ISSN: 2182-2069 / E-ISSN: 2182-2077

Assessment of Cybersecurity Risks and threats on Banking and Financial Services

Rami Shehab[1*], Abrar s.alismail[2], Dr. Mohammed Amin Almaiah[3*], Dr. Tayseer Alkhdour[4], Dr. Belal Mahmoud AlWadi[5], and Dr. Mahmaod Alrawad[6]

[1*]College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia. Rtshehab@kfu.edu.sa, https://orcid.org/0009-0007-4262-921X

[2]College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa Saudi Arabia. 222401435@student.kfu.edu.sa, https://orcid.org/0009-0003-7104-3331

[3*]King Abdullah the II IT School, University of Jordan, Amman, Jordan. m.almaiah@ju.edu.jo, https://orcid.org/0000-0002-2215-2481

[4]College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia. talkhdoue@kfu.edu.sa, https://orcid.org/0009-0007-0158-1301

[5]Management and Entrepreneurship, Al-Zaytoonah University of Jordan, Amman, Jordan. b.alwadi@zuj.edu.jo, https://orcid.org/0000-0003-1677-1275

[6]Department of Quantitative Methods, College of Business, King Faisal University, Saudi Arabia. malrawad@kfu.edu.sa, rtshehab@kfu.edu.sa and m.almaiah@ju.edu.jo, https://orcid.org/0000-0002-8871-3392

Received: March 08, 2024; Revised: May 07, 2024; Accepted: June 12, 2024; Published: August 30, 2024

Abstract

Technology is important in all aspects of our lives, particularly in the banking sector. Advanced technologies resulted in a fundamental shift in the way banks operate. Malicious use of technology leads to security breaches, customer distrust, financial instability, and other forms of cybercrime. This paper focuses on the most important threats and challenges to be considered while interacting with banks and financial institutions. Significant number of literatures will be reviewed to identify the most common threats and attacks on banks and financial institutions sector, as well as appropriate mitigation techniques and countermeasures. This paper focuses on bank and financial services institution infrastructure vulnerabilities that are escalating attacks on the sector and affecting the banking system, individuals, and organizations. The security study in these 35 projects demonstrates how cyber intrusions continue to attack the financial sector due to the weakness of security defense and data containment. It turns out that malware attacks are the most common threats to banks and financial institutions. Sharing and exchanging information between banks and financial institutions, as well as best practices taken by bank cards issuers and users are the most effective mitigation techniques. Some previous studies proposed a successful model for mitigating the impact of threats on banks and financial institutions, as well as reducing risks that cannot be mitigated using current mitigation techniques. According to banks and financial services statistics and surveys, existing

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 3 (August), pp. 167-190. DOI: *10.58346/JISIS.2024.I3.010*

*Corresponding author: College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia; King Abdullah the II IT School, University of Jordan, Amman, Jordan.

controls and laws do not provide appropriate security meet the banks and financial services institutions systems' demands and requirements.

Keywords: Cybersecurity, Threats, Attacks, Challenges, Risks, Banks Security, Financial Services Institutions Security, Attacks Mitigation, Countermeasures.

1 Introduction

Technology plays a critical role in various areas of our life, especially in the banking sector. Technology has effectively enhanced the banking sector and financial services institutions. Stunning development in technology brought a fundamental turning point in the way the banking sector works, which provided many opportunities for banking institutions toward enhancing and improving the level of services provided to customers. Nowadays, technology has contributed to banks and financial services institutions in providing banking and financial services through electronic transactions, which leads to saving time, effort, and money.

Despite the opportunities and possibilities that technology creates in the banking sector, it also represents a special challenge for the banking sector and financial services institutions (Paul Thomas & Rajini, 2024). We are all aware that malicious use for technology leads to disruption of the infrastructure of banks and financial services institutions, breach of security, customer trust, endangering financial stability, and other cybercrime. An information security breach may occur suddenly at any time as everything is integrated with the internet and cybercriminals who are manipulating the Internet of banks and financial services institution things are able to hack banks customer data and steal financial institutions customers' money digitally (Tariq, 2018).

With the significant increase in the technology in the banking sector, the risks associated with technology have increased. Therefore, many types and forms of cybersecurity attacks/threats appear every day regarding the banking sector. Cybersecurity attacks pose a threat to the entire financial system, this fact is confirmed by reports issued in this regard at the international, regional, and local levels. In this context, the world bank reports indicate the concentration of cybersecurity attacks in banking sector and financial services institutions, which in 2016 witnessed a significant jump in cybersecurity attacks by 65 %, representing an increase of 29 % over the previous year. Also, the global bank reports indicate that thefts against the financial sector using malware increased by 80 % per year in 2015 compared to the previous year, while these attacks accounted for 38 % of reported incidents in 2015, up from 23 % in 2014 (Camillo, 2017).

The emergence of a multinational gang of cybercriminals (Najaf et al., 2021) in late 2013 which carried out a series of sophisticated cybersecurity attacks close to 100 attacks against banking entities around the world. These attacks occur by cybercriminals using "Car bank" attacks sending fraudulent response emails to bank employees in order to infect bank systems with customized malware that contains video files to capture the activities of bank employees (Srinadi et al., 2023). Cybercrime is one of the main challenges facing financial institutions (Najaf et al., 2020) as it leads to money theft, leakage of sensitive data and significant financial loss. Based on Group IB experts' assessment of discussing cybercrime facing financial institutions, nearly 99% of cybercrimes facing financial institutions are money theft, which destroyed many companies in 2017, such as MDLZ and DLA Piper, in addition to identity theft, and Equifax was one of the victims where cybercriminals use sensitive personal information and use it for identity theft. In 2018, the World Economic Forum noted fraud and financial crimes, which amounted to one trillion dollars in this year (Hasham, Joshi, & Mikkelsen, 2019), which prompted private companies to spend approximately 8.2 billion dollars on combating money laundering crimes in 2017.

Fraud crimes (Hasham et al., 2019) resulted in losses on banks and financial institutions approximately 3 Dollars for every dollar fraud organization. Financial institutions (FIs) are the target of three times as many cyber-attacks as any other industry (Johnson, 2016). Mobile banking and ATMs make financial institutions more vulnerable to cyber-attacks. Internal motivations for attacking financial institutions differ greatly among malicious cyber attackers (Surendar et al., 2024). Cybercriminals are increasingly directly attacking bank networks (Udayakumar et al., 2023). Each attack has resulted in financial losses ranging from $2.5 million to $10 million per bank (Johnson, 2016).

Financial institutions must prioritize continued investment in the collection, analysis, and sharing of cyber threat intelligence data. By taking measures to protect their own networks and sharing knowledge with others, they can help mitigate the threat of cyber-attacks on a broader scale. This requires a sustained commitment of time, money, and resources to address the increasing risk of cyber-attacks at an institutional level. According to the Verizon 2017 Data Breach Investigation Report (Acharya & Joshi, 2020), over half of the firms surveyed were affected by the top five cyber threats: denial of service (DoS), phishing, malware, spear phishing, and ransomware. The report also found that more than 88 percent of all security incidents stemmed from three main attack patterns: DoS, web application attacks, and credit card skimming. In India, phishing, identity theft, and malware are the most prevalent crimes in the banking sector, often exacerbated by small errors and a lack of awareness of cybersecurity policies. Public sector banks should allocate more resources to enhancing security, leveraging public-private partnerships, and increasing funding for data protection. By 2020, the global online banking user base was projected to reach 2 billion, doubling from 1 billion in 2017—a milestone achieved two years ahead of schedule in 2018. Between 2015 and 2017, cyber-mediated security breaches targeting financial institutions increased by more than 30%. In Nigeria, the growing popularity of internet banking has made financial institutions increasingly dependent on computer technology.

Breach of cyber security has become one of the most serious hazards to this industry (Wang et al., 2020; Alghazo et al., 2017). According to a cybercrime and security survey report (Wang, Nnaji, & Jung, 2020), injecting malware, phishing, computer theft, and bot attacks are prevalent tactics to cyber-attacks. Tanzania has lost $6 million as a result of multiple cybercrime incidents, forcing the country to build CCUs and CERTs. To protect privacy in the virtual world, new security measures are required. Wang et al., (2020) provides Cyber-attack management solutions, to achieve a cybernetic defensive cycle through four components. Cyber-attacks and risk have become a major source of worry (Bukht et al., 2020). The important discovery was that regardless of whether there is a strong attack, Iraqi private banks retain a certain level of protection. Because of Iraq's insufficient security (Bukht et al., 2020), some respondents are still hesitant to use internet banking services. Terrorism's effects appear to differ (Elnahass et al., 2022) across industrialized and developing countries, depending on the characteristics of the country where the incidence happened. In comparison to countries with greater beginning economic growth rates, countries with low levels of economic growth are projected to be more vulnerable to terrorism. Lack of democracy and the post-Arab spring environment (Bukht et al., 2020) are key factors of domestic and transnational terrorism in the MENA area. Terrorist (Bukht et al., 2020) strikes in the MENA region tend to have more severe economic impacts when they target vital economic sectors. When we compare the amount of money lost in online banking in the UK in 2015 to the amount lost in 2014, there is a significant difference (Paul Thomas & Rajini, 2024) in the amount of money lost.

There are several security issues in banking systems (Elnahass et al., 2022), causing lose a lot of money. Remote banking fraud was the most common sort of financial fraud in 2019 (Paul Thomas & Rajini, 2024), however other types of financial crime include card payment fraud. In the year 2019 (Elnahass et al., 2022), criminals in the United Kingdom stole almost 1.28 billion pounds. Credit card fraud accounts

for nearly half of all financial fraud. Through the Banking Protocol, bank branch personnel collaborated with police to prevent £19 million in fraud in the first half of 2020. The Banking Protocol (Manivannan & Dhatchina, 2020) is a UK-wide program that allows bank branch employees to notify their local police agency if they feel a customer is being defrauded. Police will then go to the branch to investigate the alleged fraud and apprehend any suspects who are still on the premises. Between January and June 2020, the initiative saved £19.3 million in fraud and resulted in over 100 arrests. According to the most recent numbers, the initiative has saved victims £116 million in fraud. The most recent development in phishing is the employment of a Trojan horse malware that infiltrates a user's computer via email and takes the user to a website that looks identical to a financial institution's website. In compared to other similar approaches, phishing generates the most loss to customers/institutions. During the months of October and December 2015, a rogue anti-spam tool (rakin.zip or raking.exe infected with the haxdor.ki Trojan) (Manivannan & Dhatchina, 2020) stole the identities of over 250 clients and $ 1.5 million from Sweden's largest bank.

The financial damages incurred by Russian firms because of "carder" (Manivannan & Dhatchina, 2020) were $20,000,000,000. Carders that specialize in falsifying plastic cards utilize the Internet to obtain information about cardholders and card numbers. Phishing Customers of Citibank receive text messages. "Your personal account has received a wire payment in foreign currency in excess of $ 2'000," the Russian notification states. You must confirm your data in accordance with Citibank On line's agreement to successfully receive money into your account. To verify this activity, launch the account management tool and follow the suggested instructions. Wire transfers will be returned to sender if they are not confirmed." Saytarly Saytar (2014). A 20-year-old school dropout got into an online banking system (Manivannan & Dhatchina, 2020) and stole 50 million won ($A66, 111), raising concerns about the security of the countries commonly utilized internet banking systems. Lee 22 added hacking software (Manivannan & Dhatchina, 2020) to a message he planted on a community internet site, according to investigators. When the woman clicked on it, she unwittingly downloaded the "keystroke" logging tool, which allowed Lee to acquire access to her account's passwords and security code. According to the police, internet users should avoid installing strange programs from the internet and use bank-provided security software.

Cybercriminals target the banking sector every year, stealing billions of dollars from all over the world. The annual economic loss (Action Fraud, 2020) due to cybercriminals has surpassed $ 500 billion. Habib Bank Limited was the target of a cyber-attack perpetrated by Indian hackers in September 2015. In cyber-attacks on banks on October 26, 2018, the data of 19,000 debit cards from 22 Pakistani banks was compromised. On October 27, 2018 (Action Fraud, 2020), Bank Islami announced another cyber-attack, in which the bank lost $ 2.6 million. The Reserve Bank of India issued a cybersecurity guiding principle to banks. For the preparedness of a cyber-attack, 148 financial institutions participated in mock cyber drills. India is regarded as a world leader in several fields. For financial system stakeholders, cyber risk has emerged as a major concern. The use of the internet (Action Fraud, 2020) is rapidly increasing over the world between 2010 and 2016, 1.5 billion new internet users were added. In the last five years, Bangladesh was placed fifth, ahead of India, among the six South Asian countries. In comparison to 2016, (Zahoor et al., 2016) Bangladesh's score has been steadily declining in 2017 and 2018. Intrusions into banking systems that could happen are conveyed Denial of Service is the most well-known attacks that could occur in the financial framework (CDoS). Breach of data, Malware such as Infections, Trojan horses, worms TCP/IP attack that allows the attacker to gain root access to the victim's server, in this case the financial framework, allowing the development of an indirect access section way into the targeted frameworks. The study by (Naseer et al., 2020) investigated cyber security challenges in Nepal's banking sector. The most common threats were phishing, email attacks, and Distributed Denial of Service (DDoS).

Banks need to be more secure against intrusions using public-facing networks, according to data. Cybersecurity concerns put the assets, data, and information of banks, financial institutions, and customers at risk, resulting in a new and evolving digital environment (Oleksandr et al., 2024). As the number of cyber-attacks against the financial industry and institutions rises, it's more important than ever to research and analyze these attacks and devise remedies. In addition, it's important to develop and propose models that mitigate the impact of cybersecurity threats on banks and financial intuitions.

A. Motivation

As the use of technology in the banking sector and financial services institutions is increasing, more threats and attacks are emerging. Therefore, it is necessary to study this topic, analyze the new emerging attacks targeting the banking sector, and search for solutions to mitigate these risks. It is important to know what attacks targeting the banking sector, what methods are used for such attacks, and how to protect the financial services institutions from these threats. Thus, this paper will be discussed more.

Due to the enormous perceived value of this data, banks and financial services institutions are vulnerable to many data breach cybersecurity attacks. One of the problems is also represented in building an effective strategic plan to manage and analyze the risks faced by banks and financial services institutions. Data is one of the most important assets in the banking sector and financial services institutions. Therefore, effective data management contributes protect data, mitigate risks, and facilitate data recovery.

B. Problem Statement

Banks and financial services institutions are exposed to high-risk cyber security threats and attacks, as they include highly sensitive and confidential customer data. Customer data can be sensitive and generic such as names, addresses, national customer number. Customer data can also be sensitive and confidential financial data such as credit card, debit card, bank customer account numbers. Banks and financial services institutions work with a massive amount of confidential and sensitive customer data for business transactions.

C. Research Questions

This project aims to answer the following questions:

- What are the common types of cyberattacks on banking and financial institutions?
- What are the suitable countermeasures for banking and financial institutions?
- What are the main techniques that have been used for mitigating the cybersecurity threats on banking system?
- What are the common proposed frameworks, approaches, and techniques in the previous studies?

D. Expected Outcomes

At the end of the study, the expected results are:

- Highlight the most common cybersecurity attacks in banking and financial institutions systems
- Review and Analyze cybersecurity threats of banks and financial institutions from the literature.
- Recommend a robust security countermeasure for banks and financial institutions that improves security and mitigates cybersecurity threats.
- Assist decision-makers in selecting an appropriate risk management technique for mitigating the severity of cybersecurity threats on banks and financial institutions.

E. Research Methodology

The paper employs a systematic literature review (SLR) technique to conduct a comprehensive examination of previous studies and research on cybersecurity threats on banks and financial institutions. In the first stage, the following search string was used to identify the related paper to this paper subject: (Cybersecurity threats on banks) AND attacks AND (Risks on financial institutions).

The following parameters were used to perform the search in Google scholar and the Saudi Digital Library: Cybersecurity threats on banks and financial institutions in academic journals or conference papers published between January 2016 and May 2022. The following were the exclusion criteria: papers that are not related to security threats on banks and financial institutions and not written in English. During the identification phase, 28,800 papers were found, after eliminating the duplicated papers, there were 2,780 papers remained. In the screening abstract and title, 2,630 papers were eliminated, and leaving 150 for the next phase. After the full-text examination in the eligibility phase, 115 papers were eliminated, and leaving 35 papers for this literature study as shown in fig.1.

Table 1 illustrates the process of selecting the relevant papers and articles based on the inclusion and exclusion criteria.

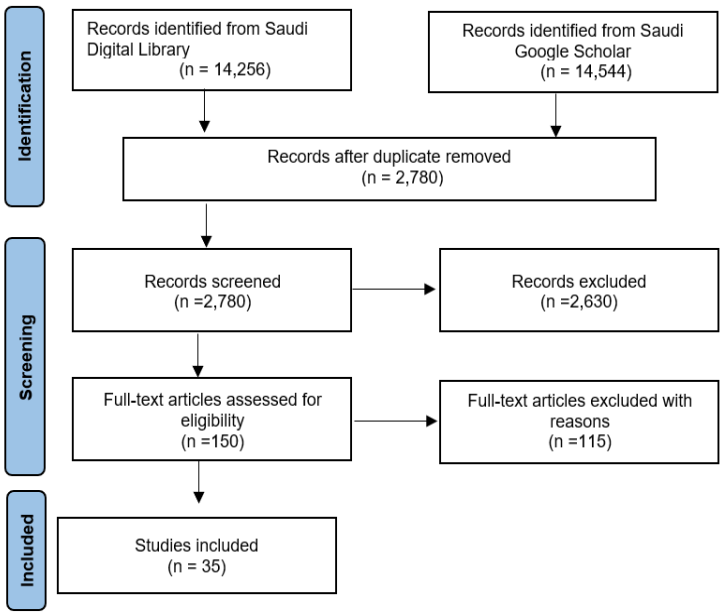

Figure 1: PRISMA Literature Review

Table 1: Inclusion and Exclusion Criteria

Inclusion Criteria	***Exclusion Criteria***
Journals, Conferees papers.	Papers published not in indexed journals.
Published after 2015.	Not written in English.
Presents threats, attacks, challenges of banks and financial institutions security.	

2 Literature Review

Due to the importance of banks sector and financial services institutions and the rapid growth of cybersecurity attacks and direct consequences of these attacks. This section of paper will provide a different number of literature review that has researched the same areain relation to cybersecurity attacks on banks and financial services institutions. In order toanalyze and mitigate the risks of banks and financial services institutions, this section willpresent much research to examine the infrastructure of banks and financial servicesinstitutions, highlight the potential threats in banks and financial services institutions system, research expected attacks on banks and financial services institutions, and highlightthe proposed solutions to mitigate the possibility of attacks on banks and financial services institutions system.

A study by (Tariq, 2018) identified and explored the significant impact of cybersecurity attacks on financial institutions. The study noted that cybersecurity attacks targeting financial institutions are growing rapidly compared to previous years, and this situation is worrying for financial institutions, so the banking sector and financial institutions must pay attention, adopt preventive security measures, and tighten security countermeasures that enhance internal security, assess cyber security, and audit cyber security on an ongoing basis. The study concluded that paying attention and adopting security controls by banks and financial institutions contributes to reducing cybersecurity crime and mitigating risks. In the same way, (Camillo, 2017) introduced various cybersecurity risks facing global banks and financial institutions and discussed the impact of cybersecurity attacks on the banking sector, as it is the most targeted sector among other sectors. In addition to propose a model to increase the security and mitigate the risks on the global banking sector and financial institutions. This paper proposes a model that is used to manage cybersecurity risks through risk transfer, which provides protection against cybersecurity attacks on the global banking sector and financial institutions based primarily on insurance. Another research by (Najaf et al., 2021) presented the impact of technology on financial institutions and its reflection on the sustainability of banks. Also, authors in (Hasham, et al., 2019) demonstrated the economic impact of cybersecurity risks on banks. Previous studies indicated that traditional banks have become more vulnerable to cyber breaches after cooperating with financial technology (fintech) companies. This cooperation with financial technology companies has led to many cybersecurity risks such as data integrity and data leakage of bank customers and malware attacks targeting the systems of banks and financial institutions. Also, cybersecurity attacks directly affect the economy of banks and financial institutions. This paper proposed a theoretical model that combines the advantages of cooperation between traditional banks and digital technology, such as saving operational costs, reducing costs to customers, and providing faster service in addition to the faster response of financial institutions by reporting problems related to cybersecurity attacks. This theoretical model will contribute to a decrease in the rate of cybersecurity attacks on financial banks, which will result in an improvement in the economies of countries and the sustainability of traditional banks. A study by (Johnson, 2016) demonstrated and highlighted the evolution of fraud and financial crime. This study has proven that fraud and financial crimes are evolving and adapting to the areas they target. Cybersecurity attacks over the Internet have become beyond scope and boundaries in order to exploit weaknesses in security controls and carry out fraud crimes. This research paper has proposed three types of models that address financial crime. The first model is called the cooperative model, where it represents most banks and financial institutions, each with its own financial crimes and fraud, while maintaining their own roles, responsibilities, and reports. The second model is called the partially integrated model of cyber security, many banks and financial institutions are working towards this model. The third model is called the unified model, and this is a completely integrated approach to financial crimes, fraud, and cybersecurity,

where all operations are integrated with common assets and systems that are used to manage security risks in banks and financial institutions. The study concludes that unified model is considered one of the best models that contribute to revealing the basic risks facing banks and financial institutions.

According to the Verizon 2017 data breach investigation report, more than half of the firms were reportedly hit by the primary five cyber threats of denial of service (DOS), phishing, malware, spear phishing, and ransom ware. More than 88 percent of all security issues are caused by the top three cyber-attack patterns: denial of service (DOS), online application attacks, and credit card skimming. The study developed a safety mechanism and preventive measures. safety mechanism achieved through securing banks surroundings; banks are now implementing cutting-edge cyber-security solutions. Discovering bulk of vulnerabilities in Indian universities are due to web application vulnerabilities and poor network security and using the SSL protocol to achieve a secure backend internet application against cyber-attacks. Preventative measure in which passwords should be strong, changed at a regular period, and encrypted, multiple layered protection frameworks should be available to secure the system's core, two-factor or multi-factor authentication is a better option when dealing with login issues, firewall settings must be employed, to protect networks, operating system and other software should be patched and upgraded on a regular basis as well as regular data backups, emails from unknown senders should be avoided and reported to the bank's phishing department.

Researchers in a study by (Wang et al., 2020) have presented in this article conclusions of a research project on cyber security in the Nigerian Internet banking business, which includes the biggest cyber security breaches that the industry has faced, as well as its cyber security capacity and practices. The top three most common breaches in Nigerian banks are viruses, worms, and spam emails. From low-tech cyber-enabled crimes to high-tech sophisticated breaches, the sector has evolved. Despite this, it still has a poor adoption rate, with just over 40% of clients using online banking platforms. Cyber security breaches have become a major problem for Nigeria's financial sector (both the banks and their customers). 'Subscribing to account activity alerts' and 'not sharing personal account details with anyone,' according to 80 percent of our participants, are effective preventative measures. The paper shows that cyber security breaches in the Nigerian banking industry might be greatly minimized if appropriate measures are implemented. Bukht et al., (2020) investigated the targeted cyber-attacks on Pakistani banks that occurred or were targeted in 2018, as well as the solutions for preventing these crimes. As a result of the development of ICT and the cyberage, various privacy and security concerns have been recognized and documented. According to a cybercrime and security survey report (Bukht et al., 2020), injecting malware, phishing, computer theft, and bot attacks are prevalent tactics to cyber-attacks. A Tanzanian delegation suggests that Pakistan establish a Cybercrime Unit (CCU) to combat cybercrime. Tanzania has lost $6 million as a result of multiple cybercrime incidents, forcing the country to build CCUs and CERTs. To protect privacy in the virtual world, new security measures are required. The paper (Bukht et al., 2020) provides Cyber-attack management solutions, to achieve a cybernetic defensive cycle through four components. Elnahass et al., (2022) investigated the influence of terrorism on bank stability, as measured by bank risk and financial performance. Terrorism's effects appear to differ across industrialized and developing countries, depending on the characteristics of the country where the incidence happened. In comparison to countries with greater beginning economic growth rates, countries with low levels of economic growth are projected to be more vulnerable to terrorism. Lack of democracy and the post-Arab Spring environment are key factors of domestic and transnational terrorism in the MENA area. Terrorist strikes in the MENA region tend to have more severe economic impacts when they target vital economic sectors. The lack of diversification among resource production sectors, as well as generally weak legal and governance structures, are fundamental elements of many MENA countries' financial infrastructure. Terrorist attacks enhance banks' risk exposure, which leads to

an increase in their profitability. The study (Elnahass et al., 2022) developed a robustness checks model that utilizes the Fragile States Index (FSL) as an IV then use a two-step system to ensure that our findings are reliable. In addition, fixed effect models are used to verify for robustness. (Manivannan & Dhatchina, 2020) examined through the most recent scenario of online banking and cyber- attack. The primary goal of these banking attacks is to gain access to the victim's bank accounts and funds. In some cases, fraudsters exploit banking passwords such as PIN, password, certificates to gain access to banks and steal enormous sums of money. Denial-of-service (DoS), Phishing, Malware, Spam emails, Man-in-the-middle attack, Spamming, and Spyware are seven types of cyber-attacks that target banking apps, according to the report.

The study (Manivannan & Dhatchina, 2020) found that customers need to be more aware of the presence of cybercrime in online banking and the handling of personal financial data, as well as how to defend themselves against these external threats. Criminals are also mastering new cyber-attack technologies. As the world becomes increasingly digital, security measures must be updated on a regular basis. Firewall and two-factor authentication are two types of technologies used to maintain a security system in the banking industry. Customers should also be more aware of the presence of cybercrime in online banking by following best practices, such as using a secure network when using online banking or banking applications. For online banking, you need create a strong password. Change your password on a frequent basis and be sure it's a strong one. Remove personal data from social networking sites, regularly check your account, and do not read emails from unknown senders because they may contain malware (Airehrour et al., 2018). Zahoor et al., (2016) examined the new security and privacy challenges that banks are facing identify countermeasures that could be done to ensure that such attacks do not occur in the future, or how to minimize their impact and, in the long run, improve bank security and privacy. Due to the customers' increased usage of internet banking, the security threat to the banking sector has increased at an alarming rate. The banking industry has been subjected to the many cyber-attacks on their privacy and security, including online payment fraud, ATM machine fraud, electronic card fraud, and net banking transaction fraud. As emerging information security attacks on banks, Phishing, Cross-site scripting, Vishing, Cybersquatting, Bot networks, E-mail-related crimes, Malware, SMS spoofing, Denial of service attacks, Pharming, and Insider risks are all possible. Finally, banks should implement remedies to protect themselves from these threats and provide a secure banking environment for their customers. Banks should strengthen their defenses for preserving client data and implement remedies to make the banking system more resistant to cyberattacks. Continuous risk assessment, in which the company should perform a series of steps to put in place security controls, identify threats, loopholes, and risks, and design and implement security controls that address these risks, is one of the suggested countermeasures that banks should take to mitigate cyber security attacks and enhance the banking security infrastructure. Anti-key logger and Anti-key logging Technology are two approaches that can be used to withstand keylogging attacks as financial institutions have become the target of keyloggers. Techniques that mitigate the phishing attacks without affecting the usual authentication and authorization method (PIN/TAN) and approaches that modify the traditional authentication and authorization method (PIN/TAN) are the two types of countermeasures against phishing. Hardware Tokens, PKI, and Digital Certificates are examples of approaches that augment the usual authentication and authorization technique (PIN/TAN).

A study (Naseer et al., 2020) stated that countermeasures for DOS and DDOS attacks are divided into three groups based on the location of the defense mechanism including source-based, destination-based, and network-based. Source-based methods are deployed near attack sources and effectively prevent network consumers from launching DDOs attacks. Based on a location These strategies are used close to the victim, such as at the destination's access router or edge router. IP Traceback techniques and

packet marking, and filtering procedures are two examples. Most network-based methods are found inside networks and on the routers of autonomous systems. Detecting and filtering rogue routers, as well as route-based packet filtering, are examples of network-based defense techniques. A bank can use the most advanced security measures, but they will be useless if the customer does not understand how to use them. End customers should be informed about new security features and how they may utilize them to secure their accounts on a regular basis by banks through user awareness campaigns. A study by (Naseer et al., 2020) investigated four categories of cyberthreats on financial institutions including cyber warfare, cyber espionage, and cybercrime and cyber terrorism. The study explored how big power is engaged in both cyberwar and cyber diplomacy at the same time. The great powers are unlikely to be able to exert as much control over this area as they have over land, sea, air, and space. States are currently confronting four categories of cyber threats. Cyber warfare and espionage are primarily carried out by nation states, whilst cybercrime and cyber terrorism are attributed to non-state actors. Cybercriminals target the banking sector every year, stealing billions of dollars from all over the world. The annual economic loss due to cybercriminals has surpassed $ 500 billion. Habib Bank Limited was the target of a cyber-attack perpetrated by Indian hackers in September 2015. In cyber- attacks on banks on October 26, 2018, the data of 19,000 debit cards from 22 Pakistani banks was compromised. On October 27, 2018, Bank Islami announced another cyber- attack, in which the bank lost $ 2.6 million. The paper stated that, in order to stop the cyberwar, it promotes regional and global cyber diplomacy. Also, to avoid an unintentional clash, India and Pakistan must establish confidence-building measures (CBMs). In addition, Pakistan and India should cooperate in cyber-diplomacy to build a system for dealing with cyber-attacks by non-state actors. A study by (Sai Manoj, 2021) provided insight into the banks' strategy and tools to cyber risk mitigation. Cloud has been ranked as the No. 1 new technology in which large financial institutions seek to invest for the previous three years. Large respondents ranked data and analytics as the second most important upcoming technology. For financial system stakeholders, cyber risk has emerged as a major concern. The use of the internet is rapidly increasing over the world Between 2010 and 2016, 1.5 billion new internet users were added. The five most serious dangers to a bank's cyber security are unencrypted data, malware, third party services that aren’t secure, data that has been manipulated, spoofing. For comprehensive protection of industrial facilities against internal and external cyber threats, an approach that covers all levels concurrently – from operational to field level, and from access control to copy protection – is required "active defense" approach, organizations must use active defense to anticipate attacks before they occur, detect alerts to contain attacks, and secure important assets in a tiered manner.

Maharjan & Chatterjee, (2019) investigated cyber security challenges in Nepal's banking sector and to provide an innovative approach for reducing cyber risk. ATM attacks are part of the banking sector's threat landscape. Many ATMs are still running on vulnerable Windows XP or Windows 7, which has insufficient security safeguards. POS (Point of Sale) attacks. End-users who visit a retail store, a bank, or an insurance branch are looking for point-of- sale (POS) equipment. Security controls are often not physically present on these POS systems. The most common threats were phishing, email attacks, and Distributed Denial of Service (DDoS). Banks need to be more secure against intrusions using public-facing networks, according to data. The framework proposed will aid in the control or avoidance of significant corporate risk due to delays in mitigation. Explored and proposed a framework that encompasses the strategies used in targeted attacks, vulnerabilities, and countermeasures. Vulnerability assessments are used to find out about a bank's security flaws. Securing the perimeter to protect assets can be a broad, but still effective, IT perimeter security strategy. Network segregation and firewalls are required, with both internal and external firewalls in place to prevent unwanted network access. Limiting open interfaces in which mobile workstations must be shielded in order to avoid catastrophic failures.

Another study conducted by (Hasan & Alramadan, 2021) analyzed and tested the Iraqi banking experience with cyberattacks. Cyber- attacks and risk have become a major source of worry. The important discovery was that regardless of whether there is a strong attack, Iraqi private banks retain a certain level of protection. Because of Iraq's insufficient security, some respondents are still hesitant to use internet banking services. This paper (Udayakumar et al., 2023) developed a multiple regression model to address and test the relationship with study variables, multiple regression was used. Because the research model has very low (R2) values for each variable, the results demonstrate that using it to shape the relationship between the study variables is challenging. The model residuals contain no autocorrelation, indicating that the Durbin - Watson value was only slightly higher than two, and therefore the model could not have been utilized as a guide for the influence of climate change on world temperatures. Korauš et al., 2017) investigated the integral role of information sharing in cyber in cyberattacks mitigation for financial institutions. Cybercriminals are increasingly directly attacking bank networks. Each attack has resulted in financial losses ranging from $2.5 million to $10 million per bank. Financial institutions must continue to invest in the collection, analysis, and exchange of cyber threat intelligence data. The government can better protect itself by sharing cyber threat information to examine facts and trends in a comprehensive cyber threat database. The Financial Services Industry Security Advisory Committee (FS-ISAC) has worked to get security clearances for important financial services sector workers, who have been briefed on emerging security threats and information. The cost of exchanging information is low, and the advantages can be substantial, according to the authors. Summary of Related Work shown in table 2.

Table 2: Summary of Related Work

S/N	Authors	Publication year	Addressed threats	Type of IT	Suggested mitigation techniques
1	Camillo	2017	The threat posed by cybersecurity attacks to global financial institutionsand banks using malware.	User domain Workstation domain	Propose a model to increase the security and mitigate the risks on the global banking sector and financial institutions.
2	Johnson	2016	Series of sophisticatedcybersecurity attacks close to 100 attacks against banking entities around the world. Known as “Car bank”. DDoS attacks.	Server domain	Information Sharing Help detect and mitigatesubsequent DDoS attacks faster.
3	Tariq	2018	Cybercrimes facing financialinstitutions are money theft and identity theft	User domain	Paying attention and adopting security controls bybanks and financial institutions contributes to reducing cybersecurity crime and mitigating risks.
4	Hasham et al.,	2019	Fraud, financial crimes, illegal trafficking, and money laundering crimes that target countries, public and private institutions.	User domain Workstation domain	Cooperative model, partially integrated model and unifiedmodel. The unified model is considered one of the bestmodels that contribute torevealing the basic risks facing banks and financial institutions.
5	Hasham et al.,	2019	cybersecurity risks such asdata integrity and dataleakage of bank customersand malware attacks targeting the systems of banks and financial institutions. Theft of sensitive and valuable dataand phishing on bank employees.	User domain	Theoretical model thatcombines the advantages of cooperation betweentraditional banks and digital technology. Theoreticalmodel will contribute to a decrease in the rate of cybersecurity attacks on financial banks, which willresult in an improvement in the economies of countriesand the sustainability of traditional banks.
6	Bukht et al.,	2020	Injecting malware, phishing,computer theft, and bot attacks are prevalent tactics to cyber-attacks.	User domain workstation domain Lan domain Remote access domain	Cyber-attack managementsolutions, to achieve a cybernetic defensive cycle through four components.
7	Hasan & Al-Ramadan	2021	Iraq's insufficient security, some respondents are still hesitant to use internet banking services.	User domain	Multiple regression model toaddress and test therelationship with study variables, the model could not have been utilized as a guide for the influence of climate change on world temperatures.
8	Johnson	2016	Cybercriminals areincreasingly directlyattacking bank networks. Each attack has resulted in financial losses ranging from $2.5 million to $10 million per bank.	User domain Workstation domain Lan domain	Financial institutions mustcontinue to invest in thecollection, analysis, andexchange of cyber threat intelligence data. The cost ofexchanging information islow, and the advantages can be substantial.
9	Acharya & Joshi	2020	Five cyber threats of denial ofservice (DOS), phishing,malware, spear phishing, andransom ware.	User domain Workstation domain Lan domain	Safety mechanism and preventive measures. Preventative measure inwhich passwords should be strong, changed at a regular period, and encrypted,multiple layered protection frameworks should be available to secure the system's core, two-factor or multi-factor authentication.
10	Wang et al.,	2020	The top three most common breaches in Nigerian banks are viruses, worms, and spam emails.	User domain Workstation domain Lan domain	Cybersecurity breaches in theNigerian banking industrymight be greatly minimized if appropriate measures areimplemented.
11	Korauš et al.,	2017	Safety risks and cyber- attacks related to bank cards.Due to the misuse of banks payment cards results in significant financial losses all around the world.	User domain	Best practices for bank cardsissuers are suggested in this study where issuers must be able to balance a variety of responses, includingeducation, authentication, detection, and the provision of various services.
12	Elnahass, et al.,	2022	Terrorism's effects appear todiffer depending on the characteristics of the countrywhere the incidence happened. Lack ofdemocracy and the post-Arab Spring environment arekey factors of domestic and transnational terrorism in theMENA area.	User domain	Robustness checks model that utilizes the Fragile StatesIndex (FSL) and fixed effect models are used to verify forrobustness.
13	Naseer et al.,	2020	Four categories of cyberthreats on financialinstitutions including cyberwarfare, cyber espionage, cybercrime and cyber terrorism.	User domain Workstation domain Lan domain	In order to stop the cyberwar,it promotes regional and global cyber diplomacy. In addition, build a system for dealing with cyber-attacks by non-state actors.
14	Sai Manoj et al.,	2021	There is a growing gap between banks' expectationsand users' actions when it comes to Internet banking.	User domain	Proposed a model forbridging the gap for internet banking security. The bankshave the primary duty for ensuring a secure Internet banking experience.
15	Airehrour, D. Et al	2018	Social engineering attacks rely on the ability to affect human behavior, they can bevaried and complicated.	User domain	The top three offensivesecurity practices used by banks are fraud detectionsystems, authenticationprocedures, and customer practices.
16	Najaf et al.,	2020	Data integrity risk, data leakage risk, and virus threats.	User domain Workstation domain Lan domain	The study developed a theoretical model has beenbuilt to highlight different types of cybersecurity concerns.

S/N	Authors	Publication year	Addressed threats	Type of IT	Suggested mitigation techniques
17	Sai Manoj et al.,	2021	The five most serious dangers to a bank's cyber security are unencrypteddata, malware, third party services that aren't secure,data that has been manipulated, spoofing.	User domain Workstation domain Lan domain	"Active defense" approach inorder to achieve comprehensive protection ofindustrial facilities againstinternal and external cyberthreats. covers all levels concurrently – fromoperational to field level, and from access control to copy protection.
18	Joveda et al.,	2019	Conveyed Denial of Serviceis the most well-known attacks that could occur inthe financial framework (CDoS). Breach of data, Malware such as Infections, Trojan horses, worms TCP/IP attack.	User domain Workstation domain Lan domain	Proposed a one-of-a-kindcybersecurity solution for detecting money laundering in financial institutions.
19	Maharjan & Chatterjee	2019	POS (Point of Sale) attacks. The most common threatswere phishing, email attacks, and Distributed Denial ofService (DDoS).	User domain Workstation domain Lan domain Server domain	Explored and proposed aframework that encompassesthe strategies used in targetedattacks, vulnerabilities, andcountermeasures. Including network segregation and firewalls and limiting openinterfaces.
20	Chen et al.,	2021	Customers' conversationswith the bank are now conducted online, accordingto this result. The associationbetween PD and bank service quality and workefficiency is positive and significant, implying that increased service quality canmitigate some of the drawbacks of employingFTPs.	User domain	Banks strengthen systemoversight of financial technology for fraud protection and to minimize illicit data sharing as a resultof one FinTech companyserving numerous banks. In addition, banks shouldcreate a distinct department for cloud storage systems.
21	Roy & Viswanathan	2019	Interaction of workforce difficult elements includinga lack of skills, adequate time for skill transformation,a structured compensation mechanism, trainingexposure, job role compliance career planning, competencyconstraints, and bankofficials' support for performance management.	User domain	Conceptual mitigation modelthat depicts the interaction ofworkforce difficult elements as well as an assessment of identified problems and mitigation strategies. Also, implementing a focused and flexible workforceapproach and establishing acustomer-oriented and technologically capable organization.
22	Tosh et al.,	2017	Cyber-insurance is designedto offer coverage for insureds who have suffered losses as a result of cyber- attacks.	User domain Workstation domain	Collaborative approach to sharing cyber-threat information could help firmskeep on top of cyber threats. To maintain the sharing system's long-term viability, rigorous analysis is required to establish the limits and boundaries of maliciousness during information transmission.
23	Williams **et** al**.,**	2019	Compliance information security standard compliance is influenced by detection certainty,normative belief, awareness of information security dangers, and threat perception biases.	User domain	Employees mustcomprehend how serious the dangers are and how they might harm the organization's informationand assets, according to IT managers and security teams.
24	Jibril et al.,	2020	Customer concerns aboutcybersecurity are preventinge-banking uptake and retention. perceivedimpersonation, perceivedaccount hijacked,confidentiality, integrity, and availability, is alsoincluded in this model.	User domain	The conceptual framework would serve as a wake-up call to financial institutions that provide Internet-based products and services to ensure that their customersare authenticated in a trustworthy and secure manner.
25	Bouveret	2018	Data breach, fraud, andbusiness disruptions	User domain Workstation domain Lan domain	Quantitative approach that institutions and regulators may use to analyze cyber riskin the financial sector. according to the type ofcyber-attack (data breach, fraud, and business disruptions).
26	Ng & Kwok	2017	In the context of Fintech, there are strategic riskscontributed to rising.	User domain Workstation domain	A risk-based approachamong the regulated is expected to give an extra layer of protection against any unforeseeablecircumstances that arise as a result of the Fintech movement.
27	Kanishcheva et al.,	2021	Banks are more vulnerable tocybercrime than other businesses.	User domain	Educating clients on fundamental security standards, OTP, two factorauthentication. Audits should be performed regularly.
28	Ojeka & Egbide	2017	Audit committee is deemed ineffective in providingoversight functions on cybersecurity in Nigerian listed companies.	User domain	The audit committee should be fully independent, with half of the members beingindependent directors theremaining half being shareholders who have knowledge and expertise in information technology and cybercrime in addition to financial expertise.
29	Kaur et al.,	2017	Phishing, Pharming, Salami Slicing, Cookies, Hacking, cracking, spoofing.	User domain Workstation domain Lan domain	Enacting strict laws for the protection of consumer rightsin e-Banking is substantial.
30	Uddin et al.,	2020	DDoS attacks	Server domain	Reconfiguring networkinfrastructures reduces the risk of a DDoS attack. Also, cloud-based DDoS mitigation services tosafeguard their networks from cyber threats.

S/N	Authors	Publication year	Addressed threats	Type of IT	Suggested mitigation techniques
31	Belás et al.,	2016	Link between customer happiness and bank security that was unfavorable.	User domain	Commercial banks must constantly develop their applicable technologies andsafeguard themselves against any hacking attacks their business is primarily based on their own reliability. Customers' awareness of security measures and risks is an important component of this reliability.
32	Ololade & Ogbeide	2017	User error, bad internet connections, access challenges, and security issues are some of the other E-banking issues.	User domain Remote Access domain	Security controls, clientauthentication techniques, data protection, audit trail protocols, and consumer privacy standards.
33	Manivannan et al.,	2020	Denial-of-service (DoS) Phishing, Malware, Spam emails, Man-in-the-middle attack, Spamming and Spyware	User domain Workstation domain Lan domain Remote Access domain	Firewall, two-factorauthentication are two types of technologies used tomaintain a security system in the banking industry. Customer best practices, such as using a secure network, strong password, change your password on a frequent basis, remove personal data from socialnetworking.
34	Singh	2017	Phishing attacks	User domain Remote Access domain	Educating clients on how to spot phishing scams, neverclick on an e-mail purportingto be from a bank, antivirus software, read banker's postings for security updateson a regular basis, never use a link to access online banking, multi-factor authentication, passwords will also be replaced with biometric technologies.
35	Zahoor et al.,	2016	Online payment fraud, ATM - machine fraud, electronic card fraud, and net banking transaction fraud. keylogging attacks Phishing, Pharming, cross-site scripting, Vishing, Cybersquatting. Bot networks, E-mail-related crimes, Malware, SMS spoofing, Denial of service attacks.	User domain Workstation domain Lan domain RemoteAccess domain	Continuous risk assessment Countermeasures for the keylogging attacks including Anti-key logger and Anti-key logging Technology. While the techniques that mitigate the phishing attacks including hardware tokens, PKI, and digital certificates. In addition, countermeasures for DOS and DDOS attacks are source-based defense, destination-based defense and network-based defense including detecting and filtering rogue routers, route-based packet filtering. User awareness campaigns.

3 Data Collection

The following sources provided data for this study:

- Journal of Risk Management in Financial Institutions: Oxford University Press publishes the Journal of Risk Management in financial Institutions. It's for everyone involved in risk management at financial institutions. Each quarterly 100-page issue is guided by competent Editors and a prominent Editorial Board and features in-depth articles, reviews, and applied research.
- North Carolina Banking Institute (NC banking Inst): For attorneys, judges, legislators, and academics, the North Carolina Banking Institute is a major banking law resource. It includes both practical and academic articles and features. Students at the University of North Carolina School of Law publish the Institute's publications.

- Journal of Internet Banking and Commerce (JIBC): The Journal's goal is to produce monthly journals that have been peer reviewed by editorial board members from all over the world. It serves as a research platform in the fields of business, marketing, banking, finance, economics, and commerce.
- International Journal of Financial Engineering (IJFE): IJFERM is a scholarly peer-reviewed international publication that covers all elements of financial engineering and risk management theory and practice. The journal focuses on research into the creation and application of novel quantitative models that lead to operational financial decision aids.
- International Journal of Computer Science and Network Security (IJCSNS): The International Publication of Computer Science and Information Security is a monthly journal that publishes articles in all fields of computer science, communication networks, and information security that bring novel theoretical discoveries.
- International Journal of Law, Crime and Justice: The International Journal of Law, Crime, and Justice is accepting submissions on a wide range of criminological research and analysis topics. The journal is particularly interested in cyber-enabled crime, fraud-related crime, terrorism, and hate crime.
- Journal of security and sustainability issues: The Journal of Security and Sustainability Issues publishes original research papers after peer review. It is an international journal published in collaboration with the institutions listed on the journal's cover. It comes out every three months.
- NDU Journal: The NDU Journal is largely concerned with Pakistan's national security problems. The articles are chosen following a thorough examination and blind peer review both at home and abroad. Students, scholars, experts, policymakers, and the intelligentsia all hold the journal in high regard.
- IEEE international conference on engineering technologies and applied sciences (ICETAS): The 7th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS) will serve as a forum for the exchange of innovative ideas and research results. The conference's subject is "Engineering, Technologies, and Applied Science Applications are Driving Our Future."
- International Journal of Advanced Research in Engineering and Technology (IJARET): The International Journal of Advanced Research in Engineering and Technology (IJARET) publishes original research and review articles that are peer-reviewed, open access, interdisciplinary, and completely refereed. The journal's goal is to provide a forum for sharing cutting-edge developments in engineering and technology.
- International Journal of Economics and Finance (IJFE): The International Journal of Economics and Finance (IJEF) is a peer-reviewed international journal that is double-blind. The subjects of economics and finance are covered by the IJEF. The Canadian Center of Science and Education publishes the journal monthly in both print and online forms.
- Research Journal of Science, Technology and Management (LBEF): LBEF wants to be known for excellence in teaching, research, and public engagement, as well as for consistently raising quality and service standards. To aim for excellence in the collecting, creation, and institutionalization of the most recent advances and innovations that have the potential to improve the efficiency and effectiveness of the academy's ability to provide education.

- Empirical Economic Letters (EEL): Papers on all topics of empirical economics and finance are welcome in the journal Empirical Economics Letters (EEL). Papers can be submitted at any time and will be considered for publication in future issues. All articles must include empirical data and theoretical models to support them.
- Springer Journal: Springer Nature is a pioneer in the field of open research and the publisher of some of the world's most influential scientific publications. Springer cover the complete range of academic subjects across our large collection of publications, offering a place for all excellent research and a platform for significant discoveries.
- International Journal of Computing and Digital Systems: IJCDS is an international peer-reviewed journal that publishes six issues per year. Technical papers, as well as review articles and surveys, are published in the IJCDS journal. Artificial Intelligence & Robotics, Image Processing, Computer Vision, Pattern Recognition & Graphics, Data Mining & Big Data are just a few of the topics covered.
- International Conference on Cyber Warfare and Security (ICCWS): Old Dominion University in Norfolk, Virginia will host the 15th International Conference on Cyber Warfare and Security (ICCWS 2020). The ICCWS has become a staple on the academic research calendar. The opportunity for participants to share ideas and meet one another remains the primary goal.
- Journal of Financial Regulation and Compliance: The Journal of Financial Regulation and Compliance is a scholarly and authoritative venue for financial regulation and compliance research from around the world.
- International Scientific and Practical Conference: In 2019, Ukraine will host a symposium on the restoration of architectural monuments under high subsurface water levels and increasing interior humidity. A request for papers has been issued by the International Council for the Protection of Historical Monuments and Museums (ICCROM).
- Research Journal of Finance and Accounting (RJFA): The Research Journal of Finance and Accounting (RJFA) is available in both print and electronic format. RJFA aspires to be a well-known top-tier journal known for refocusing worldwide financial research and studies to define new directions. Asset pricing, investments, risk management, regulation, and insurance are among the topics covered, as are corporate finance, financial intermediation, and financial econometrics.
- International Journal of Computer Applications (IJCA): The Foundation of Computer Science publishes the International Journal of Computer Applications (IJCA) (FCS). Information Systems, Distributed Systems, Graphics and Imaging, Bioinformatics, Natural Language Processing, Software Testing, Human-Computer Interaction, Pattern Recognition, and Signal Processing are just a few of the areas covered in the magazine. Fig. 2 illustrates the sources used in the study.

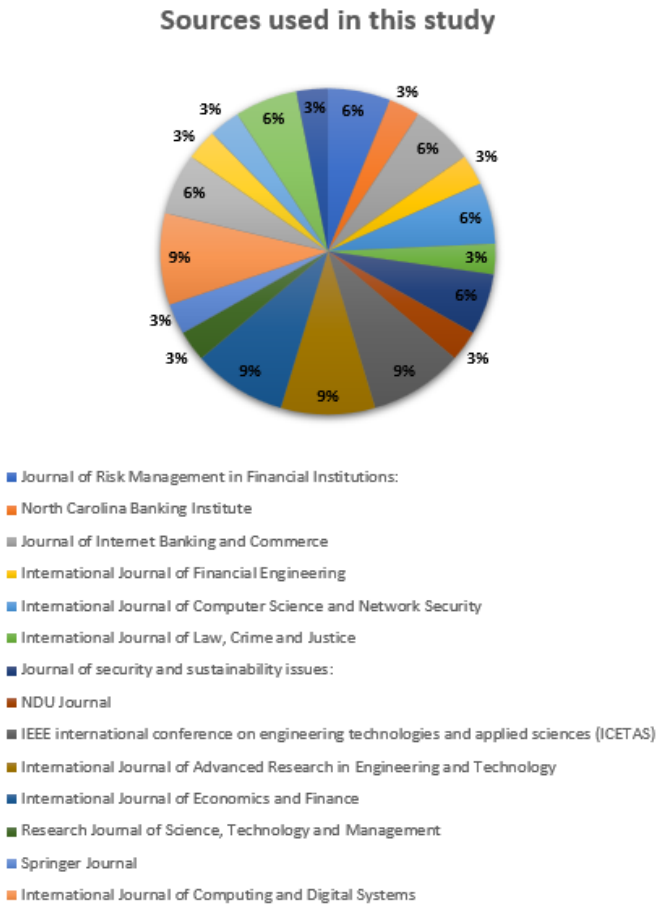

Figure 2: Sources Used in this Study

4 Data Analysis

Various types of cybersecurity attacks have resulted in cyber incidents and data breaches in the banking and financial services institutions sector. "An occurrence that really or potentially jeopardizes the confidentiality, integrity, or availability of an information system or that constitutes a violation or imminent threat of violating security policies, security procedures, or acceptable use policies." according to NIST [NIST Glossary].

Data breaches can have a significant impact on banking and financial services institutions' IT assets, resulting in data loss, financial consequences, and a negative impact on the organization's reputation and value. They can also harm individuals, not just organizations and IT assets, such as customer lives and privacy. Banking and financial institutions are the most targeted and vulnerable sectors when it comes to cyber-attacks and threats. According to studies, there are two key reasons for the banking sector's vulnerability: first, banks sector is a rich supply of valuable data, and second, banking and financial organizations' security defenses are inadequate.

Table 3 depicts cyber incidents by sector and compares cyber-attacks in the last 15 years (2005-2019) to cyber-attacks in the last 5 years (2015-2019) across numerous sectors. The number of breaches has decreased in most sectors over the last five years, except for banking and financial institutions, where the number of breaches has risen by 73.06 %, indicating that banking and financial institutions is the most vulnerable sector among others (Financial Services Risk).

Table 3: Number of Breaches and Percentage of Security Incidents among Different Sectors

Sector	Data Breaches in last 15 years (2005-2019)		Data Breaches in Last 5 Years (2015-2019)	
	Number of breaches	Percentage	Number of breaches	Percentage
BSF	412	50.61	198	73.06
NGO	77	9.46	5	1.84
BSR	325	39.63	68	25.08
Total	814	99.70	271	99.98

Fig. 3 is the graphical representation of Table 3 demonstrating the decreasing number of cyber breaches in each industry, except for the business financial sector, which is increasing.

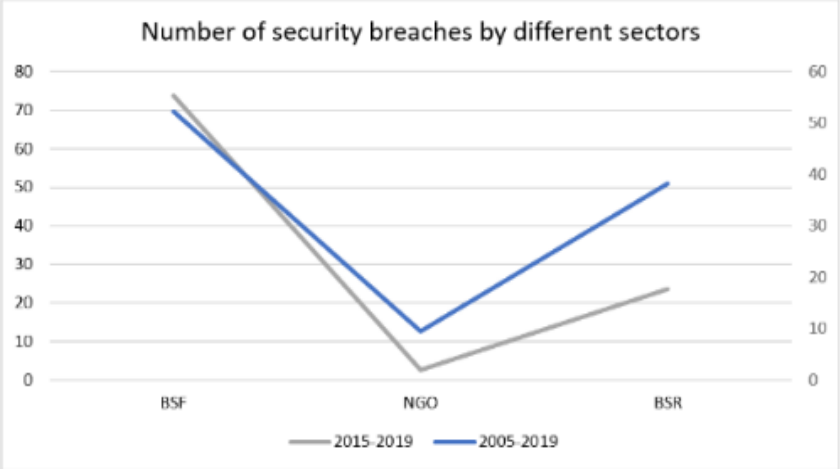

Fig. 3: Number of Breaches and Percentage of Security Incidents among Different Sectors

5 Banking and Financial Institutions Data Breach

The digitalization of the banking and financial institutions sector, including IoT-based financial equipment and the shift from traditional data collecting to Electronic Financial Record (EFR), has increased exploitable vulnerabilities in the systems, exposing the banking sector to high risks. According to reports, cyber-attacks targeting certain industries are on the rise. Cyber-attacks targeting the banking industry increased by more than 80% in 2020. Internal or external data breaches in banking and financial institutions are described as "illegitimate access or disclosure of protected financial information that affects its privacy and security." Any activity or action that breaches any of the security objectives of confidentiality, integrity, availability, or authenticity is termed a cyber breach.

Despite the legislation and the mitigation mechanisms, the number of cyber breaches in the banking sector is increasing. Table 3 shows the number of reported breaches to NBA over the last ten years (2010-2020). The number of exposed records because of these breaches is reflected in Table 4. Despite an increase in the frequency of breaches, the number of exposed records is expected to drop in 2020, according to Table 4. Malware attacks (ransomware, phishing, viruses, and worms), distributed denial of service (DDoS), conveyed denial of service (CDoS), money theft, identity theft, money laundering, data leakage, social engineering attacks, hacking/IT incidents, unauthorized access, data loss or theft, impersonating, and SMS spoofing are all examples of cyber-attacks that target the banking and financial services institutions sector.

Table 4: Number of Reported Data Breaches in Banks and Financial Institutions

Year	Number of Data Breaches	Exposed Records in Millions
2010	195	5.27
2011	215	5.81
2012	221	5.95
2013	277	7.47
2014	310	8.37
2015	265	7.30
2016	322	8.70
2017	350	9.45
2018	368	9.94
2019	510	13.76
2020	664	17.94
Total	3697	99.96

Fig. 4: The Most Common Cyber Threats in Banking Systems

6 Common Data Breach on Banking and Financial Institutions Analysis

This section focuses on analyzing of most common reported data breaches on banks and financial institutions sector regarding to year-by-year, reported incidents, and security statistics reports. According to analysis of statistics and reported incidents, the most common data breaches in banks and financial institutions sector are malware attacks (ransomware, phishing, viruses, and worms), distributed denial of service (DDoS), conveyed denial of service (CDoS), money theft, identity theft, money laundering, data leakage, social engineering attacks, hacking/IT incidents, unauthorized access, data loss or theft, impersonating, and SMS spoofing.

These common attacks are briefly described below:

- Malware attacks: Like Ransomware, phishing, viruses, and worms are all well-known malware examples. Malware attacks on banks and financial organizations are expected to increase by 80% by 2022.
- Distributed denial of service (DDoS)\ Conveyed denial of service (CDoS): This type of cyberattacks considered as computer attack that uses several hosts to overwhelm a financial institution's server, causing the website to fail completely.
- Money theft\ money laundering: This type of cyberattacks considered as illegal practice of making large sums of money obtained through criminal activities appear to have originated from a legitimate source. Money obtained through illicit activity is deemed dirty, so the procedure "launders" it to make it appear as if it came from a trustworthy source.

- Identity theft: This type of cyberattacks involves the theft of another person's personal or financial information in order to commit fraud in their name. Its victims are usually left with credit, financial, and reputational loss.
- Data leakage\ data loss\ data theft: This type of cyberattacks involves unauthorized transmission of data from within an organization to an external destination or recipient is known as data leakage. Data that is exchanged electronically or physically falls under this category.
- Social engineering attacks encompass a variety of malicious activities that exploit human interactions. As defined by cybersecurity expert Bruce Schneier of the US National Institute of Electrical and Electronics (NIEC), these attacks rely on psychological manipulation to trick individuals into making security errors or divulging sensitive information.
- Hacking /IT incidents: The term "security hacking incidents" refers to significant or noteworthy occurrences in the context of security hacking and cracking.
- Unauthorized access occurs when an individual gains entry to a website, software, server, service, or other systems by using someone else's account or employing other methods. This type of cyberattack often involves guessing another person’s password or username until they successfully gain access to an account that does not belong to them.
- Impersonating: This type of cyberattacks Impersonation is the act of pretending to be someone else. Impersonation is when someone spend all day at bank pretending to be other user.
- SMS spoofing: SMS spoofing is a method of altering the sender information on a text message received through the short messaging service (SMS) system. Cell phones, personal digital assistants, and other devices send SMS text messages, which are commonly referred to as text messages. Fig. 4 represents an illustration of the most common addressed threats targeting banks and financial services institutions.

Based on the previous studies, it can be recognized that malware attacks including (ransomware, phishing attempts, viruses, and worms), posed the greatest threat to the banking and financial institutions sector, followed by data leakage\data loss, money theft\identity theft, social engineering attacks, DDoS attacks, unauthorized access, hacking\IT incidents, SMS spoofing, money laundering. It is obvious that impersonating attacks were the least likely threats to banks and financial institutions customers. Fig. 5 demonstrating that malware attacks pose a significant threat to the banking and financial institutions sector, whereas impersonating attacks pose an insignificant threat to the banking and financial institutions sector.

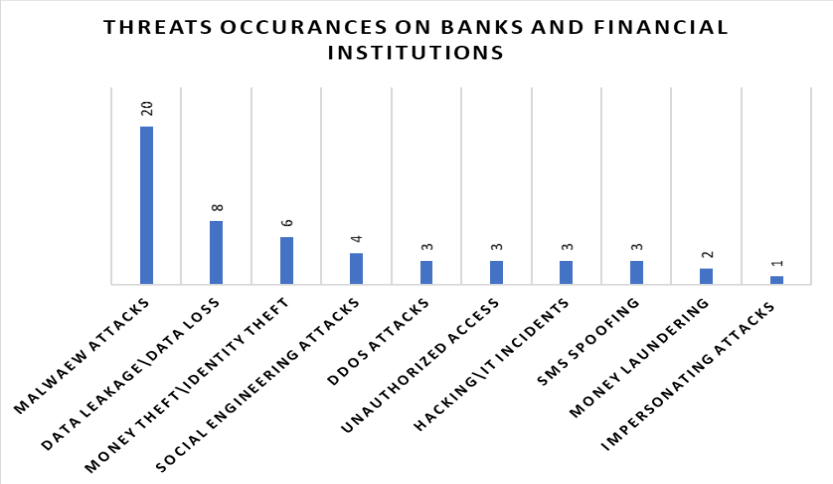

Figure 4: Threats Occurrences on Banks and Financial Intuitions

Based on the previous studies, it can be recognized that the user domain is the most targeted in cyberattacks on banks and financial institutions, then the workstation domain, then the LAN domain, then the remote access domain. It is obvious that server domain is the least targeted in cyberattacks on banks and financial institutions.

Fig. 6 demonstrating that user domain is the most targeted in cyberattacks on banks and financial institutions sector, whereas the server domain appears to be the least targeted in cyberattacks on banks and financial institutions sector.

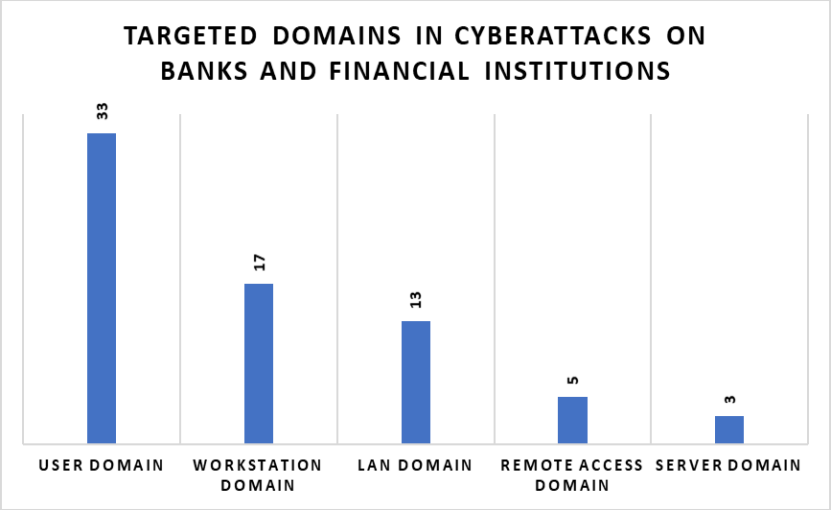

Figure 5: Targeted Domains in Cyberattacks on Banks and Financial Institutions

7 Discussion

The transition from traditional to digital systems, such as electronic financial records (EFR), as well as the banking system's weaknesses, expose the industry to greater risks. The banking sector's security vulnerabilities are growing in tandem with the industry's technological advancements, such as the integration of IoT technology with financial devices, cloud financial applications, and the digitalization of banking information systems and financial databases. To achieve the required security standards, financial device manufacturers and developers should address security early in the development cycle and deliver suitable financial devices that can handle security upgrades. Suggested Mitigation Techniques and Countermeasures for Banks and Fanatical Institutions. The following are some facts on banking and financial institutions security:

- A 28% increase in data breaches at banks and financial services year over year.
- From 2005 to 2019, 45.44% of banks and financial institutions data was compromised, the highest rate in any sectors.
- The most common types of attacks used to breach protected financial data are malware attacks (ransomware, phishing attempts, viruses, and worms), distributed denial of service (DDoS), conveyed denial of service (CDoS), money theft, identity theft, money laundering, data leakage, social engineering attacks, hacking/IT incidents, unauthorized access, data loss or theft, impersonating, and SMS spoofing.
- A 66% of banks data breaches and 88% of breached financial records were due to hacking or IT issues. The main goal of this research is to depict and analyze typical attacks that put banking

and financial services institutions at risk, as well as to offer controls to improve security and provide system policies to improve security of banks and financial services institutions.

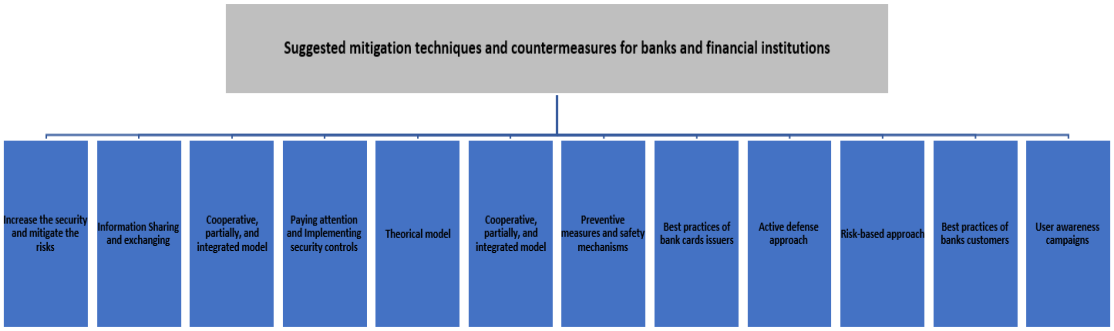

Fig. 6: Suggested Mitigation Techniques and Countermeasures for Banks and Fanatical Institutions

8 Conclusion

This project focuses on bank and financial services institution infrastructure vulnerabilities that are escalating attacks on the sector and affecting the banking system, individuals, and organizations. The security study in these 35 projects demonstrates how cyber intrusions continue to attack the financial sector due to the weakness of security defense and data containment. It turns out that malware attacks are the most common threats to banks and financial institutions. Sharing and exchanging information between banks and financial institutions, as well as best practices taken by bank cards issuers and users are the most effective mitigation techniques. Some previous studies proposed a successful model for mitigating the impact of threats on banks and financial institutions, as well as reducing risks that cannot be mitigated using current mitigation techniques. According to banks and financial services statistics and surveys, existing controls and laws do not provide appropriate security meet the banks and financial services institutions systems' demands and requirements. Future work that considers all new integrated technology in banking and financial services institution systems and devices is urgently needed.

9 Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research,

King Faisal University, Saudi Arabia (Grant No. KFU241635).

References

[1] Acharya, S., & Joshi, S. (2020). Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures. *PalArch's Journal of Archaeology of Egypt/Egyptology, 17*(6), 4656-4670.

[2] Airehrour, D., Vasudevan Nair, N., & Madanian, S. (2018). Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model. *Information, 9*(5), 110. https://doi.org/10.3390/info9050110

[3] Alghazo, J. M., Kazmi, Z., & Latif, G. (2017). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. *In 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, 1-6.

[4] Bank branch staff and police team up to stop £19 million of fraud in first half of 2020, Action Fraud. https://www.actionfraud.police.uk/news/bank-branch-staff-and-police-team-up-to-stop-19-million-of-fraud-in-first-half-of-2020.

[5] Belás, J., Korauš, M., Kombo, F., & Korauš, A. (2016). Electronic banking security and customer satisfaction in commercial banks. *Journal of Security and Sustainability Issues*, *5*(3), 411-422.

[6] Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

[7] Bukht, T. F. N., Raza, M. A., Awan, J. H., & Ahmad, R. (2020). Analyzing cyber- attacks targeted on the Banks of Pakistan and their Solutions. *IJCSNS International Journal of Computer Science and Network Security*, *20*(2), 31-38.

[8] Camillo, M. (2017). Cybersecurity: Risks and management of risks for globalbanks and financial institutions. *Journal of Risk Management in Financial Institutions*, *10*(2), 196-200.

[9] Chen, X., You, X., & Chang, V. (2021). FinTech and commercial banks' performance in China: A leap forward or survival of the fittest?. *Technological Forecasting and Social Change*, *166*, 120645. https://doi.org/10.1016/j.techfore.2021.120645

[10] Elnahass, M., Marie, M., & Elgammal, M. (2022). Terrorist attacks and bank financial stability: evidence from MENA economies. *Review of Quantitative Finance and Accounting*, 1-45.

[11] Financial Services risk: Cyber | AGCS, AGCS Global. https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/financial-services-risk-cyber.html.

[12] Hasan, M. F., & Al-Ramadan, N. S. (2021). Cyber-attacks and cyber security readiness: Iraqi private banks case. *Social Science and Humanities Journal (SSHJ)*, 2312-2323.

[13] Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity*. McKinsey & Company, 1-11.

[14] Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020). Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. *In ICCWS 15th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited*.

[15] Johnson, A. L. (2016). Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation. *NC Banking Inst.*, *20*, 277.

[16] Joveda, N., Khan, M. T., Pathak, A., & Chattogram, B. (2019). Cyber laundering: a threat to banking industries in Bangladesh: in quest of effective legal framework and cyber security of financial information. *International Journal of Economics and Finance*, *11*(10), 54-65.

[17] Kanishcheva, N. A. (2021). Current state of commercial banks in a digital economy. *In International Scientific and Practical Conference "Russia 2020-a new reality: economy and society"(ISPCR 2020)*, 169-172.

[18] Kaur, D. G. (2017). Threats to the rights of consumers in E-banking in India: An overview. *Available at SSRN 2983199*.

[19] Korauš, A., Dobrovič, J., Rajnoha, R., & Brezina, I. (2017). The safety risks related to bank cards and cyber attacks. *Journal of security and sustainability issues*, *6*(4), 563-574. https://doi.org/10.9770/jssi.2017.6.4(3).

[20] Maharjan, R., & Chatterjee, J. M. (2019). Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal. *LBEF Research Journal of Science, Technology and Management*, *1*(1), 82-98.

[21] Manivannan, A., & Moorthy, D. (2020). Cyber attacks in the banking industry. *In Conference Cyber Attacks in the Bank, Bournemouth*.

[22] Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: why cybersecurity risk matters?. *International Journal of Financial Engineering*, *8*(2), 2150019. https://doi.org/10.1142/S2424786321500195

[23] Najaf, K., Schinckus, C., Mostafiz, M. I., & Najaf, R. (2020). Conceptualising cybersecurity risk of fintech firms and banks sustainability. *In The International Conference on Business and Technology, Istanbul, Turkey, 14-15 Nov 2020. Springer Nature*.

[24] Naseer, R., Amin, M., & Shaheen, K. (2020). Cyber Security Challenges in South Asia and Room For Cyber Diplomacy. *NDU Journal*, *34*, 97-114.

[25] Ng, A. W., & Kwok, B. K. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance*, *25*(4), 422-434.

[26] Ojeka, S. A., & Egbide, B. C. (2017). Cyber security in the nigerian banking sector: an appraisal of audit committee effectiveness. *International Review of Management and Marketing, 7*(2), 340-346.

[27] Oleksandr, K., Viktoriya, G., Nataliia, A., Liliya, F., Oleh, O., Maksym, M. (2024). Enhancing Economic Security through Digital Transformation in Investment Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability. *Natural and Engineering Sciences, 9*(1), 26-45.

[28] Ololade, B., & Ogbeide, S. (2017). E- Banking in Nigeria: Issues and Challenges. *Research Journal of Finance and Accounting, 8*(6), 16-24.

[29] Paul Thomas, K., & Rajini, G.. (2024). Evolution of Sustainable Finance and its Opportunities: A Bibliometric Analysis. *Indian Journal of Information Sources and Services*, *14*(2), 126–132. https://doi.org/10.51983/ijiss-2024.14.2.18

[30] Roy, C. N., & Viswanathan, T. (2019). Disruptive technologies and its effect on the workforce in banks: a framework of assessment for mitigation. *The Empirical Economic Letters*, *18*(3), 267-281.

[31] Manoj, K. S. (2021). Banks' holistic approach to cyber security: tools to mitigate cyber risk. *International Journal of Advanced Research in Engineering and Technology, 12*(1), 902-910.

[32] Singh, N. P. (2007). Online frauds in Banks with phishing. *Journal of Internet Banking & Commerce*, *12*(2), 1-27.

[33] Srinadi, N.L.P., Hermawan, D., & Jaya, A.A.N.A. (2023). Advancement of banking and financial services employing artificial intelligence and the internet of things. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(1), 106-117.

[34] Surendar, A., Saravanakumar V., Sindhu, S., & Arvinth, N. (2024). A Bibliometric Study of Publication- Citations in a Range of Journal Articles. *Indian Journal of Information Sources and Services*, *14*(2), 97–103. https://doi.org/10.51983/ijiss-2024.14.2.14

[35] Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce, 23*(2), 1-11.

[36] Tosh, D. K., Shetty, S., Sengupta, S., Kesan, J. P., & Kamhoua, C. A. (2017). Risk management using cyber-threat information sharing and cyber-insurance. *In International conference on game theory for networks*, 154-164.

[37] Udayakumar, R., Chowdary, P. B. K., Devi, T., & Sugumar, R. (2023). Integrated SVM-FFNN for Fraud Detection in Banking Financial Transactions. *Journal of Internet Services and Information Security, 13*(3), 12-25.

[38] Uddin, M., Ali, M., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management, 22*(4), 239-309.

[39] Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice, 62*, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415

[40] Williams, A. S., Maharaj, M. S., & Ojo, A. I. (2019). Employee behavioural factors and information security standard compliance in Nigeria banks. *International Journal of Computing and Digital Systems, 8*(04), 387-396.

[41] Zahoor, Z., Ud-din, M., & Sunami, K. (2016). Challenges in Privacy and Security in Banking Sector and Related Countermeasures. *International Journal of Computer Applications, 144*(3), 24-35.

Authors Biography

Rami Shehab, is a lecturer in the College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia. He got master degree in Computer Information Systems from the College of Information Technology, Jordan. He has published many research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.

Abrar s.alismail, is a master degree in the College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia. He has published many research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.

Dr. Mohammed Amin Almaiah, is an Associate Professor in the Department of Computer Science, University of Jordan, Amman, Jordan. Almaiah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.

Dr. Tayseer Alkhdour, is as an Assistant Professor in the College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia. He got his PhD in computer science and engineering from KFUMP, AL Dhahran, Saudi Arabia. He has a certificate as IDEAL scholar "Program assessment Leader". He worked as a reviewer with national center for academic accreditation and evaluation (NCAAA) and national center for training assessment and accreditation (MASAR), Saudi Arabia. He is working as a consultant for quality and academic accreditation in deanship of development and quality accreditation in KFU.

Dr. Belal Mahmoud AlWadi, is as an Assistant Professor in the Management and Entrepreneurship, Al-Zaytoonah University of Jordan, Amman 11733, Jordan. Vice President at Jordanian Association for Entrepreneurship. He has published many research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. His current research interests include Management and Entrepreneurship.

Dr. Mahmaod Alrawad, is an Associate Professor in the Department of Quantitative Methods, College of Business, King Faisal University, Saudi Arabia. Mahmaod Alrawad is an associate professor of risk management at the College of Business, Al Hussein Bin Talal University, Ma'an, Jordan. He received his master's degree in risk management from Glasgow Caledonian University, Glasgow, UK, and his PhD from the University of Salford, Salford, UK. His research interests include the roles of risk perception and trust in the adoption and acceptance of technology.