ISSN: 0067-2904

Consumer Use of E-Banking in Iraq: Security Breaches and Offered Solution

Qusay Zuhair Abdulla*, Mustafa Dhiaa Al-Hassani
Department of Computer Science, Collage of science, Mustansiriyah University, Baghdad, Iraq

Received: 7/12/2021 Accepted: 11/2/2022 Published: 30/8/2022

Abstract

After the software revolution in the last decades, the field of information technology had a tremendous evolution that made many organizations reach the best benefits from this evolution in technologies. The banking sector evolved their old system from ordinary system to the online system. The term E-banking appears to cover almost all bank operations such as money transactions, account management, instant reports, instant notifications. E-banking offers several advantages to clients, but this opens many challenges and motivates unauthorized parties to focus on creating methods and exploiting weaknesses to attack and steal critical information that belongs to the banking system or clients. Iraqi banks recently adopted E-banking serves and made them available to all their clients. However, this shift in approach leaves many clients vulnerable to cyber-attacks. This paper presents an analytical study on Iraqi clients using E-banking as a service using real case studies. Many researchers prevent these threats by introducing novel methods to support cybersecurity specialists. This paper covers related work and the most common terms involving E-banking. It also covers the risks involved in E-banking, most common attacks, and modern security methods to prevent attacks.

Keywords: E-banking, cybersecurity, Risk, Security, Authentication, Electronic fraud.

استخدام المستهلك للخدمات المصرفية الإلكترونية في العراق: الخروقات الأمنية والحلول المقدمة

قصي زهير عبدالله*, مصطفى ضياء الحسني
قسم علوم الحاسوب, كلية العلوم, الجامعة المستنصرية, بغداد, العراق

الخلاصة

بعد ثورة البرمجيات في العقود الماضية ، شهد مجال تكنولوجيا المعلومات تطورًا هائلاً جعل العديد من المنظمات تصل إلى أفضل الفوائد من هذا التطور في التقنيات ؛ طور قطاع البنوك نظامها القديم من النظام العادي إلى النظام عبر الإنترنت. يبدو أن مصطلح الخدمات المصرفية الإلكترونية يغطي جميع العمليات المصرفية تقريبًا مثل المعاملات المالية وإدارة الحسابات والتقارير الفورية والإشعارات الفورية. تقدم الخدمات المصرفية الإلكترونية العديد من المزايا للعملاء ، ولكن هذا يفتح العديد من التحديات ويحفز الأطراف غير المصرح لها على التركيز على إنشاء طرق واستغلالها للهجوم لسرقة المعلومات الهامة التي تخص النظام المصرفي أو العملاء. اعتمدت البنوك العراقية مؤخرا الخدمات المصرفية الإلكترونية وجعلتها متاحة لجميع

*Email: qusayzuhairabdulla@gmail.com

عملائها. من ناحية أخرى ، فإن هذه التقنية الجديدة تجعل العديد من العملاء يعانون من الهجمات الإلكترونية. توضح هذه الورقة الدراسة التحليلية للعملاء العراقيين الذين يستخدمون الخدمات المصرفية الإلكترونية كخدمة عندما تحتوي هذه الخدمة على نقاط الضعف مع دراسة الحالات الحقيقية. يمنع العديد من الباحثين هذه التهديدات من خلال تقديم طرق جديدة لدعم متخصصي الأمن السيبراني. تتناول هذه الورقة الأعمال ذات الصلة والمصطلحات الأكثر شيوعًا المتعلقة بالخدمات المصرفية الإلكترونية. كما يغطي مخاطر الخدمات المصرفية الإلكترونية ، والهجمات الأكثر شيوعًا ، وأساليب الأمان الحديثة لمنع الهجمات.

1. Introduction

Banking services can now be delivered electronically because of the rapid rise of the internet and the widespread use of computers. Iraq has lately been aggressively developing e-banking services that are compatible with the innovative components of the electronic marketplace. As Iraq moves towards industrialization and a knowledge-based economy, the PC and online way of life are becoming more commonplace in the country's daily lives. E-banking has become more well known to the general public, so more individuals are willing to employ technological applications.

Traditional Bank systems migrate their most important data, transactions data, to a software system that can take full responsibility for doing all functions; these systems are known as Banking systems. By the time banking systems evolved to other dimensions, "E-Banking" this new technology; enhanced service quality, cost reduction compared to the traditional services delivered to the customer. These systems work on the internet; however, Internet is a worldwide network that contents nods and computers that allow people to share information and data.

Banking services introduced for the customer are monitoring accounts, checks, deposits, payments via telephonic transfer, Automated Teller Machine (ATM), loans, smart cards, etc. [1].

Banks that conduct business over the internet need adequate technologies to build a secure environment for such activities. E-banking provides many benefits, and by using this technology, the customer can use it remotely. However, many security concerns and threats appear at this point [2]. E-banking security concerns and threats motivate the researcher to provide research, solutions, and future suggestion to avoid security threats [3].

Computer security is more complicated than online security. Attackers have often targeted social media accounts, personal banks accounts, and E-mail accounts. Until now, these attackers hacked into many banks' websites and stole large amounts of data and money through their high level of technical expertise and by exploiting the weaknesses in banking systems. An electronic transaction is entirely reliant on electronic banking. The privacy of software, also known as software security, is what E-banking security focuses on. [4].

According to the number of advantages that E-banking offered, there are several concerns associated with security factors such as privacy and trust, which many researchers have addressed as they greatly impact clients' acceptance of adopting E-banking services. No clients would want to lose their personal banking information and money by being hacked. Some clients do not use or adopt E-banking services without due to lack of trust [5].

Several studies have endeavoured to quantify the effect of security concerns on the client's acceptance of E-banking, especially as early as these electronic banking services are offered to clients. Another significant risk management aspect is how risk is perceived. This explains the worry or fear of missing critical data. Clients would trust E-banking when they know or perceive it to be stable and efficient. [6].

By their very nature, clients are suspicious about the protection, confidentiality, secrecy of transactions, and a financial institution's data integrity. It is now becoming apparent to many financial organizations that security is crucial in developing a strong electronic banking

infrastructure. There is a need to further protect the system before attracting clients. It can be done by enhancing protection. Cybersecurity analysts will say with certainty that any time someone attempts to hack into a bank account, the challenges have become more difficult [7].

It should be remembered that there are many security problems with E-banking. Safe infrastructure for electronic banking and mobile banking is difficult to build because of the many diverse operating systems on various platforms. Consequently, many clients are worried about confidentiality and privacy; financial data is one of the most challenging obstacles for any e-banking adoption [8].

Inadequate privacy and restricted bank protection resources can prevent the bank from improving its efficiency. As a consequence, obtaining additional clients to fund online services would be challenging [9].

The effects of cybercrime on the banking sector's e-transaction technology highlighted that the cybercrime rate has recently risen dramatically, with 80 per cent of cybercrimes originating from outside the country. Banks do not take serious measures to deter cybercrime threats, and, as a result, they do not devote adequate capital to fighting cybercrime. Because of the bank's lack of expertise and capacity to deal with cybercrime threats [10].

In order to satisfy the banking protection criteria, confidential details must be checked by the customer. This authentication must be scalable and reliable, and data must be secured for the client to accept E-banking services. Banks must maintain and build confidence to further increase the level of electronic banking adoption because trust is the core of all financial performance [11] [12].

E-banking needs to provide more secure and hassle-free alternatives in the rapidly changing digitalising world, such as palm, face, and eye recognition, where biometrics such as fingerprint and eye recognition are further integrated to ensure user comfort and security. Biometrics, the measurement of human biological data using fingerprint, facial scanning, and eye recognition, is now adopted by several financial institutions worldwide, resulting in an effective and trustworthy authentication method [13].

The following sections explain E-banking overview with a description of the types of E-banking, after that the Iraqi E-banking system is explained with more details. Next, an explanation of the methodology for applying the statistical study on real clients to understand their security problems is presented. Finally, there is a summary of the most modern attacks on E-banking with the solutions and a discussion section.

2. Electronic banking overview

Early in the 1970s banking industry was evolving when banks sought these types of alternative services instead of traditional banks services. This evolution provided many services such as ATM and systematic fund transfer. At that time, these kinds of services were among the quality difference between banks. [14]. In the early 1980s, the word "e-banking" became common, relating to use a computer system to access banking facilities through a phone-line. Early E-banking offerings were restricted to checking bank balances and paying invoices electronically rather than offering a full transaction banking operation [15].

Formal banking facilities were established in 1995 when the Maryland Presidential Bank had established online banking accounts. Nearly 17% of American adults in the United States used electronic banking in the middle of 2004 [16]. This new term defines online banking systems; that means customer and bank connecting on internet channel [17].

According to banking supervision established by the Basel Committee: “e-banking includes the provision of retail and small value banking products and services through electronic channels as well as large value electronic payments and other wholesale banking services delivered electronically” [16].

This type of service allows users to complete their work remotely with a bank system differently, such as mobile banking and web banking. Several challenges appear when using E-banking. Though it has many benefits such as cost reduction, distance reduction between bank and customer, and speed in completing tasks.

2.1 E-banking types

E-banking refers to digital transfers between banks and clients. E-banking applies to various systems through which consumers may request details or complete purchases via a machine, tablet, or cell phone, based on the customer's needs and the consumer device [16].

The associated types of E-banking services shown in Figure.1 are:

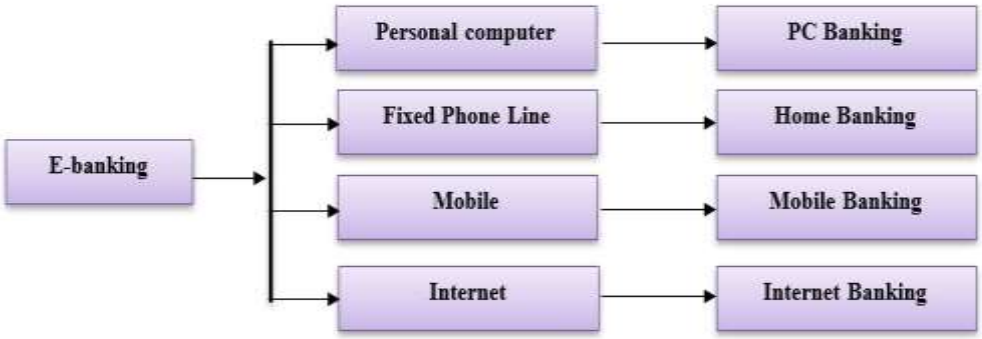

Figure 1-E-banking types services.

2.1.1 PC banking

This term relates to a banking service that allows clients to reach and use services provided by a bank from a PC through banking application software [16]. This software is unique and does not work with other software [18].

2.1.2 Home banking

This term can be defined as banking that permits clients to view their accounts or complete phone transactions. It required installing a fixed phone line for customer security information such as passwords that provide personal information; clients can discuss account balances, transfer money within their accounts, and handle regular transactions [16].

2.1.3 Mobile Banking

It is known as M-banking, a new kind of E-banking service that lets customers maintain multiple financial activities. Depending on Wireless Applications Protocols, technologies for a smartphone require a browser to access personal information [16].

2.1.4 Internet Banking

Since it is delegated to the PC, the service may be defined as either internet-based or web-based. This portal helps consumers use their computers to access both product and service details and make purchases on the same page and access the bank employees, including account transfers, bill payments, and account balances. Customers can contact the bank personnel via the website [16].

3. Iraq E-banking

Iraqi banks started using E-banking in last few years to provide the best service to their clients. However, this new technology needs time and more practice from banks and costumers to use it the right way and avoid the possibility of falling victim to vulnerabilities or attacks on their information. This section shows a statistical study for most effective attacks on banks clients.

3.1 Methodology

This study chose the most commonly used banks in Iraq (Rafidain-bank, Rasheed-bank, IDB-bank, TBI-bank, Taif Islamic Bank). The methodology used to collect data is an online questionnaire containing several multichoice questions to be answered by clients. The items

included in the questionnaire were built based on [19] to assure content validity. Screening questions were asked to ensure that the respondents have previously used e-banking services to ensure their opinions are based on genuine experience. There are three main questions to the survey:

1. Have you ever been exposed to electronic fraud?
2. If someone called you claiming to be from the bank's technical support team and wanted some information about your account, would you give the information?
3. Do you prefer to use more than one method to verify your login to your bank account management software?

The sample used in this study was 595 clients and it explored the client experience with security breaches (fraud, social engineering, phishing).

3.2 Statistical results

This section shows the statistical results by tables and charts reflecting the previous section's questions. Each question had a result table and a chart to explain the results:

Table 1-Exposure to electronic fraud

Bank Name	Client's answer "YES"	Client's answer "NO"	Total Clients
Rafidain-bank	13	124	137
Rasheed-bank	10	23	33
IDB-bank	3	13	16
TBI-bank	2	18	20
Taif Islamic Bank	1	4	5
Total	29	182	211

Table-1 shows 211 samples after filtering by question one. 15% of clients answered "Yes" they were victims to electronic Froud and 85% answered "No." To better visualize the results, the numbers are represented in the chart bellow

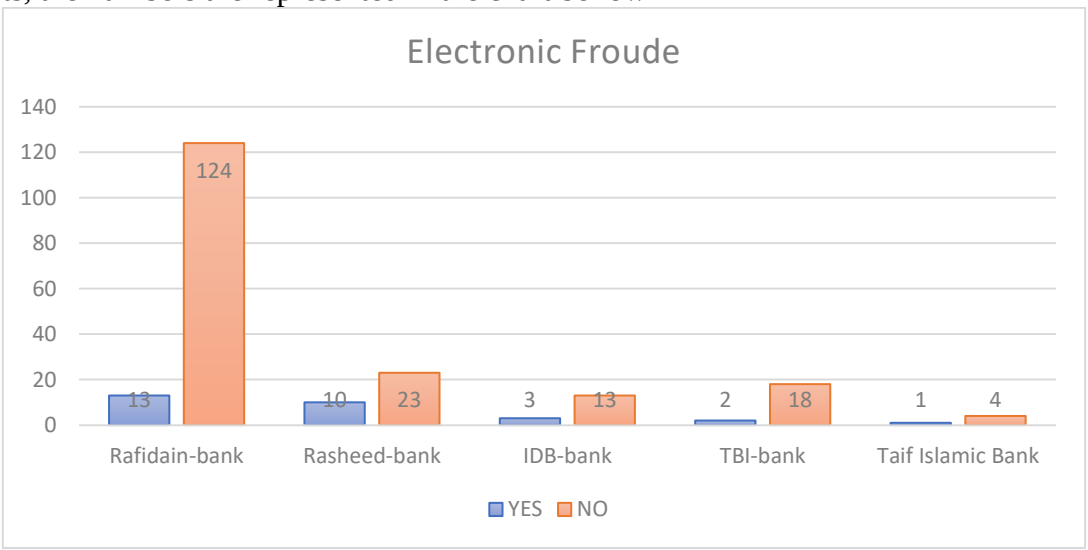

Figure 2-Exposure to electronic fraud

Table 2- Exposure to social engineering

Banks Name	Clints answer "YES"	Clints answer "NO"	Total clints
Rafidain-bank	37	111	148
Rasheed-bank	9	23	32
IDB-bank	6	27	33
TBI-bank	5	8	13
Taif Islamic Bank	1	2	3
Total	58	171	229

Table2: shows 229 samples after filtering by question two, 26% of clients answered "Yes" they will give their secret information, and 74% answered "No." To better visualize the results, the numbers are represented in the chart bellow

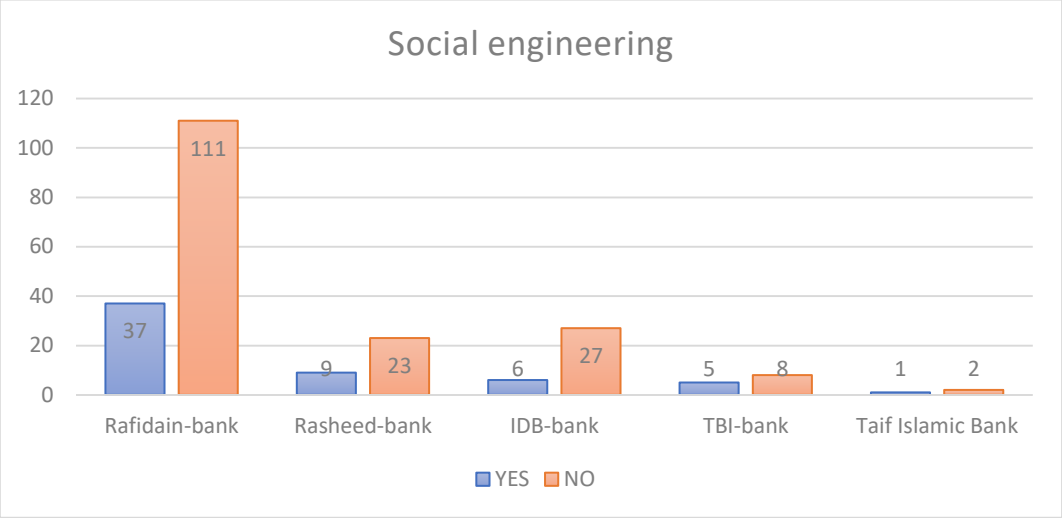

Figure 3- Exposure to social engineering

3.3 Result discussion

According to statistics, results collected from real bank clients shows a clear picture about security breaches (Fraud, Social engineering). That means banks need to apply more security solutions to help their clients. Banks should briefly explain the security breaches that clints may be faced with. The following section will view E-banks' most common security attacks and their solution.

4. Attacks on E-banking Systems

The advancement of financial systems has made customer accounts and transfers a prime goal for cybercriminals. The implementation of E-banking includes many of the threats addressed previously, including security issues. It is concerned with protecting networks and transactions, such as data confidentiality, leakage, modification of records, authentication, unauthorized usage, repudiation, and service unavailability, which may contribute to severe threats, such as hackers. [16]. E-banking networks are vulnerable to a wide range of cyber threats.

4.1 Phishing

Phishing is a type of social engineering approach that is used to mislead people. Users are drawn to messages that appear to come from reputable sources, such as social networking sites, auction sites, banks, emails, online payment systems. Such an automated strategy involves manipulating users to collect sensitive information for financial benefit. Phishing attacks use malicious websites or emails as genuine banking interfaces to request personal information from clients. [2].

Phishers relied massively on spoofed E-mails to activate phishing attacks in which the victims are persuaded to respond with the requested details [20].

4.2 Malware

Malware is a mixture of the terms harmful and malware. Malware is often described as any program that is purposely intended to inflict harm to a device, server, client, or computer network. There are several different kinds of malware, such as computer viruses, worms, Trojans, ransomware, adware, spyware, rogue applications, scareware, and wipers. A virus can corrupt the data on the client's device when transmitted through email or via infected files. Worms migrate themselves from machine to machine individually, spreading security vulnerabilities. Trojans try to steal sensitive information, including usernames and passwords and return it to the attackers [21].

4.3 Pharming

Pharming applies to refined phishing attacks. It is a form of electronic fraud in which users are redirected to a false banking website by changing DNS entries. Consequently, the intruder may access the client's records, which the client inputs into the false website and execute transactions. However, Pharming was influenced by the phrase "farming" and "phishing". Phishing is a method used to capture usernames and passwords. Phishing and pharming have also been used to procure user identities for online identity fraud. Since phishing, carried out on e-commerce or online banking platform has become a problem for businesses [16].

4.4 Denial-of-service (DoS attack)

Prevent targeted consumers from using the e-banking resource by flooding the network. This form of attack is often referred to as a cyber-attack. The attacker tries to bring down a computer or network by removing its linked hosts or severing service to the Internet. [2].

4.5 Distributed denial-of-service (DDoS attack)

Many malicious actors use multiple attack points for their root of assaults, so it is almost difficult to prevent an attack merely by blocking a specific one. The DDoS attack can be compared to a flock of shoppers clustered in a shop's front door, blocking the genuine people from obtaining entrance. Such criminals also choose high-profile websites and internet providers to focus on Distributed Denial of Service (DoS) attacks. Several devices can produce more traffic than one, and this attack is complicated to locate and disable [22].

4.6 Social Engineering Attacks

Currently, social engineering assaults pose the greatest danger to data security. However, they may be discovered but not prevented by users. Social engineers use victims to access private information that may be utilized for particular objectives or sold on the dark web. The growth of Big Data has made it easier for criminals to profit from stolen data [23].

4.7 Spear phishing attack

Phishing attacks that target particular people or groups are known as spear-phishing attacks because they use the victims' identities to make claims or communicate. They call for a thorough investigation of the victim's web history. Unlike other assaults, insider attacks are challenging to detect and differentiate from legal users, which is why they have a high success rate [23].

4.8 Electronic fraud

Electronic fraud is a scam in which funds are fraudulently removed from one bank account and transferred to another bank account utilizing web technology. Identity theft may be accomplished via phishing, lottery scams, and online banking fraud [24].

5. Popular Security Solution Models

One of the primary challenges related to electronic banking is security. Recent approaches have been suggested and implemented to enhance E-banking security. Suggested technologies focus on identity, permission, and authentication. We surveyed the authentication methods used by E-banking providers in this article. They are usually focused on three factors: something the consumer is aware of, biometrics, usernames, and passwords.

5.1 Web Browser Protection

When a website or network allows internet protection, it prevents data and operating systems from being accessed and exploited by incorporating internet security into their browsers. Browser security vulnerabilities mostly use JavaScript, sometimes in conjunction with cross-site scripting (XSS). The browser enables the clients to enter the banking system protected from known malware by controlling the allocated memory range. This approach makes it possible to avoid credential theft and capture [3].

5.2 Anti-phishing (Blacklist-based approach)

It is a collection of URLs that are considered to be malicious. Blacklists are compiled using a variety of tools, including web crawler heuristics and E-voting. When a website is visited, the

browser will be checking it to the blacklist to see if the current URL is already there. It's a malicious website if it covers the Blacklist. As a result, the browser warns users not to send any sensitive data. Blacklists should be kept either locally on the client's machine or on a server that the browser queries for each URL request [25].

5.3 One Time Password

A dynamic password is referred to as a One Time Password (OTP). OTP is randomly generated through a complex algorithm and can't be used more than once. To eliminate password hacking, authentication information theft, and reuse, it is only valid for a single login [21]. There are two types of OTP (Soft-Token, Hard-Token). The soft-Token term means the OTP created by software applications, which are typically installed on the client's smartphone. The hard-Token term means a unique hardware device instantly generates an OTP.

6. Conclusions

Banks have acted as a lighthouse for E-business in recent years. The E-banking revolution has principally impacted the financial landscape by expanding borders and offering new products and services. When banks use E-banking, one of the benefits they get is increased client confidence and satisfaction. Clients can also interact with their banking accounts more effectively and perform various functions, such as making remote financial transactions from anywhere. Additional advantages are increased product lines and broader regional coverage, a reduced distance between clients and banks, 24-hour per day online support for clients, offering high-level security, supporting online purchases using a credit card.

However, E-banking has several risks and drawbacks. This allows the unauthorized party to find several ways to attack E-banking technology. Several risks are known when using e-banking, such as security risk that focused on bank and clients' critical information, operational risk focused on the intrusion on the bank's system, inaccurate processing of transactions, data integrity, the privacy of information. Besides, attacks on E-banking systems have several ways to hack clients or bank information by establishing several attacks such as Phishing, Malware, DoS attacks.

As mentioned earlier in this paper, Iraqi banks and clients need to follow the security policies and handle the E-banks services safely. As mentioned previously in statistical results, many clients suffer from different attacks such as (social engineering and electronic fraud). Drawbacks open the door to researchers to focus on this issue and create novel methods to prevent these risks and attacks. This research cycle continues and grows because of the bank sector's sensitivity, which means the attackers find a new way to attack. Cybersecurity is a great field to research and contribute to this sensitive sector.

References

[1] R. M. Khan, "Customer Affecting-Satisfaction Factors in Electronic Banking Systems: Three Significantly Selected Research Perspectives," *Iraqi Journal of Science*, pp. 271-275, 2021.

[2] Vrîncianu, M., Popa, L. A., "Considerations regarding the security and protection of e-banking services consumers' interests," *The Amfiteatru Economic Journal*, vol. 12, no. (28), p. 388–403, 2010.

[3] Peotta, L., Holtz, M. D., David, B. M., Deus, F. G., Timoteo de Sousa, R., "A formal classification of internet banking attacks and vulnerabilities," *International Journal of Computer Science and Information Technology*, vol. 3, no. (1), p. 186–197, 2011.

[4] Utakrit, "*Security awareness by online banking users in Western Australian of phishing attacks," Edith Cowan University*, 2012.

[5] Akhlaq, "The effect of motivation on trust in the acceptance of internet banking in a low income country," *International Journal of Bank Marketing*, pp. 115-25, 2013.

[6] Ali, "Factor analysis approach of decision making in Indian E-banking: A value adding consumer's perspective," *International Journal of Business Innovation and Research*, pp. 298-320, 2010.

[7] Cuomo, "*Report on Cyber Security in the Banking Sector.," New York State Department of Financial Services*, 2015.

[8] Lee, Huei; Zhang, Yu; and Chen, Kuo Lane, "An investigation of features and security in mobile banking strategy," *Journal of International Technology and Information Management*, vol. Vol. 22, no. Iss. 4, p. Article 2, 2013.

[9] R. Balebako, L. Cranor, "Improving App Privacy: Nudging App Developers to Protect User Privacy," *IEEE Security & Privacy*., vol. vol. 12, no. no. 4, pp. 55-8, 2014.

[10] S. WAITHAKA, "FACTORS AFFECTING CYBER SECURITY IN NATIONAL GOVERNMENT MINISTRIES IN KENYA," UNIVERSITY OF NAIROBI, 2016.

[11] Maruf Gbadebo Salimon,Rushami Zien Yusoff,Sany Sanuri Mohd Mokhtar, "The Impact of Perceived Security on E-Trust, E-Satisfaction and Adoption of Electronic Banking in Nigeria: A Conceptual Review," *Journal of Business and Management*, vol. 17, no. 10, pp. 64-9, 2015.

[12] Abdul WahabH. B., & AbedT. M., "E-commerce Application Based on Visual Cryptography and Chens Hyperchaotic," *Iraqi Journal of Science*, vol. 59, no. (1C), pp. 617-628, 2018.

[13] R. C. Agidi, "Biometrics: The Future of Banking and Financial Service Industry in Nigeria," *IJ of Electronics and Information Engineering*, vol. Vol.9, no. No.2, pp. 91-105, 2018.

[14] A. Mobarek, "E-Banking Practices and Customer Satisfaction - A Case Study in Botswana," 20th Australasian Finance & Banking Conference, 2007.

[15] R. Shannak, "Key Issues in E-Banking Strengths and Weaknesses: The Case of Two Jordanian Banks," *European Scientific Journal*, vol. vol.9, no. (7), pp. 239-263, 2013.

[16] Drig, I., & Isac, C., "E-banking services – Features, challenges and benefits," *Annals of the University of Petroşani, Economics*, vol. 14, no. (1), pp. 49-58, 2014.

[17] Kurnia, S., Peng, F., Liu, Y. R., "Understanding the adoption of electronic banking in China," In 43rd Hawaii International Conference on System Sciences, Honolulu, Hawaii, USA, p. 1–10, 2010.

[18] Liao, S., Shao, Y. P., Wang, H., Chen, A., "The adoption of virtual banking: An empirical study.," *International Journal of Information Management*, vol. 19, no. (1), p. 63–74, 1999.

[19] W.-C. Poon, "Users' adoption of e-banking services:," *Journal of Business & Industrial Marketing*, vol. 23, no. 1, pp. 59-69, 2008.

[20] FolorunsoS. O., AyoF. E., AbdullahK.-K. A., & OgunyinkaP. I., "Hybrid vs Ensemble Classification Models for Phishing Websites," *Iraqi Journal of Science*, vol. 61, no. (12), pp. 3387-3396, 2020.

[21] Park, K. C., Shin, J. W., & Lee, B. G., "Analysis of authentication methods for smartphone banking service using ANP," *KSII Transactions on Internet & Information Systems*, vol. 8, no. (6), 2014.

[22] Charalampos, "Distributed Denial of Service Attacks," The Internet Protocol Journal, 2019.

[23] K. N. Salahdine F, "Social Engineering Attacks: A Survey," *Future Internet*, vol. 4, no. 89, p. 11, 2019.

[24] E. DR. IBANICHUKA, "Electronic Fraud and Financial Performance of Quoted Commercial Banks in Nigeria," *International Journal of Advanced Academic Research*, vol. 5, no. 4, 2019.

[25] Mohammad, "Tutorial and critical analysis of phishing websites methods," *Computer Science Review*, p. 1–24, 2015.