Journal of Artificial Intelligence and Computational Technology

Journal homepage: https://ojs.omgfzc.com/index.php/JECT

Quantitative Studies on Hacking Methods and Types of Cyber-Attackers of Electronic Banking Networks

Mahmoud I. Alfeel, Suliman M M Abakar, Mafawez Alharbi, Ibrahim Abdallah Hageltoum

[1]Department of Computer Sciences Merowe University of Technology. Sudan
[2,3]Department of Natural and Applied Sciences, Community College, Buraydah, Qassim University, Kingdom of Saudi Arabia
[4]Department of Information Technology, Faculty of Computer Science and Information Technology, Kassala University. Sudan.
Correspondence: E-mail: alfeeeeel@gmail.com

Article Info

Article History:
Submitted/Received 14 July 2024
Revised in revised format 21 August 2024
Accepted 25 December 2024
Available 15 October 2024
Publication Date 15 October 2024

Keyword:
Cyber-attacks, Cybercriminals, Electronic Banks, Network Risks, Network Attackers, Hacking Methods & Types.

Cite this article: *Alfeel, M. I., Abakar, S. M. M., Alharbi, M., & Hageltoum, I. A. (2024). Quantitative studies on hacking methods and types of cyber-attackers of electronic banking networks. Journal of Artificial Intelligence and Computational Technology, 1(1)*

ABSTRACT

Cyber-attacks on electronic banking networks are a growing concern in today's digital age. Cybercriminals try to penetrate the Electronic Banking infrastructure, by bypassing all protection mechanisms, and the media continue to report new bank cyberattacks and thefts. The study attempts to identify the impact of attacks and methods that threaten bank networks. To know the kinds and methods of the attackers of bank networks, a questionnaire was prepared and distributed to the selected banks and their branches, namely Omdurman National Bank, Bank of Khartoum, and Bank of Sudan. From the studied sample, competitors stood out as the most qualitative network attackers on the banks, while penetration through the Internet was one of the ways through which the attacks on the financial banks networks could be carried out. The sample of the study showed that the quality of bank attackers are the competitors, with a rate of 29.2%, which is considered the largest percentage of all assumptions and the highest network attacker's method Through the internet with a rate of 52.7%. The study concluded that Competitors and Internet have highest impact per methods and kinds of attacks respectively. This conclusion supports the problem statement since the impact was known within the case study Banks.

1. Introduction

The era of information and networks witnessed at the beginning of the third millennium a tremendous and rapid development in the technologies used, which made the indicators of the volume of dealing in this era grow dramatically. On the threshold of the third millennium, the Third Generation "G3" of the unified system for telecommunications and mobile digital networks, which aims to harmonize and unify the various mobile communication systems in the world in a global communication network called International Mobile Telecommunications-2000 (IMT-2000). This network operates in different environments, supports multimedia, and connects to the Internet and the "web" of personal and mobile devices [1]. With this development, the importance of the issue of information security has increased, so it has already become a problem looking for a solution. This issue has become of concern to all institutions, especially financial institutions, and everyone who has information.

The interests of the ordinary beneficiary, companies that provide information services, system and application designers, as well as companies developing hardware and software, and with the development of technology and means of storing information and exchanging information in various ways or the so-called transfer of data across the network from one location to another, have become a matter of security of that data and information is a significant concern and vital issue [2].

The rapid evolution of technology has transformed the financial sector in the world, empowering organizations with innovative tools and platforms to enhance their operations, but it has also exposed them to a plethora of digital security threats [1], [2]. In this era of digitalization, computer network security has become paramount in safeguarding sensitive financial data, transactions, and the trust of customers. Understanding the challenges faced by the financial sector and identifying effective solutions for mitigating digital security threats is of utmost importance [3], [4], [5].

Before 30 Years back Banks are protected from money stealing by gun guards standing 24 hours at the bank's building and later CCTV Cameras deployed to monitor the suspected people who are may be criminals. However, today's criminals can penetrate the bank's infrastructure, which is usually quite well-guarded. Nonetheless, criminals still manage to bypass all protection mechanisms, and the media continue to report new bank cyberattacks and thefts. In the wild, we currently see attacks on interbank transfers, card processing, ATM management, e-banking, and payment gateways. The range of targets is broad—if intruders have the necessary knowledge and technical means, access to such systems can bring them more revenue than fraud against bank customers [3]. Attackers are faced with the task of gathering as much information about the bank as possible to breach security systems and "case" the bank. Since the use of external resources can be detected by security systems, in order not to get caught during this initial stage, criminals resort to passive methods of obtaining information: for example, identifying domain names and addresses belonging to the bank. At the survey stage, unscrupulous bank employees are actively engaged as well. These insiders are prepared to disclose information for a fee, as shown by numerous offers on web forums. Criminals can lurk in a bank's infrastructure for months or even years, remaining stealthy as they collect information about the infrastructure and processes, leisurely examine the systems selected for attacks, and observe employees' actions. This means that theft can be prevented if compromises are detected quickly, even after criminals have already penetrated the bank network and gained a foothold.

The main methods of theft are [3]:

- Transferring funds to fictitious accounts through interbank payment systems
- Transferring funds to cryptocurrency wallets

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

- Controlling bank cards and accounts
- Controlling ATM cash dispensing

It is also to protect certain information from being viewed, or used by people who are not authorized to do so, or from being disclosed to the public, distributed, modified, or destroyed or deleted. Therefore, information assurance is not only related to information security, but also to securing systems where information is circulated, stored, and its contents, as well as by strategic procedures for managing information security-related risks [4].

All the technologies the world has reached cannot be used without information security. For example, the banking system, if there was no information security, anyone could enter the system, change their account, and become a millionaire out of nothing. There is no doubt that the field of information security is of great importance, this field secures information and protects it from the dangers that surround it, and the field of information security is one of the vital, renewable, and much required fields, as it is absolutely indispensable. The rest of the Paper is organized as follows: Section 2: represents Related Works, Section 3: illustrates the Problem Statement, Section 4: explains the Research Methodology, Section 5: represents some Discussion and finally Section 6: reports the Conclusion of the research.

dustries and have also been successfully applied to predict crop yield in other studies. [5]

2. Related Works

The financial sector in many countries has witnessed remarkable growth in recent years, driven by technological advancements and a surge in digital financial services [6], [7], [8]. As financial institutions and businesses continue to embrace digitalization, they have become attractive targets for cybercriminals seeking to exploit vulnerabilities in computer networks [7]. These threats include but are not limited to, data breaches, ransomware attacks, phishing scams, and insider threats. The consequences of such security breaches extend beyond financial losses, impacting customer trust, regulatory compliance, and the overall stability of the financial system [9], [10].

The Current research is directed towards attacks and malicious activities identification in online banking systems. Cybercriminals carefully monitor publication of new vulnerabilities and quickly modify their tools to take advantage. For example, in 2017, Cobalt hackers used vulnerabilities in Microsoft Office (CVE-2017-0199 and CVE-2017-11882), expecting that banks had not managed to install appropriate security updates. Inside the network of a target bank, the intruders are able to move freely using known vulnerabilities and legitimate software while remaining unnoticed by administrators. The key point is that if an attack is detected and stopped in time, intruders can be thwarted. Preventing losses is possible at any stage if appropriate protective measures are taken [3]. This is why security events must be monitored by an internal or external security operations center (SOC) with use of security information and event management (SIEM) solutions, which significantly facilitate and improve the processing of information security events [3]. Types of attacks: In order to propose security models and radical solutions, it is necessary to understand and to determine, at first, the attack methods and the existing vulnerabilities on which they are based [5]. The search attempted to categorize and classify the diverse sorts of attacks against the E-Banking in different ways. The main security threats or attacks of electronic banking platforms are; denial of service, illegitimate use, disclosure of information and repudiation [6]. However, a model solely based on legitimate user identification is not computationally efficient due to the growing number of online banking systems users. Other researchers have presented a classification for the current attacks on the online banking

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

systems [7]. Another study proposed a hierarchy causes that included three main categories; legitimate access, control of devices, and theft of property [8]. There is a model (Attack Weapon Model) that presents the main and the effective attacks, explains how to exploit inherited vulnerabilities (social engineering and phishing attacks) and takes control of software (malicious software) and identity theft of a legitimate user (fake pages of websites and malicious software). Such a grouping is one of the such as: secure Internet, secure mobile applications, secure electronic money, etc. They mentioned that today, attacks are more complicated, combined and wider, then more former and common solutions are no longer used and there is a need for new more powerful methods [9]. Also, there is a solution for detection of behavioral anomalies proposed for banks in order to detect the financial transactions made in suspicious circumstances, but this solution is implemented in the internal systems only, hence its limitation [10]. And finally, one of the most relevant results revealed that even the strongest passwords can be easily guessed with dictionary attacks or via Key-loggers (via sniffers, snoop-ware,). In order to overcome this risk, electronic banks have included virtual keyboards in their applications, but the risk remains latent when a hardware Trojan in the VGA screens can capture any sensitive information inserted via a virtual keyboard, which constitutes a new security challenge in mobile banking [11]. Some of the authors introduce attack techniques focused on vulnerabilities which are present in a specific internet banking system, presenting attack implementation results. However, a model solely based on legitimate user identification is not computationally efficient due to the constantly growing number of online banking systems users. Banks need to increase prescriptive approaches to cybersecurity. This research will focus on the type of e-banking attackers and E-Banking Network penetration methods i.e. in what ways can network be penetrated?

Kumar et al. they presented a technique named Crop Selection Method (CSM) to select sequence of crops to be sowing over season. This method takes crop, their sowing time, plantation days and predicted yield rate for the season as input and finds a sequence of crops whose production per day are maximum over season. The crop sowing table data are gathered from farmer(s) of Patna District, Bihar (India). Performance and accuracy of this method depends on predicted value of influenced parameters so there is a need to adopt a prediction method with more accuracy and high performance. [23]

This is a research project on the management of crops, Karthikeyan et al. explored the efficiency and usefulness of the crop deployment methods. They used Random Forest technique, which showed it can make an efficient processes and the accuracy of the prediction is high. [24] The work done by Waikar et al. [9], it built a system that suggest crop based on soil classification with assembling classifiers system has been created. The system combined Artificial Neural Network (ANN), Bagged Tree, Naive Bayes, Adaboost, and Support Vector Machine (SVM) algorithms to improve the accuracy of the selection which gives the list appropriate crop according to the soil type. In order to anticipate the crop selection for an increase in crop yield rate and to provide more profit to the farmers, this study used the Crop Variety Selection Method, or CVSM, which used machine learning techniques and artificial learning algorithms in agriculture. Waikar et al. suggest that the more input parameters, such as micronutrients, fertilizer needs, and disease susceptibilities, the more precise and trustworthy the findings of production rate prediction. [14] This work introduced by Majumdar et al. [10], which focuses on the analysis of the agriculture data and finding optimal parameters to maximize the crop production using data mining techniques, based on historical data of crop yield. It covered the Partition around medoids (PAM), clustering large applications (CLARA), Modified DBSCAN clustering methods and multiple linear regression method. Using these methods crop data set is analyzed and determined the optimal parameters for the wheat crop production. They used Multiple linear regression to find the significant attributes and form the equation for the yield prediction. This work

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

found out that DBSCAN gives the better clustering quality than PAM and CLARA, CLARA gives the better clustering quality than the PAM. Becker et al., work on agriculture planning, to analyze and predict the crop using soil properties parameters. There are 1600 datasets used in this application, support vector machine model used to train and test this application. The accuracy achieved to predict the suitable crops and fertilizers for the field using the SVM model is 100%. [25]

1.1 Network Threats:

It has become very clear in spite of all the advantages and benefits of the information network to the world, as it is now always threatened by crimes and dangers of information, data, sites, files and rules available through it, which cost people or organizations very large financial losses. Among the most important of these threats or risks are the following [1]:

- Massive penetrations threatening the security of information and data
- Expansion of the use of the network
- The nature of material circulating over the network

After all the above talk about the dangers facing information networks and their protection systems, we would like here to list the sources through which a threat or breaches of information networks can be formed, namely:

First: Internal Threat

Internal threat means attackers from within the scope of the information network; the most important aspects of internal hazards are as follows [13]:

a- Hacking information systems by stealing, switching, changing or deleting.
b- Finding and creating loopholes in the network security system.
c- Changing the configuration of the information network system.

A report issued in the United States of America in 2003 showed that 36% of the agencies consider that internal users are more dangerous to the information systems available within these institutions than external danger [14].

We find that there are a number of motives, for example [15].

a- Cases of dissatisfaction.
b- Proof of self.
c- Take advantage of material.

Second: External Threat

External threat, of course, means that people who make attempts to penetrate the security of networks from outside the institutions, whether they are connected to these institutions or not [12].

1.2 The Concept of Electronic Banks:

The term electronic banking or Internet banking is used as a sophisticated and comprehensive expression of concepts that emerged in the early nineties such as the concept of remote financial services, remote electronic banking, home bank, or online bank (Online

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

Banking) or Self - Service Banking, all of which are expressions related to customers managing their accounts and completing their business related to the bank through the home, office or any other place at the time the customer wants. [16].

There are three basic forms of electronic banks on the Internet [17]:

1- The information site

2- The communication site

3- Reciprocal Location

1.1 Electronic Banking Threats:

In the banks' practice of their electronic business, they face risks that result in financial losses, and from these risks they can be classified into different groups represented in the following [18]:

- Technical Risks
- Fraud Risk
- Risks arising from the malfunction of the electronic system
- Legal risks
- Sudden Risks
- Technological risks

2. Problem Statement:

Cybercrime is continuing to evolve and advance quickly, making it crucial that instead of hiding incidents, banks pool their knowledge by sharing information on industry attacks, learning more about relevant indicators of compromise, and helping to spread awareness throughout the industry. Therefore, taking advantage of flaws in corporate network security, the intruders are able to gain full control over the bank's infrastructure within a short period. Lack of understanding types and methods of E-Banking attacks always lead missing of increased continues attacks to the E-Banking Networks. Cybercriminals target banks because their data is more valuable. Whereas information on a social media site may lack detail or accuracy, bank data will contain details such as addresses and dates of birth. This data has inherent value and can be used for other malicious activity such as ID fraud, which makes the consequences of attacks more devastating. With more services being offered online and increasing the risk of data breaches, there's now a greater emphasis to examine the importance of attacks types and methods. So far, cybersecurity strategies across industries have focused on reacting quickly after problems occur. But strategies need to be more anticipatory than reactive; after all, prevention is better than cure. The problem of indicating certain types and methods of E-Banking attacks namely, in the case study Banks is highly demanded. The research's problem will focus on the revealing of types of e-banking attackers (Competitors Banks, Internal staff, Individuals who have different views and Individuals who want revenge) and E-Banking Network penetration methods i.e. in what ways can network be penetrated? (Through the internet Network penetration methods Internal systems (from within the bank), Through the different branches of the bank).

4. Research Methodology:

The study examined some penetration methods and the efficiency of bank attackers from the perspective of both the Central Bank of Sudan, the Khartoum Bank and the National Bank of Omdurman.

First: Such banks were chosen Because they are among the country's largest and most important financial institutions in terms of the number of clients and branches.

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

Second, an initial questionnaire was designed and distributed to identify the risks of banks in general, consisting of 20 experts in the field of banking security. Third, the questionnaire was distributed to random sample numbering 179 participants of 874 forming the total population of the study.

Fourth, the sample size was determined according to the Law on the Use of Specifying the Sample Size in Descriptive Studies [20]. The following law:

$$N = (Z2\ \alpha/2\ P(1-P))\ /\ D2 \quad \ldots\ (1)$$

P: proportion of employee (good)

$$P = 50\% \quad = 0.5 \quad \ldots (2)$$

$$1-p = 50\% = 0.5 \quad \ldots (3)$$

$Z\alpha/2$: critical value

(Available in the normal distribution table)

α=significance level

Finally, the data was analyzed using SPSS.

4.1 The types of the network attackers: -

To know the dangers threatening the networks, we must know the source of this attack and the types of attackers and the motives that led to the attack. The attack depends on the type of system to be hacked and banking and banking systems are among the most penetrated systems. To know the quality of the attackers of the banking networks, a number of assumptions were made to the sample members, and the results were as follows:

Table (1) shows the type of network attackers

Type of network attackers	Count	Pct. of Responses	Pct. of Cases
Internal staff	45	18.5%	27.4%
Competitors Banks	71	29.2%	43.3%
Individuals who have different views	47	19.3%	28.7%
Individuals who want revenge	32	13.2%	19.5%
Individuals who want to be famous	48	19.8%	29.3%
Total responses	243	100.0%	148.2%
15 Missing cases:164 valid cases			

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

Firstly, Competitors Banks: - Competition has become large between companies in all fields, and competition may take a number of forms, including carrying out attacks on the systems of competing institutions, stealing designs or financial reports or destruction of customer data, if the work in a financial institution, for example, has high competition, then The aspiring competitor sees some interest in sabotaging the network of this institution and making it unusable [14].

The sample of the study confirmed that the quality of bank attackers are the competitors, with a frequency of 71 and 43.3%, which is considered the largest percentage of all assumptions.

Second, Individuals who want to be famous: - Fame is one of the desires for which the networks of large institutions are penetrated and its site receives a large number of visitors. Therefore, the attacker's goal is to obtain fame and satisfy vanity, for example the primary purpose of the attack on large companies such as Microsoft, YAHOO It is fame [15].

According to the individuals in the study sample, the individuals who wanted to fame as a result of their attacks on the bank's sites were in second place with a frequency of 48 and a rate of 29.3%.

Third, Individuals who have different views: - If one of the institutions operates in controversial areas, there will be different views on its business, such as an institution that sponsors the human cloning process and is vulnerable to threats from different points of view with it, and sabotage is deliberate, as some people consider banking institutions as institutions. Usurious and especially non-Islamic banks [21].

The results of the study showed that the type of attackers of the bank from individuals who have different views or goals in third place, with a frequency of 47 and 28.7%.

Fourth, the Internal staff:- The local staff represent one of the threats to the networks, as not every employee adheres to the insurance procedures within the relevant institution, so we must not completely trust all the local employees, so they can be monitored during working hours by setting up surveillance cameras to monitor their presence inside the institution and create a special password for each device from The banking system, adhering to these procedures reduces the problems caused by employees [14] [22].

Through the study sample, it was found that the local employees represent 27.4% and the frequency of 45 of the network attackers, and this percentage comes in the fourth place.

Fifth, Individuals who want revenge: - The purpose of the attack may also be revenge on the institution by attacking its location and files for a number of political, religious, etc. motives. As for the field of work, revenge is through a former employee who has been separated from work, and this motive represents the most motive for revenge. A risk for the employee to possess a set of information that enables him to penetrate [13] [23].

The revenge came as the lowest assumption of the targets of the attack on the networks by 19.5% and with a frequency of 32.

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

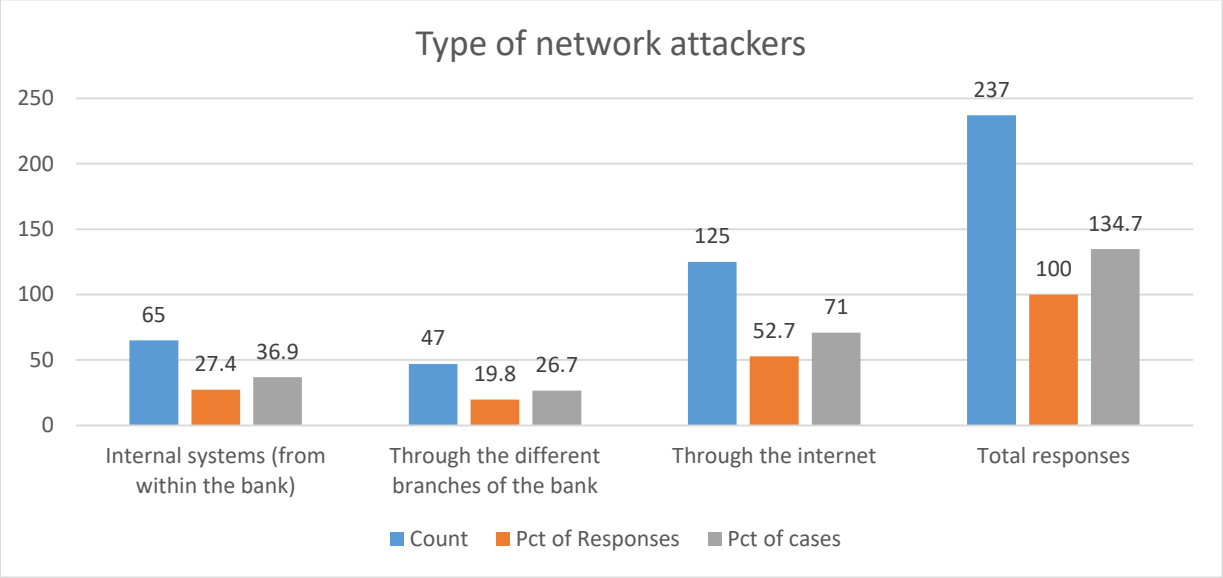

Figure (1): Shows the type of network attackers

4.2 In what ways can network be penetrated?

Studies indicated that most of the breaches on network insurance systems are from within institutions. Studies have shown that about 80% of breaches on networks have been carried out by individuals from within these institutions or by individuals who have internal information and according to estimates by the Computer Security Institute (CSI), the costs of the attack The inside is $ 2.7 million per attack, while the rate of one attack coming from abroad does not exceed $ 7,000 [1] [13].

A set of assumptions was made to the individuals of the sample to know the ways in which the banks 'networks are attacked. The results were as follows:

Table (2): Shows Ways to Penetrate Networks

Network penetration methods	Count	Pct. of Responses	Pct. of cases
Internal systems (from within the bank)	65	27.4%	36.9
Through the different branches of the bank	47	19.8%	26.7
Through the internet	125	52.7%	71.0
Total responses	237	100.0	134.7
3 Missing cases:176 valid cases			

First, the Internet: - One of the most important things that characterizes our era is the large number of information, as strategic studies have indicated that the amount of information produced in the last ten years only equals the information produced by mankind throughout the past time periods [2], this means every ten years in an era Information, and perhaps less in the future, is sufficient to double the amount of information produced by mankind, due primarily to the expansion of the Internet.

The number of Internet users in the world exceeded the number of one billion users for the first time in December of 2008, and China leads the largest number of Internet users, as the number of users reached 298 million users, followed by the United States in the second place with 163 million users and Japan came in third with 60 million users. This huge number of users led to a number of risks when

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

connecting to the Internet. When using private credit cards over the Internet, another party can obtain the numbers of this card. Also, online selling sites can be false sites [12].

According to the study sample, the internet penetration methods came with a frequency of 125 and a percentage of 71.0%, and this percentage represents the largest percentage of network penetration methods.

Secondly, the internal systems: Most of the security systems are based on protecting networks from external breaches, but there is an important aspect is the local employees who have accurate information about those systems and how they work [18] [19].

When designing a security system, these local employees must be taken into consideration and monitored, and preventive measures can be applied to prevent any employee from being in a place not assigned to him. Each employee must adhere to the floor on which he works, and by applying this system we reduce local penetrations that occur from within the institution [24].

According to the study sample individuals, the ways in which the network can be penetrated, the internal systems came second with 36.9% and a frequency of 65.

Third, the branches: - Most Sudanese banks have different branches in most states. Some banks also have branches outside the country to facilitate the linking of the customer during his travel abroad. These branches come in many positive aspects that are not hidden to anyone, so it can be used to provide the service in any place that needs it Client.

But those branches cause some problems. The larger the size of the institution, it is difficult to control and increase the problems and penetrations in that network that connect these branches with each other [25]. Hence the question comes about how to control these branches and how to secure the transactions sent and received through them.

To secure the communication process between the branches, a number of procedures can be applied by creating a virtual private network (VPN) between these different branches in order to secure communication lines between all branches [2]. The importance of this network is that it secures all information exchanged between the parties to the network where Transfer it through an encryption channel, whether this information is transmitted through the FTP service, FTP email, webpage, or other transmission services. There are also other security techniques such as firewalls and data encryption systems [2].

And according to the study sample, the different bank branches were chosen with a frequency of 47 and 36.9%, and this option comes in the third rank of attack methods on the network.

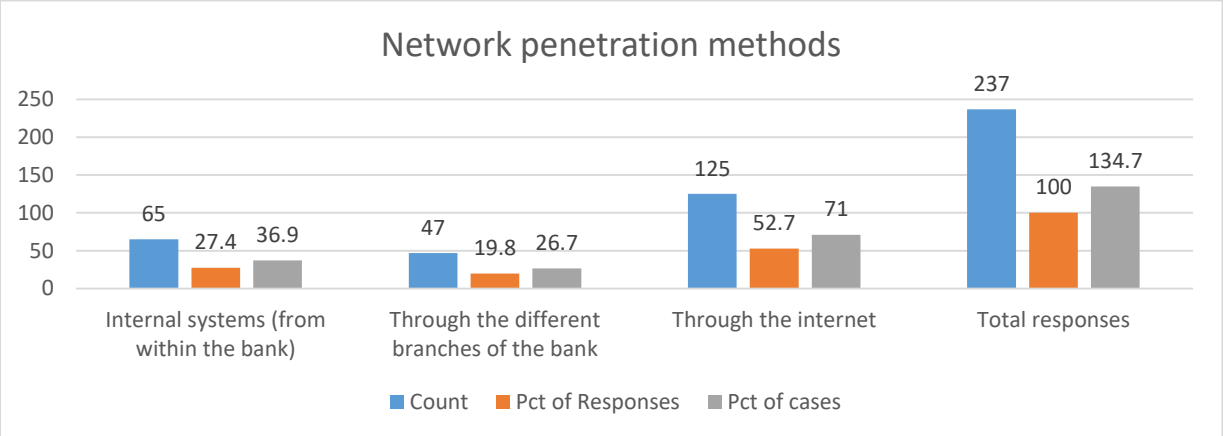

Figure (2): Shows ways to penetrate networks

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

5. Discussion:

Based on the analysis of a number of the risks of financial banks and according to the opinions of the studied sample, competitors stood out as the most qualitative network attackers on the banks, while the penetration through the Internet was one of the ways through which the attacks on the financial banks networks could be carried out.

Given the great importance of information technologies in all banks and banks in this era, and the increasing dependence on information and communication networks, all this increases the impact of the risks that banking operations may face.

Therefore, it is necessary to continue the processes of seeking and attention to developing the necessary technical methods and means to confront these dangers. In addition, finding the best administrative rules that contribute to supporting this confrontation in order to reduce the potential dangers to all financial banks and banks and even strive to get rid of them is essential for such work.

In order for electronic banks to play their role effectively, it must work to control communication technologies, protect the Internet from fraud, and ensure the confidentiality of all banking operations.

The importance of supervisory bodies in financial institutions to provide high-level training courses, workshops and conferences with the participation of advanced international bodies in the field of information technologies to introduce technical squads and bank employees to the latest technologies to keep pace with rapid development, along with the importance of developing Arab regulatory agencies for a clear monitoring mechanism on banks and financial institutions to ensure whoever checks the insurance controls like the international banks and banks.

Financial institutions and banks must also obtain the latest technology, whether either hardware or software, to meet the latest developments and methods used in the field of insurance against piracy, electronic attacks, and work to intensify awareness among clients through audio and video programs and educational seminars, to raise the level of security culture Informatics, and finally, stressing the importance of conducting bank security checks on an ongoing basis.

6. Conclusion:

The research addressed the identify types and methods of E-Banking attacks. Knowing attackers and their methodology can easily support detecting Cybercriminals bypass the E-Banking protection. Cybercriminals carefully monitor publication of new vulnerabilities and quickly modify their tools to take advantage. Cybercrime is continuing to evolve and advance quickly, making it crucial that instead of hiding incidents, banks pool their knowledge by sharing information on industry attacks, learning more about relevant indicators of compromise, and helping to spread awareness throughout the industry. The study is an attempt to identify the impact attacks and methods that threat Banks networks.

A review of some related works have addressed including Network Threats (Internal Threat and External Threat), the Concept of Electronic Banks and Electronic Banking Threats then problem have been stated based on the review. Research Methodology carried based on the questionnaire outcomes, in order to know the kinds and methods of the attackers of Banks networks. The questionnaire was distributed to the selected banks and their branches, namely: Omdurman National Bank, Bank of Khartoum and Bank of Sudan. From the studied samples, Competitors Banks stood out as the most qualitative network attackers on the banks, while the penetration through the Internet was one of the ways through which the attacks on the financial banks networks could be carried out. The sample of the study showed that the quality of bank attackers are the competitors, with a rate of 29.2%, which is considered the largest percentage of all assumptions and the highest network attacker's method

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

Through the internet with a rate of 52.7%. The study concluded that Competitors and Internet has highest impact per methods and kinds of attacks respectively.

Reference:

Bishop, M.A. ,2012. The art and science of computer security.

Pahlavan, K. and Krishnamurthy, P., 2009. Networking fundamentals: Wide, local and personal area communications. John Wiley & Sons.

Finance/Banking, how hackers rob banks, Published on May 21, 2018, https://www.ptsecurity.com/ww-en/analytics/banks-attacks-2018/

Jacobs, S., 2011. Engineering information security: The application of systems engineering concepts to achieve information assurance (Vol. 14). John Wiley & Sons.

Meriem Tabiaa, Banking: Security risks, previsions and recommendations, IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.11, November 2017.

E. Abu-Shanab and S. Matalqa, "Security and Fraud Issues of E-banking," Proc. Int. J. Comput. Netw. Appl., vol. 2, no. 4, pp. 179–187, 2015.

S. Geramiparvar and N. Modiri, "Security as a Serious Challenge for E-Banking: a Review of Emmental Malware," Int. J. Adv. Comput. Res., vol. 5, no. 18, p. 62, 2015.

S. Kiljan, K. Simoens, D. D. Cock, M. V. Eekelen, and H. Vranken, "A Survey of Authentication and Communications Security in Online Banking," ACM Comput. Surv. CSUR, vol. 49, no. 4, p. 61, 2016.

P. Peris-Lopez and H. Martín, "Hardware Trojans against virtual keyboards on e-banking platforms–A proof of concept," AEU-Int. J. Electron. Commun., vol. 76, pp. 146– 151, 2017.

Z. Hussain, D. Das, Z. A. Bhutto, M. Hammad-u-Salam, F. Talpur, and G. Rai, "E-Banking Challenges in Pakistan: An Empirical Study," J. Comput. Commun., vol. 5, no. 02, p. 1, 2017.

H. G.Mark, "SANS Institute Survey Reveals 2016's Biggest Cyber Security Threats and Risks in the Financial Sector," Dec-2016.

Douligeris, C. and Serpanos, D.N., 2007. Network security: current status and future directions. John Wiley & Sons.

B.A Forouzan, Cryptography AND network security, McGraw-Hill, Inc, 2007, PP 35-112.

O. Syniavska, N. Dekhtyar, O.Deyneka, T. Zhukova, and O. Syniavska, "Security of e-banking systems: modelling the process of counteracting e-banking fraud," In SHS Web of Conferences ,Vol. 65, p. 03004, EDP Sciences, (2019).

W. Stallings, Cryptography and network security: principles and practice, Upper Saddle River: Pearson, 2017, pp. 92-95.

A. N. Isfahan, A. Mircholi, A. Asadi, and M.A Vasfi," A study of the effect of E-bank service on E-trust: An E-security approach," In 7th International Conference on e-Commerce in Developing Countries: with focus on e-Security pp. 1-10, IEEE., 2013, April

N. Yildirim, A Varol, "Research on Security Vulnerabilities in Online and Mobile Banking Systems, In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) ,pp. 1-5,. IEEE. ,2019, June.

A. Bouveret, Cyber risk for the financial sector: a framework for quantitative assessment. International Monetary Fund,2018, PP.25 -91.

S.A.H Seno,O .G Bidmeshk, and K. Ghaffari, "Information security diagnosis in electronic banking (case study: Tejarat bank's branches of Isfahan," In 2015 9th International Conference on e-Commerce in Developing Countries: With focus on e-Business (ECDC), pp. 1-8,. IEEE, 2015, April.

W. Cochrane, Theory and practice of electron diffraction, 1993, PP 25-73.

Stinson, D.R., 2005. Cryptography: theory and practice. Chapman and Hall/CRC.

P. Subsorn, S. Limwiriyakul, "A case study of internet banking security of Mainland Chinese Banks: A customer perspective" In 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks, pp. 189-195, IEEE, (2012, July).

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243

C Johanson, “Information Security Basic,”, Journal of Information System Security Association (ISSA), pp. 28-34., 2010.

N. Yildirim, A Varol, “Research on Security Vulnerabilities in Online and Mobile Banking Systems, In 2019 7th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-5, IEEE. ,2019, June.

Z. B. Omariba, N. B. Masese and D. G. Wanyembi, “SECURITY AND PRIVACY OFELECTRONIC BANKING,” IJCSI International Journal of Computer Science Issues, vol 9, no. 4, pp. 432-446.

DOI: https://doi.org/10.70274/jaict.2024.1.1.18.
p- ISSN 34562-3478 e- ISSN 5443-1243