdrawing money and checking account [1]. The information that is used by bank belongs to different institutes and it belongs to different customers. They have to be in safe, no one can access them without permission of the owner. Intruders can carry out an intrusion for any reason, from tampering with personal data to stealing money from financial institutions. Any failure or damaged caused by this intrusion may lead to great losses for the financial institute. The miss trust between the customers and banks might take place and due to those events the performance of the bank will be affected accordingly in the negative aspect. In USA, the government requires banks to report all losses, while banks wouldn't like report losses and avoid publicity. Reporting losses are considered

Emerging Technology Trends on the Smart Industry and the Internet of Things, January 19, 2022, Kyiv, Ukraine
EMAIL: mohammed.khudhaer.elc@ruc.edu.iq (M. K. Hassan); alihtaresh@uoitc.edu.iq (A. Hassan); aymenaldulaimi@uoalfarahidi.edu.iq (A. M. Khodayer); aldulaimiomer187@gmail.com (O. M. Khodayer)
ORCID: 0000-0003-0283-9443 (M. K. Hassan); 0000-0002-8776-0322 (A. Hassan); 0000-0002-0355-3618 (A. M. Khodayer); 0000-0001-8581-0448 (O. M. Khodayer)

efficiency errors [2].Time saving and ease of use have positive on the performance of the E- banking system, which leads to good relationship and adoption of internet banking [3].

2. Types of E-Banking System Intrusions

A. Attack of Denial of Service

Denial of service is one type of attacks. Due to this attack the financial institutes become unavailable to the clients or customers. The bank will suffer significant financial harm as a result of this, and repairing the damage will be extremely expensive. After terrorism and espionage, the FBI considers this attack to be the third greatest danger. Distributed Denial of Service (DDoS): [4] this is the most common attack that could happen in banking system. DDoS involved in hundred 'zombie' computers to lunch the attack to the targeted system. Anew program is installed in 'zombie' computer. The program can self-propagate and automatically create a large attack to the network. These 'zombie' send large number of packets to the system at the same time and load the network with useless packets and force the real requested packet to drop due to the time out. Due to this type of intrusion, system will effect on the availability and continuity of the banking system. The financial institutes fail to conduct with its customer, business partners and vendors [5]. There are other risks that encounter the financial institutes; operational risk can be caused by fraud, mistake, or service failure. Due to the denial of service, a company's reputation is at danger of being tarnished.

B. Data Intrusion

Data intrusion happens when there are loopholes in the security banking system. The unauthorized individual can access to the system and perform illegal job due to the lack in the security system of the bank. So banks have to be aware of all threat that would affect the system security in the organization. Whenever there are data breach, integrity and confidentiality would likely been violated by unauthorized persons. This attacker may view, alter or steal the personal information of the customers or the information of banking system which result in violating the confidentiality of the bank. The integrity can be also be effected when unauthorized person alter and changing the data information in the system [6]. Stolen identification is considered the main ticket for unauthorized individual to attack the secret information of the financial institution to get their own benefits. The loss of credit card and poor authorization can lead to data breaches. Without proper authentication and authorization. Intruders can enter the system illegally and can get any information they want. That is why authentication and authorization are very important factor to protect information and ensure the integrity and secrecy of the financial institutes.

C. Malware Program Attacks

It is software Program that is used to change computer's system without the permission of the authority or the owner. Malware can transferred from one computer to another through the network It may include viruses, worms, script attacks. Malware attack could influence the confidentiality, vulnerability, and integrity of the banking system. In confidentiality, malware attacks are including key stroke, password, and credit card numbers, and downloading files, what is going on the servers screen [7]. Attacking against integrity does corruption of the data files and application of banking system by unauthorized file writers, also over writing data , attacking may change the configuration of the banking system, all these accident have the potential to influence the banking system. Availability of banking system can also be affected when denial of service attack occurs and prevent legal clients from accessing banking system and disabling security system. It includes deletion of files and subdirectories on and renaming them. Malware attack cause severe damage to the financial institutes. Trust wave , a Chicago –based provider of information security and card industry have uncovered malware attack, while investigate ATM breaches in many countries like Russia and Ukraine were infected by malware attacks , allowing the attackers to steal data ,PINs and also money. While investigation ATM's in Russia and Ukraine for over few months, about 20 ATMs were infected by malware. Attacker needs the physical access to the ATM, so they were certain that the attacker was an inside work. The attacker could be someone who gets a copy of the key to the ATM [8].

D. Attack of TCP/IP Spoofing

The attack of TCP/IP spoofing is a technique that allows unauthorized attacker to access a targeted computer or network in order to perform illegal jobs and it is consider to be one form of on-line camouflage. Spoofing is process that make malicious message has come from trusted computer toward victim server by spoof IP address of that computer. The recipient of the faked message considered it as trusted message [9]. Spoofing technique can make the attacker to send packets on a network without intercepted and blocked by firewall. While the main job of firewall to filter any external IP address that tried to communicate within network facilities. Attacker can hide his/her identity by making their IP address comes from the internal network, thus the firewall unable to detect it. The main target of this attack to allow intruder to get root access to victim server, then banking system will allow creation of a backdoor entry path into the victim system. As long as there is loophole in the security system and hidden path, the attacker can sneak in back to the target system at any time. In the TCP/IP, the technique that is used to hide source address in the header is very easy, and it is obvious to perform illegal jobs by sending packets that contains malwares to get information such as personal identification number PIN, Customer's bank accounts, credit card number, identification numbers and others. The favorite of internet-based scammers target is the financial institutions, which is done by using IP address spoofing. This type of attack has caused great losses to international bank. The main victims of spoofed emails are LIoyd's Bank, First Union Bank, Bank of America and Barclays Bank [10]. The second threat by spoofing is confidential data breaches. Sending confidential and sensitive data to unintended Gmail account may cause a lot of damages to the bank relationships with clients. This leads to mistrust toward bank's services which considered the biggest loss .This violets confidentiality and integrity of information between customer and bank organization [11]. The violation of confidentiality between customer's and the financial institution by any means is very serious problem. So the confidentiality has very important issues in term of security, because it includes private information about the client's and financial institution. The privilege of the private information of the client's has to be well protected from IP spoofing [12].

3. Electronic Measures for Intrusion Prevention

Authentication mechanism is one of the security measures which is implemented to prevent all unauthorized access to get into financial institutions to change the integrity of the system. Authentication is main parameter to ensure the trust and proper functioning of the banking system. To enhance authentication, the financial institution or banking system should increase their security measure to improve their performance by using two levels of authentication:

A. The first level uses Personal Identification Number (PIN) or Finger Print Matching (FPM). [13] The second level can use some biometric authentications by using Face Recognition Technique as shown in Fig (1).

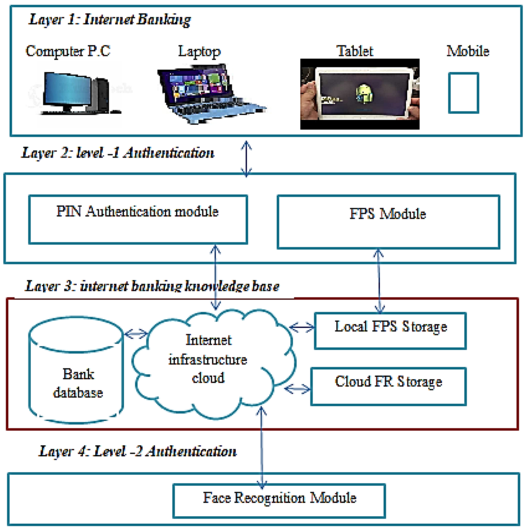
Layer 1: Internet Banking
Computer P.C
Laptop
Tablet
Mobile
Layer 2: level -1 Authentication
PIN Authentication module
FPS Module
Layer 3: internet banking knowledge base
Bank database
Internet infrastructure cloud
Local FPS Storage
Cloud FR Storage
Layer 4: Level -2 Authentication
Face Recognition Module

Figure 1: Components of 2 Levels Integrated Authentication Mechanism 2L-IAM

A. Authentication that uses PIN with 16 digits and four digits for password could strengthen the security measure that has been taken against vulnerabilities that has owned by banking system. The password used to authenticate the PIN of the customers, which is considered as a second stage, in the first level authentication when it is used in ATM by inserting credit card in it [14].

B. Biometric authentication technique is one of the methods that are used to identify the real person by its unique physical features. Biometric authentication technique has been developed and implemented widely in the banking system, by using person's eyes and thumb [15].

C. Firewall is used on specific computer that is situated between the network and the internet in order to check the incoming request before reaching the network resources. Protects against malicious attacks and blocks any attack that originates from the internet. A firewall prevents unauthorized individuals from accessing any shared files that the bank has put up. Bank-owned activities, however, haven't been stifled or halted. Hardware firewalls and software firewalls are the two main varieties. Hardware firewall build inside devices such as router, so it is used to protect the whole network, while software firewall is installed in side computer so it is used to protect the individual computer only Firewall can make restriction on the employee's within corporate network to access highly sensitive banking data. Incoming data packets are detected by firewall filters and denied entrance if they threaten the network. To keep the integrity of the information and avoid breaches, attention has to be bayed toward employees inside the financial organization or the banking system. They are considered major threats, which have all the authority to deal and manage customer's information especially those terminated employees [16].They would likely use their knowledge and authority and act as intruder to perform illegal jobs by deleting data or do some modification or fabrication of data. These acts put the bank in troubles.

D. The administrator of the bank strongly recommended changing all passwords and any means to prevent them from gaining access to the banking system and its database. On the other hand, one time password can be used which are prepared by the main server and monitored by the responsible manager. This process will protect huge information and keep the integrity of data for the banking system in safe [17]. For insider employee's, they may have the intention for violating banking system's information, to limit these activities the administrator has to do monitoring on all activities they do. Recording them and analysis all the steps that have been done, then track down any irregular behavior toward customer's information[18], Monitoring is based on ,who did the task ,what task did they do, when did they do it , where the employee did the job by this security measure and other legal action that have been done. The data integrity can be protected. Perhaps the privacy of employee is violated, but the customer's information and bank reputation are more important. There are outsider intruders; they collect information about the system and applications. There must be a safe area where the record may be maintained, and it must be physically segregated from any machines that generate the recordings [19].

E. Intrusion prevention system (IPS) is used to protect the confidential data and assets of the banking system, and detect any harmful intrusion. This feature could reduce the cost of damage and impact of the attack on the banking system such as, (DoS) and malware. An excellent example of IPS is Macfee Network Security Platform. Centralized Security system that use consolidated dashboard and robust reporting events of breaches save time and money for administration. IPS improve the performance of banking system by reducing network down time and remove all risk that comes from intruders[20].

4. Conclusions

Computer system has been used in all wide range in our daily life applications. They have been used in many different sectors both for civil application such as banks and financial organization and others. Intruders can perpetrate an attack on financial institutes in order to steel money illegally. Intrusion is not a new phenomenon, but because of the advancement of technology in the last few years, the intrusion technique has gotten more sophisticated and difficult to detect, making it more difficult to stop. Unauthorized individual and illegal users can intrude the system through vulnerability points in the security system. The violation of the security system may cause, modification, deletion, challenge to intercept data, and fabrication. Usually the intruder they have good experience and knowledge to get into the banking system or the financial institution system. The bank's high level of security and excellent customer service might potentially entice new clients to utilize the bank's authenticated system. They may be certain that their private data and, most importantly, their money, are protected. Although the vulnerabilities are available always, the financial institution should have backup to the data and operating system in order to avoid any damage or loss from future malware intrusion to the system. To protect the banking system data and information against any malicious attack, all protections and security measure should be applied and some recommendations must be followed such as all problems of ATM functionality has to be removed, blocking cards, lack of cash in the ATM, shortage of paper and printer status , and more as they are mentioned earlier. Always update security system to ensure the confidentiality, availability, and integrity of the system.

5. References

[1] M. A. M. Ataya and M. A. M. Ali, "Acceptance of Website Security on E-banking. A-Review," in *2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC)*, 2019, pp. 201–206.

[2] A. Salihu, H. Metin, E. Hajrizi, and M. Ahmeti, "The effect of security and ease of use on reducing the problems/deficiencies of Electronic Banking Services," *IFAC-PapersOnLine*, vol. 52, no. 25, pp. 159–163, 2019.

[3] M. R. Aburrous, A. Hossain, F. Thabatah, and K. Dahal, "Intelligent quality performance assessment for e-banking security using fuzzy logic," in *Fifth International Conference on Information Technology: New Generations (itng 2008)*, 2008, pp. 420–425.

[4] A. G. Bultum, "Adoption of Electronic Banking System in Ethiopian Banking Industry: Barriers and Driver," *Available SSRN 2058202*, 2012.

[5] A. Alarifi, M. Alsaleh, and N. Alomar, "A model for evaluating the security and usability of e-banking platforms," *Computing*, vol. 99, no. 5, pp. 519–535, 2017.

[6] S. V. A. Das and N. Ravi, "A Study on the Impact of E-Banking Service Quality on Customer Satisfaction," *Asian J. Econ. Financ. Manag.*, pp. 48–56, 2021.

[7] T. Kujur and M. A. Shah, “Electronic banking: impact, risk and security issues,” *Int. J. Eng. Manag. Res.*, vol. 5, no. 5, pp. 207–212, 2015.

[8] A. A. Oni, O. J. Adewoye, and I. O. Eweoya, “E-banking users’ behaviour: e-service quality, attitude, and customer satisfaction,” *Int. J. Bank Mark.*, 2016.

[9] M. Kumar and S. Gupta, “Security perception of e-banking users in India: an analytical hierarchy process,” *Banks Bank Syst.*, vol. 15, no. 1, p. 11, 2020.

[10] Q. Hammouri, T. Majali, D. Almajali, A. Aloqool, and J. A. AlGasawneh, “Explore the Relationship between Security Mechanisms and Trust in E-Banking: A Systematic Review,” *Ann. Rom. Soc. Cell Biol.*, vol. 25, no. 6, pp. 17083–17093, 2021.

[11] C. U. Bah, A. H. Seyal, and U. Yahya, “Combining PIN and Biometric Identifications as Enhancement to User Authentication in Internet Banking,” *arXiv Prepr. arXiv2105.09496*, 2021.

[12] S. Firdous and R. Farooqi, “Impact of internet banking service quality on customer satisfaction,” *J. Internet Bank. Commer.*, vol. 22, no. 1, pp. 1–17, 2017.

[13] M. Bala, S. Baghla, and G. Gupta, “Data Mining and E-banking Security,” in *Green Information and Communication Systems for a Sustainable Future*, CRC Press, 2020, pp. 73–92.

[14] H. E. Inegbedion, “Factors that influence customers’ attitude toward electronic banking in Nigeria,” *J. Internet Commer.*, vol. 17, no. 4, pp. 325–338, 2018.

[15] I. U. Haq and T. M. Awan, “Impact of e-banking service quality on e-loyalty in pandemic times through interplay of e-satisfaction,” *Vilakshan–XIMB J. Manag.*, 2020.

[16] S. A. Subbotin, “Methods of sampling based on exhaustive and evolutionary search,” *Autom. Control Comput. Sci.*, vol. 47, no. 3, pp. 113–121, 2013.

[17] S. N. Huda, S. Aktar, and M. S. Islam, “Impact of E-Banking on Service Quality and Customers Satisfaction in Selected Private Commercial Banks in Bangldesh,” *Glob. An Int. J. Manag. IT*, vol. 11, no. 2, pp. 21–27, 2020.

[18] H. Stewart and J. Jürjens, “Data security and consumer trust in FinTech innovation in Germany,” *Inf. Comput. Secur.*, 2018.

[19] J. Hammoud, R. M. Bizri, and I. El Baba, “The impact of e-banking service quality on customer satisfaction: Evidence from the Lebanese banking sector,” *Sage Open*, vol. 8, no. 3, p. 2158244018790633, 2018.

[20] S. Subbotin, “The neuro-fuzzy network synthesis and simplification on precedents in problems of diagnosis and pattern recognition,” *Opt. Mem. Neural Networks*, vol. 22, no. 2, pp. 97–103, 2013.