Milev Journal of Research and Studies

Vol.6, No. 2, December 2020

Pp: 524-542

Security Risk Management in the Electronic Banking Environment: Some Evidence for Banking Systems

Abdelmageed Algamdi

Dept. of Computer and information systems, Community College, University of Bisha, BISHA, (Saudi Arabia)

amofrh@ub.edu.sa

Received: 03/09/2020 *Accepted: 06/10/2020* *Published: 31/12/2020*

Abstract:

The banking industry has witnessed a significant growth in the use of the Internet, and in the procurement of goods and services and electronic data exchange, which requires a secure Internet to achieve a high level of confidence with institutional customers, so banking institutions realized the importance of security and confidentiality in electronic banking operations.The research aims to answer the following question: How to reduce the security risks in the e-banking environment?. In order to achieve the objective of the research, a descriptive analytical approach was adopted and specialized research was used in the field of e-banking risk management, leading to findings and recommendations.

***Keywords**: security risk management; electronic banking; firewall; physical security; ryptography.*

Introduction:

Financial and E-commerce institutions are developing the infrastructure of online payment instruments to make online commerce operations safe. The banking industry has seen significant growth in the use of the Internet in the procurement of goods and services and electronic data interchange, requiring that the Internet be secure to achieve a high level of confidence with both customers and companies(Shankar & Jebarajakirthy, 2019).

Banking institutions should be aware of the importance of security and confidentiality in e-banking operations in order to achieve a high level of confidence by their individual and institutional customers(Hertzum, Jørgensen, & Nørgaard, 2004; Jogi, 2020), to ensure the security of the operations carried out and the security of information flowing through electronic communication channels.

Elements of security risk management

The levels of good management of banking products and services, including those provided online is essential to maintain a high level of public confidence, not only at the level of the bank's brand name but at the level of the banking system as a whole. Key elements that would help maintain a high level of public confidence in an open networked environment include the following (Robinson & Julie, 2019):

- Security.
- Authentication (Authentication: identity).
- Trust.
- Non-Repudation.
- Privacy.
- Availability.

1. Security

Security is one of the main issues of online banking systems, and all banks strive to achieve a level of security commensurate with the sensitivity of the information in the bank(Ataya & Ali, 2019; Limba, Plėta, Agafonov, & Damkus, 2019; Nayanajith & Damunupola, 2019). The risk of some banks results from their permitting to dial-up over the network, and other banks provide access to the network through the Internet, although the Internet is accessible to the public, and both types of communications may be less secure and vulnerable to hacking and changing hardware or software. For example, "pirates" can obtain passwords, account numbers, credit card codes, etc (Easttom, 2019; MURUGAN, 2020). regardless of the means of access to banks. Therefore, the internal control system must be sound to protect from security breaches of all forms of electronic access, and it must be a sound precaution and preventive system in accordance with corrective controls that help to ensure the integrity of the network and the information it processes(Diego, 2019).

2. Authentication :[*]

The identity must be confirmed in transactions on the Internet, Internet banks, or any other communication network in order to be safe. In order to

[*]. Authentication is a very important technique to cover the risks faced by the bank, There is a lot of data available for the same, We have covered the crux of the topic for further reading you may go through the following documents": www.ffiec.gov/pdf/authentication_guidance.pdf, & https://www.firstexchangebank.com/WebPDF03_authentication.pdf

achieve a high level of public confidence in the Internet space, as is the case with tangible international banks, as customers need assurances that they will get the service as they wanted or the goods with the required specifications, and to know the identity of the person you are dealing with you (Aldridge, White, & Forcht, 1997; Buttle & Maklan, 2019; Cheng, Gan, Imrie, & Mansori, 2019; Diego, 2019; Longstaff et al., 1997).

- **Identity confirmation:**

Confirmation of identity is a very important technique for covering the risks faced by the bank. The identity verification process is based on the techniques, procedures, and processes used by banks to verify the identity of current and future customers(Committee, 2003; Pejović, 2016). Therefore, banks use reliable and safe methods that confirm the identity of their customers and users of electronic banking systems, taking into account the assessment of the risks associated with that application. The use of only one factor to verify customer identity is inappropriate in high-risk transactions, which include access to customer information, money transfers, or access for high-privileged users, such as a network administrator (Cerovic, 2008).

Identity confirmation is used to verify the identity of any person or entity within the scope of electronic banking systems. The identity verification process is the only way that is used to control and access customer accounts and personal information. Confirmation of identity usually depends on the presence of customers and their provision of valid identity data, and provides one or more papers Identity adoption to prove their identity.

Customer IDs with bank cards using an ATM can be a form of authentication to log in remotely through an identity verification agent (PIN or password), which is confidential or unique information associated with a specific customer identifier that is used to verify Identity. Currently, the process of confirming customer identity is accomplished by introducing some of the identity verification factors. These factors include one or more of the following:

- Some information, such as passwords or personal identification numbers (PINs).

- Self-powered devices that operate with Token ownership, and must be connected to a computer or devices that have a small screen, as a one-time password (OTP: One-Time Password) is displayed, for example a smart card.

- Physical properties, such as sound engineering, handprint, or "biometrics", such as a model of the cornea of the eye, which requires the installation of certain devices on the system in order to be able to access them.

There are many methodologies to confirm identity ranging from a simple to a complex level of providing security on the basis that each method differs from the other methods used. As it is not possible to consider any of the previous three methods alone as a guarantee, because each method has its limitations. The password can be hacked or guessed, and the Token code can be copied or stolen while the biometric feature is expensive and inaccurate one hundred percent. It may not recognize a person with a cold according to the sound system, or a fingerprint reader, as well as the case with biological molds when they are not exposed will create serious problems for life because it cannot be replaced as passwords. Therefore, it is preferable to use more than one method such as entering the password and inserting the smart card in the card reader, which provides safe access.

- **Biometrics:**

Biometrics are a technique for verifying identity or identifying a person based on physiological or physical characteristics (which is a person's matter). Physiological features include fingerprints, iris and the face structure, and the physical properties include the rate of flow of movements, such as the data entry pattern on a computer keyboard(Briggs & Olivier, 2008).

The process of introducing people to a system of biological characteristics is called "biometric" based on the use of the input technology (Enrollment) or recording and then taking data samples from one or more physiological properties. Then the samples are converted into a mathematical model, then registered with a database of data analysis that can perform to application software(Hanaek, Malinka, & Schafer, 2008; Ortiz-Yepes, 2008) . In contrast to identity verification mechanisms, the biometric feature does not rely on user memory, so it distinguishes each user(San Martino & Perramon, 2008).

After the data entry process is completed, customers communicate with a live examination thanks to the technology of biological characteristics, as this examination is used to identify and confirm the customer’s identity (authentication) according to the recorded calibration forms stored inside the system, and when they are identical, the system is accessed (Briggs &

Olivier, 2008). Various biometrics that are being developed and tested for the following:

- Fingerprint Recognition.
- Face Recognition.
- Voice Recognition.
- Keystroke Recognition.
- Handwriting Recognition.
- Finger and Hand Geometry.
- Retinal Scan.
- Iris Scan.

Fingerprint recognition and facial recognition are among the most widely accepted biometric technologies.

The fingerprint recognition techniques rely on the analysis of data extracted from the fingerprints, and it is very dense, because the density explains why fingerprints are the most reliable means of identification. Also, fingerprint recognition and data storage systems are the only ones that describe exactly the fingerprint details; images of actual fingerprint being preserved, and the fingerprint can be built into a computer or a mouse keyboard, or stand-alone devices such as computer-connected scanners(Xueyan & Shuxu, 2008).

Fingerprints are unique and sophisticated enough to provide a robust identity verification model with multiple fingerprints, providing the individual with the greatest degree of accuracy. Where fingerprint recognition techniques, are among the most mature and accurate methods of biometric identification. According to fingerprint technology companies, there are several remote registration scenarios that provide adequate protection, but for large accounts to be addressed, the organization must ask customers to attend in person(Hemery, Mahier, Pasquet, & Rosenberger, 2008). ID devices are an advanced model that may take the form of finger retina scanning or thumb and face or voice printing. Only a limited number of banks use biological properties, which are by far the main model.

- **Confirmation of subscriber identity:**

Confirmation of subscriber identity is a process whereby the customer’s identity is confirmed on a website, and most financial institutions currently do not confirm customer identity on Internet sites before collecting sensitive information about clients(Billmaier, Billmaier, & Kellum, 2008;

Ericson, 2020). One of the strong causes is phishing or hacking attacks, which can direct customers to spoofed websites.

Therefore, it constructed for ordinary users what enables them to differentiate the websites of legitimate financial institutions from plagiarized sites by confirming the identity of customers on the website. The identity assertion techniques on a website are varied between the use of digital certificates or encrypted communications (Website Design Service)(Khan, Olanrewaju, Anwar, Mir, & Yaacob, 2020), and it is one of the secrets of joint use such as digital images and digital certificate authentication, which is considered one of the most powerful techniques for authenticating(Bansal, Panchal, Thaker, & Valecha, 2020; Easttom, 2020; Nan, 2020) and confirming the identity of the subscriber, as it provides protection against phishing attacks, etc.

3. Trust:

Trust can be used in Internet banking services systems, and as mentioned in the previous discussion, the main coding systems are to secure information in transactions and confirm parties ’identity in cyberspace, and a trusted third party is an essential part of the process. This third party is the certificate of authentication, in which a trusted third-party checks identity in cyberspace.

Some people believe that a power performance certificate such as a notary over the Internet, as a basic concept is that the bank or third party uses its name well to validate parties in all transactions and this is similar to the historical role played by banks with letters of credit, which the seller and buyer do not know each other. Thus, the bank uses its name well to facilitate transactions, as well as bank charges which may also need a way to validate the banks themselves in cyberspace. Identity theft has taken place according to the GAO / T-66D-99-34 certificate, as the perpetrators of this project have been hackers by copying the websites of brokerage firms and changing customer contact addresses (and sending checks), then returning the fraudulent website on the Internet except for a job The box office, and everything may be linked to a website, and banks can appear legitimate through a fire guard and a variety of frauds (Romney, Steinbart, & Cushing, 2006; Turner, Weickgenannt, & Copeland, 2020).

Frauds and online banking have become a more prominent and convenient mix, so that achieving preventive and corrective controls can help protect banks from these predicaments, digital certificates can play an important role in confirming the identity of parties, thereby placing trust in Internet banking systems.

4. Non-Repudiation:

A denial is a guide to receive the original information, in order to protect the sender from the recipient's claim not to receive the information, or to protect the recipient from a false claim by the sender not to send the information, so banks must ensure the accuracy and integrity of the electronic information sent Through internal and external electronic networks(Georgescu, 2006), to ensure the non-denial and safety of electronic banking operations(Sokolov, 2007).

5. Privacy[*]:

Privacy is an issue of extreme importance to the consumer. Banks that have proactively responded to the privacy issue have made this feature positive and beneficial to the general public, due to their growing concern about inappropriate use of personal information(Ataya & Ali, 2019) as the e-commerce and internet providers continue to grow(Alshamari, 2016).

6. Availability:

The last element is to maintain a high degree of confidence in the general network environment in which all the above components are available, and they are of little value if the network is not available and appropriate for customers who use the network. To access their systems 24 hours a day, seven days a week(Daka & Phiri, 2019). Among the considerations associated with the availability of the system are the ability to monitor the abundance of performance and to monitor the business of commercial banks and sellers who provide products and online banking services, the need to ensure their capacity in terms of hardware and a program to provide continuous high-level service. In addition to performance monitoring techniques that allow the management of information, such as the volume of traffic(Nustini & Fadhillah, 2020), the duration and quantity of transactions, and the waiting time for customers to obtain the service.

The ability to regularly monitor and monitor performance helps ensure a high level of internet availability in the banking system, and it is also important to assess network vulnerabilities, such as preventing power outages that cause network components to fail completely, and can become

[*] Ensure that customer transactions are kept confidential.

inoperable in one component or when software or hardware crashes. Commercial banks and sellers often resort to redundant devices during critical periods or have the ability to switch to alternative sites to address the latter, which is referred to as contingency planning. Therefore, when malfunctions of any part of the network occur, the following is done:

- Double the number of widely used backup servers, especially servers used as a means to achieve another service, such as a DNS server used as a means to obtain a website address while using a bank's web server.
- Double the number of iterations and redirects, if the entire router is deactivated, the bank network will still work, as if nothing happened, but at the same time it requires a large additional cost.

- **Firewall:**

Firewalls are used as a procedural security control to protect the internal systems of Internet banking systems from the bank's external network systems. Firewalls are a combination of hardware and software placed between two internal and external networks, and regardless of the flow direction, they provide an entry point for protection from individuals who are not authorized to access the bank's network. The mere presence of a firewall does not guarantee logical security and does not penetrate(NO, 1997):

- Firewalls must be configured to meet a specific operating environment.
- They must be evaluated and regularly maintained as a basis for achieving their effectiveness and efficiency.
- Individuals who represent the professional technical backbone should install, configure, evaluate, and maintain firewalls, and control specific risks that may require sharing a wide range of security controls.

Management needs to understand and monitor firewall functions to ensure that their systems are configured appropriately for the bank's business needs, and to ensure that firewall functions are appropriately activated appropriately, such as preventing attacks against security vulnerabilities known as public utilities to protect institutions.

Firms that do not have experience in designing, installing, and testing firewalls must seriously consider recruiting specialists to perform this task, with due diligence when selecting vendors to perform these tasks, and the location of sound internal controls should be combined with audits to verify vendor activities using the firewall And the institution's participation periodically with an independent source to test and clarify the weaknesses associated with the firewall annually or when circumstances require it, penetration testing to ensure appropriate control of a particular type and the level of risk arising from Internet banking rental products.

Firewall is a hardware and software program to enhance the security policy. It separates two networks, an internal network and an external network. The intention is to control traffic with all networks regardless of the direction of flow, the wall can check all traffic as authorized or not, and of course prevent unauthorized traffic from entering the banking system(NO, 1997).

Also check the traffic to determine whether it contains any unauthorized attachments such as viruses, "where viruses and parasitic programs constitute the bulk of the attack, and they search for their targets randomly, so all organizations need small institutions that do not have any secret information walls Protection to protect its networks from these automated attacks "[Northrup, 2010]. Therefore, firewalls should be effective in capturing any unauthorized traffic to prevent potential damage to the organization, because they are:

1- An isolated network is a function of firewalls.

2- The domain name is known as a server that converts unknown addresses to internal addresses. This is referred to as the "Bastion Host" or security zone. Its advantage is that it prevents intruders from accessing names and addresses within the network, where all external devices Attempting to reach suspected internal addresses are excluded(NO, 1997).

3- Firewalls are used to control access and what must be done with each packet you access, because the firewall is designed as a filter that allows the passage of those packets that meet specific conditions, for example the function of blocking messages from the internal system and the addresses of messages that have not been accepted or passed through The server's domain name, as the firewall does not allow for suspected transit and traffic.

4- Sorting application is the firewall function used to prevent entry of the system from inappropriate instructions or unauthorized access to the level of a proxy server, a device used to test the deviation from the established rules(Herz, Radin, & Madan, 2010) .

5- Scan message or complete package sorting according to the case, which is the function of the firewall used to detect inappropriate comments towards the system, where the system creates a database and searches for inappropriate comments by the message server or inquiries, for example if it is a request for information related to with the account balance and response to money transfers, "Stat full Packet Filtering" will know the response to the session termination normally. This technology works in conjunction with the firewall.

A full scan is performed by checking each package separately by maintaining a table that records all communications between the bank's computers and the Internet and the firewall again to see if the next package is part of direct internal communication or not. Studies in this field indicate that about 70 percent of intrusions originate within the organization knowledgeable of the system or network, and may have the opportunity to provoke unauthorized transactions, whether through intention to access and information systems or the occurrence of banking network knowledge, perhaps due to the lack of Protection for employee ignorance, such as exchanging passwords and running programs without virus checking or access control that includes a user and password assignment(Graham & Steinbart, 2006; Rahman & Tomar, 2020) .

- **Physical Security**

Physical security is an important function to combat and protect bank data, internal communication networks, devices, and the network of accounting systems, which must be stored in secure locations so that they are only accessible with the permission of individuals. This is a preventive control to protect banking assets and protect the institution from reputation, transactions and strategic risks. Personal computers connected to the network should have access to include proper logical controls such as the password to access the network, and network protection controls with a password at an unattended private computer even in short periods of time, and when direct physical unattended access, a professional can To successfully access sensitive data through special stimulus disks that provide privileges on the target computer, or by using the Keystroke Logger tool that copies passwords through identifiers (Credentials).

A. **Control of the bank building**: The process of monitoring physical access begins with the entry points to the bank building, where it is better to keep one entry point open during working hours, while leaving an additional entry point to be used in certain cases such as fire. These exits must be connected to an automatically activated alarm system that does not allow entry into the building with a security guard to confirm the identity of the employees.

B. **Control of entry to the building's rooms:** It is necessary for the bank building's rooms to be tightly closed and linked to Closed Circuit Television Systems. Also, regular locking of rooms with sensitive data such as card readers, network scanners, fingerprints, voice IDs, or iris should be supported.

The process of controlling system output is necessary; however, it must include:

- The employees exit from all applications on the computers when they leave their places of work to prevent the use of that data by other employees.
- Restricting access to rooms that contain important devices such as fax and printers.
- Encrypt private information.
- Not to allow visitors to tour the building.

C. **Control of the internal network of the bank:** It is necessary to restrict and prevent eavesdropping to access the wires used within the bank's internal networks (LANs: Local Area Networks), that the wires are not exposed, and that they are in places that are difficult to reach from visitors, and the same applies to the safes of communications equipment, which must be placed inside steel cages to prevent illegal access to them.

Examples include the theft of bank equipment, the theft of the personal computer of an American bank employee, Wells Fargo, who incurred significant losses to the bank and had to inform customers to amend their passwords due to the risk of the risk arising from the theft of their personal information (Graham & Steinbart, 2006) . Accordingly, security experts and experts suggest working to encrypt and store data with great confidentiality to prevent unlawful access to it.

- **Complex audit techniques:**

The internal control of banking institutions is weakened in the event that they are unable to audit the electronic banking business, as all records and supporting documents related to them are available electronically, and the bank must ensure that there are clear review paths that can audit all electronic banking transactions and applications in detail, to ensure security

Customers and bank safety alike, and the following electronic banking transactions must be clear (Chorafas, 2003; Committee, 2003):

- Opening, amending and closing the account.
- All transactions with financial results.
- The authorization granted to the client when the limit is exceeded.

It is appropriate to determine whether the bank's policies are effective and whether the network monitoring system operates as intended and the need for firewalls to monitor and audit. The dynamic firewall system needs regular reviews to ensure protection from newly diagnosed vulnerabilities in a weak system. Granting and modifying access rights to systems.

Once a solid understanding of the network's internal auditor or external auditor is formed, gains are made for the types of commercial banking businesses. So that he may decide to perform various tests to ensure the safety of access control (Logical), and this may include a test of default settings to determine whether the firewall permission only allows auditors and employees to use audit software to check activity logs, and perhaps review staff checks or install the network Also review changing the password for employees who are authorized to access data and banking network.

Therefore, according to the level of Internet banking services, the bank will engage external experts to consider reviewing security procedures and making recommendations to improve them. These reviews must be reviewed and reviewed at least annually for trade, communication and information systems.

- **Cryptography:**

There were many methods used in the data encryption process, and in the recent period, they started heading towards very complicated methods, but the idea in these methods is very similar and the difference in them in sub-matters(Kessler, 2003; Montero-Canela, Zambrano-Serrano, Tamariz-Flores, Muñoz-Pacheco, & Torrealba-Meléndez, 2020). The coding process often depends on one of two basic methods:

- Symbol.
- Code.

Symbol: is the process of changing the locations of letters in the word or replacing these letters with symbols and the like, where "Julius Caesar" was one of the first coders to use symbols in his correspondence with his companions.

Code: It changes the whole word and replaces it, meaning that its range is broader than the range of single letters, and here the coding program depends on a huge data base that contains the basic words and their corresponding encoded words.

Among the most prominent institutions that contributed to this field is the National Institute of Standards and Technology (formerly known as the US National Bureau of Standards). In 1973, this institute developed a standard called the data encryption standard. (Data Encryption Standard: DES) This standard is based on the Algorithm algorithm that uses a 56-bit encryption key (Bit), and requires that both the transmitter and receiver have the same secret key. The U.S. government used this official standard in 1976, and adopted it Banks to operate ATM machines.

After one year of applying the data encryption standard (DES), three university professors developed another coding system called (RSA), and this system uses a pair of keys: a public key and a private key instead of using a key Only one, and although this system was very suitable for complex computers, it was later compromised, and this remained the case until Phil Zimmerman in 1986 developed an RSA encryption program(Boyd, Mathuria, & Stebila, 2003), but it is distinguished Using a 128-bit key, it is called PGP: Pretty Good Privacy. A commercial and free version is available from this program. The most prevalent coding software today "(Boyd et al., 2003).

- **Definition of ciphering**:

Ciphering is defined as the process of converting information into incomprehensible coding to prevent unauthorized persons from seeing or understanding the information. That is why the coding process involves converting regular texts into encrypted texts. It is well known that the Internet is nowadays the largest medium for the transmission of information, and sensitive information (such as financial movements) must be transmitted in encrypted form if I want to maintain its integrity and secure it from the futility of intruders, saboteurs and thieves(Subashini & Kavitha, 2011).

The keys are used to encrypt and decrypt the message (Decryption)(Bhanot & Hans, 2015). These keys are based on sophisticated mathematical formulas (algorithms), and the strength and effectiveness of the encryption depends on two main factors: the algorithm, the length of the key (Bits) On the other hand, the decryption is the process of retransmission Data to its original form(Al Hasib & Haque, 2008), using the appropriate key to decode.

- **Symmetric Encryption:**

In symmetric encryption, both the transmitter and the recipient use the same secret key to encrypt and decode the message, and the parties agree at the beginning on the passphrase (long passwords) that will be used, and can contain a phrase Passage is uppercase and lowercase and other symbols. Then, the encryption software converts the passphrase into a binary number, other codes are added to increase its length, and the resulting binary number forms the message encryption key(Boldyreva, Chenette, Lee, & O'neill, 2009; Boyd et al., 2003) .

After receiving the encrypted message, the receiver uses the same passphrase to decipher the Cipher Text or Encrypted Text, as the software again translates the passphrase to form a binary key that converts the encrypted text to its original, understandable form.

The concept of symmetric encryption is based on the (DES) standard, and the big gap in this type of encryption was the exchange of the secret key without security, which led to the decline in the use of this type of encryption, to become a thing of the past(NO, 1997).

- **Asymmetric encryption (public key):**

Asymmetric encryption is a solution to the problem of insecure distribution of keys in symmetric encryption. Instead of using a single key, asymmetric encryption uses two keys that have a relationship. These two keys are called the Public Key and the Private Key.

The private key is known to only one party or one person, and it is the sender, and it is used to encrypt and decrypt the message, while the public key is known to more than one person or entity, and the public key can decode the message that the private key encrypted. It can also be used to encrypt private key owner messages, but no one can use the public key to decode a message that this public key has encrypted, since only the private key owner can decode the messages that the public key has encrypted (Boldyreva et al., 2009). The encryption system that uses public keys is called the RSA system, and although it is better and more secure than the DES system, it is slower, since the coding session and the decryption session should be almost simultaneous. The RSA system is not immune to penetration, as it is possible to penetrate it if there is time and money available. Therefore, the PGP system has been developed, which is an improved and developed model of the RSA system and uses the PGP key with a length of 128 bytes, in addition to Due to its use of the Message Digest, and this system remains impenetrable to this day" (Boyd et al., 2003).

Types of attacks on the Internet :

Banks and service providers need protection against various types of cyber-attacks(Gumussoy, 2016). One attack is trying to exploit vulnerabilities in knowledge of specific operating systems. Attackers repeatedly attempt to penetrate the Internet over a short period of time is unlawful and thus refuse to serve other clients. Types of attacks include the following (Tounsi & Rais, 2018):

- Sniffers: Also known as an anticipation network, the software used to collect keys from a private computer. This program can capture login IDs and passwords.
- Guessing Passwords: Use the program to test all possible combinations of network access.
- Brute Force: A method for capturing encrypted messages using programs to break the code to access messages and obtain user IDs and passwords.
- Random Dialing: This technique is used to dial every phone number exchanged with a bank phone and the goal is to find a modem to connect to the network and can then be used as a starting point for the attack.
- Social Engineering: The attacker invites the bank's office to help impersonate the authorized user for information about the system including changing passwords.
- Trojan Horse: The programmer can include an icon in the system that would allow the programmer or an unauthorized person to enter the system or network.
- Hijacking: interception of transmission and then an attempt to infer information, as internet traffic is vulnerable to this threat.

Conclusion:

Banks have adequate procedures that enable them to limit the accessibility of users to their information system, and therefore they must follow security measures to protect users 'accounts, because access to those accounts is not limited to financially secure workstations. In addition, some banks adopt sensitive information encryption operations while storing them inside databases or sending them over internal and external networks, and use different encryption keys with each application as well as electronic signatures when sending sensitive information via the Internet.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers and the editor for their insightful comments and suggestions.

REFERENCES

Al Hasib, A., & Haque, A. A. M. M. (2008). A comparative study of the performance and security issues of AES and RSA cryptography. Paper presented at the 2008 Third International Conference on Convergence and Hybrid Information Technology.

Aldridge, A., White, M., & Forcht, K. (1997). Security considerations of doing business via the Internet: cautions to be considered. Internet Research.

Alshamari, M. (2016). A review of gaps between usability and security/privacy. International Journal of Communications, Network and System Sciences, 9(10), 413-429.

Ataya, M. A. M., & Ali, M. A. (2019). Acceptance of Website Security on E-banking. A-Review. Paper presented at the 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC).

Bansal, R. I., Panchal, S. B., Thaker, C., & Valecha, V. A. (2020). Digital certificate containing multimedia content: Google Patents.

Bhanot, R., & Hans, R. (2015). A review and comparative analysis of various encryption algorithms. International Journal of Security and Its Applications, 9(4), 289-306.

Billmaier, J. A., Billmaier, D. P., & Kellum, J. M. (2008). Mobile device confirmation of transactions: Google Patents.

Boldyreva, A., Chenette, N., Lee, Y., & O'neill, A. (2009). Order-preserving symmetric encryption. Paper presented at the Annual International Conference on the Theory and Applications of Cryptographic Techniques.

Boyd, C., Mathuria, A., & Stebila, D. (2003). Protocols for authentication and key establishment (Vol. 1): Springer.

Briggs, P., & Olivier, P. L. (2008). Biometric daemons: authentication via electronic pets CHI'08 extended abstracts on Human factors in computing systems (pp. 2423-2432).

Buttle, F., & Maklan, S. (2019). Customer relationship management: concepts and technologies: Routledge.

Cerovic, I. (2008). Risk Management In Electronic Banking. Montenegrin Journal of Economics, 4(7), 129-133.

Cheng, B. L., Gan, C. C., Imrie, B. C., & Mansori, S. (2019). Service recovery, customer satisfaction and customer loyalty: Evidence from Malaysia's hotel industry. International Journal of Quality and Service Sciences.

Chorafas, D. N. (2003). Operational risk control with Basel II: Basic principles and capital requirements: Elsevier.

Committee, B. (2003). Risk management principles for electronic banking: Basel: Electronic Banking Group of the Basel Committee on Banking Supervision.

Daka, G. C., & Phiri, J. (2019). Factors Driving the Adoption of E-Banking Services Based on the UTAUT Model. International Journal of Business and Management, 14(6).

Diego, A. (2019). The Analysis of Cyber Security the Extended Cartesian Method Approach With Innovative Study Models: Scientific Research Publishing, Inc. USA.

Easttom, C. (2019). Computer security fundamentals: Pearson IT Certification.

Easttom, C. (2020). Information Assurance/Encryption The NICE Cyber Security Framework (pp. 1-30): Springer.

Ericson, B. C. (2020). IDENTITY CONFIRMATION DURING AUTHENTICATION REQUESTS USING NEARBY MOBILE COMPUTING DEVICES: US Patent App. 16/234,345.

Georgescu, M. (2006). Some issues about risk management for e-banking. Available at SSRN 903419.

Graham, E., & Steinbart, P. J. (2006). Wireless security Enterprise information systems assurance and system security: Managerial and technical issues (pp. 234-252): IGI Global.

Gumussoy, C. A. (2016). Usability guideline for banking software design. Computers in Human Behavior, 62, 277-285.

Hanaek, P., Malinka, K., & Schafer, J. (2008). E-banking security-comparative study. Paper presented at the 2008 42nd Annual IEEE International Carnahan Conference on Security Technology.

Hemery, B., Mahier, J., Pasquet, M., & Rosenberger, C. (2008). Face authentication for banking. Paper presented at the First International Conference on Advances in Computer-Human Interaction.

Hertzum, M., Jørgensen, N., & Nørgaard, M. (2004). Usable security and e-banking: Ease of use vis-a-vis security. Australasian Journal of Information Systems, 11(2).

Herz, F. S., Radin, M., & Madan, B. (2010). Use of proxy servers and pseudonymous transactions to maintain individual's privacy in the competitive business of maintaining personal history databases: Google Patents.

Jogi, V. (2020). A Critical Study on Emerging Risk Associated with E-Services Provided through E-Banking. Studies in Indian Place Names, 40(51), 5-9.

Kessler, G. C. (2003). An overview of cryptography: Gary C. Kessler.

Khan, B. U. I., Olanrewaju, R. F., Anwar, F., Mir, R. N., & Yaacob, M. (2020). Scrutinising internet banking security solutions. International Journal of Information and Computer Security, 12(2-3), 269-302.

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2019). Cyber security management model for critical infrastructure.

Longstaff, T. A., Ellis, J. T., Hernan, S. V., Lipson, H. F., McMillan, R. D., Pesante, L. H., & Simmel, D. (1997). Security of the Internet. The Froehlich/Kent Encyclopedia of Telecommunications, 15, 231-255.

Montero-Canela, R., Zambrano-Serrano, E., Tamariz-Flores, E. I., Muñoz-Pacheco, J. M., & Torrealba-Meléndez, R. (2020). Fractional chaos based-cryptosystem for generating encryption keys in Ad Hoc networks. Ad Hoc Networks, 97, 102005.

MURUGAN, K. (2020). A SURVEY ON SECURITY SYSTEMS AGAINST INTERNET FRAUD IN E-COMMERCE. Studies in Indian Place Names, 40(12), 1787-1791.

Nan, X. (2020). Cpk-based digital bank, digital currency, and payment method: Google Patents.

Nayanajith, G., & Damunupola, K. (2019). Effects of Subjective Norms and Security on Online Banking Adoption: Multilevel Linear Model Analysis. Asian Journal of Multidisciplinary Studies, 2(1), 9-16.

NO, X. (1997). Federal Deposit Insurance Corporation.

Nustini, Y., & Fadhillah, N. (2020). Factors that Influence the Use of e-Banking and the Effect on Consumptivism. Review of Integrative Business and Economics Research, 9, 330-345.

Ortiz-Yepes, D. A. (2008). Enhancing Authentication in eBanking with NFC-enabled mobile phones. ERCIM News(76).

Pejović, I. (2016). Challenges of Modern Electronic Banking. Paper presented at the Sinteza 2016-International Scientific Conference on ICT and E-Business Related Research.

Rahman, R. U., & Tomar, D. S. (2020). Taxonomy of Login Attacks in Web Applications and Their Security Techniques Using Behavioral Biometrics Modern Theories and Practices for Cyber Ethics and Security Compliance (pp. 122-139): IGI Global.

Robinson, Y. H., & Julie, E. G. (2019). MTPKM: Multipart trust based public key management technique to reduce security vulnerability in mobile ad-hoc networks. Wireless Personal Communications, 109(2), 739-760.

Romney, M. B., Steinbart, P. J., & Cushing, B. E. (2006). Accounting information systems (Vol. 2): Prentice Hall Englewood Cliffs, NJ.

San Martino, A., & Perramon, X. (2008). A model for securing e-banking authentication process: antiphishing approach. Paper presented at the 2008 IEEE Congress on Services-Part I.

Shankar, A., & Jebarajakirthy, C. (2019). The influence of e-banking service quality on customer loyalty. International Journal of Bank Marketing.

Sokolov, D. (2007). E-banking: risk management practices of the Estonian banks. Institute of Economics at Tallinn University of Technology, 101.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, 72, 212-233.

Turner, L., Weickgenannt, A. B., & Copeland, M. K. (2020). Accounting information systems: controls and processes: John Wiley & Sons.

Xueyan, L., & Shuxu, G. (2008). The fourth biometric-vein recognition: INTECH Open Access Publisher.