International Journal of Core Engineering & Management
Volume-7, Issue-05, 2023 ISSN No: 2348-9510

# CYBER SECURITY CHALLENGES IN FINTECHS AND BANKING

*Reshma Sudra*
*Sudra.Reshma@gmail.com*

*Abstract*

***The quick growth of FinTechs and Banking Institutions, driven by the advancements of technologies, has revolutionized payment services, providing exceptional convenience to the users. However, innovation raises with intrinsic cyber security challenges that demand severe attention. The digital age has accompanied extraordinary convenience and ease of access to financial transactions. The proposed study delves into the ever-evolving and complex landscape of cyber security within FinTechs and banking industries, aiming to recognize the available, viable solutions and challenges. The threats under cyber security in FinTechs and banking sectors encompass data leakages, malware outbreaks, and thefts. FinTechs handle sensitive information and transactions, so they are a prime focus for malicious actors searching for financial gain. The discourse of cyber security issues in banking and FinTechs leads to myriad challenges with long-run consequences. To resolve these problems, the proposed study examines the current risks in FinTech development, the association between cyber security, and the strategies of FinTechs. It overviews the factors affecting potential welfare.***
***Moreover, it evaluates the factors that induce the emergence of Cyber security and FinTechs. Various existing studies and situations provide suitable insights into the cyber security consequences in this sector. Importantly, the proposed research aims to contribute to a comprehensive understanding of cyber security challenges faced through the banking sector and FinTechs and provide recommendations for FinTech companies, cyber security professionals, and regulators to enhance security measures. Additionally, the present study recommends an effective management system in scrutinizing the impact of FinTech variables on cyber security.***

***Keywords: Cyber security, Financial Technologies, Challenges, Banking and Malware Outbreaks***

## I. INTRODUCTION

### 1.1 BACKGROUND OF THE STUDY

In the present world, an individual can send and receive any kind of information like an email, video, or only by a button click. However, he or she ponders about how safe this information is transferred from one person to another person strongly with no leakage of data. The appropriate response was relayed on cyber security (Kalakuntla, Vanamala, Kolipyaka, & Administration, 2019). Concomitantly, security incidents constantly extend and become an increasingly sophisticated and complicated one. In the last decades, the vast adoption of information technologies has changed. Moreover, cyber security can be defined as a computer-related discipline that involves technology, information, processes, and people with the target of attaining secured operations against unauthenticated attacks or access (Kovačević, Putnik, & Tošković, 2020).
Similarly, when the architecture of the system gets changed from huge patented machines with fewer associations to "far and small open systems that are coupled with an increase of networking," it is still running on the same protocols. The cyber perception created through cyberspace is perpetuating insecurity along with catastrophic consequences. It is shaped by

International Journal of Core Engineering & Management
Volume-7, Issue-05, 2023 ISSN No: 2348-9510

various key events associated with the technical sphere. Mostly, cyber incidents refer to the disruption that issues arise in digital technologies' normal operations (Dunn Cavelty & Wenger, 2020).

Globally, the banking sector has witnessed several potential disruptions in FinTechs and digital technology evolution in recent years (Ebrahim, Kumaraswamy, & Abdulla, 2021). These changes have happened due to host factors such as Globalization, digitalization, and technological advancements that benefited companies, potential stakeholders, and countries, invigorating a hacker's rising community to quickly take advantage of the same development in the technological world. FinTechs refers to a mixture of Financial and technology which represents the use of automation of financial processes and services or the use of technology. The English term financial technology refers to the vast and fast-growing industry that serves businesses and consumers (Scheau, Rangu, Popescu, & Leu, 2022).

The financial institutions took an important shift (for example, FinTechs sandbox) in recent decades because of technological innovation. In several cases, innovations can run forward on security developments (Najaf, Mostafiz, & Najaf, 2021). There have been crucial changes in payment systems caused by FinTech developments and the rising use of mobile and digital technologies. However, cybercrime is progressing simultaneously (Tkachenko et al., 2019). Moreover, Financial exploitation is a significant concern among elderly people, and it severely impacts the growing segment of the populace in industrialized nations (Nguyen & Han, 2022). The figure. 1 signifies the cyber security paradigms.

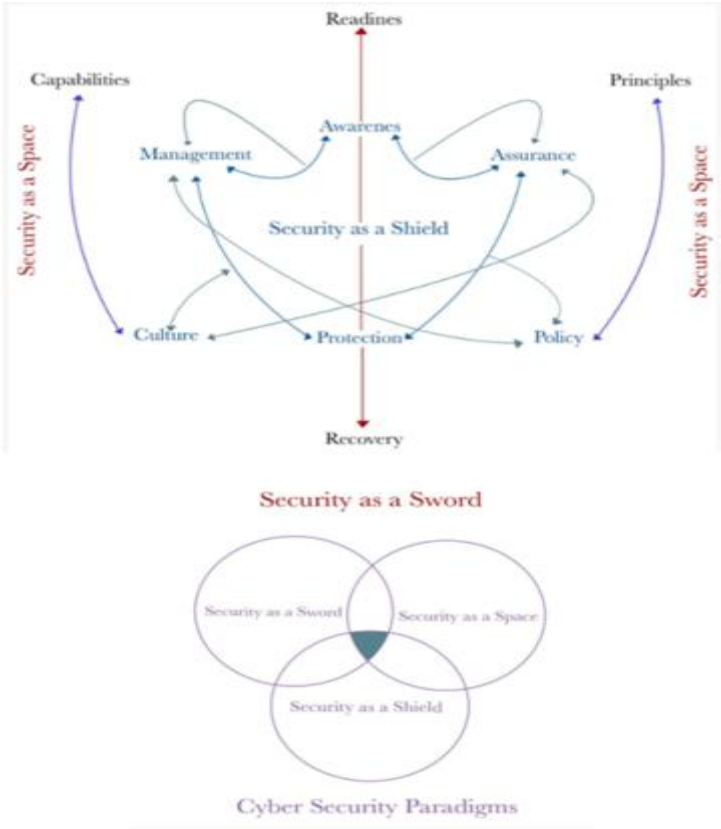


**Figure. 1 Cyber Security Paradigms**

International Journal of Core Engineering & Management
Volume-7, Issue-05, 2023 ISSN No: 2348-9510

The figure. One illustrates those cyber security paradigms to know how cyber security resilience and digitalization capabilities are associated. Security as space comprises two interconnected elements called policies, which refer to security principles and capabilities encompassing human resources, technology, and processes. Security is a sword that involves two stages: readiness, which emphasizes the plan and infrastructure ready to face the cyber-attacks, and recovery, which focuses on the ability to recover rapidly after an attack and restore normal functions.

Consequently, constant cyber-attacks can result in theft of sensitive and valuable information, ransomware, phishing for banks, insider threats, and hacking. It generates questions and dilemmas on partnerships between FinTech companies and traditional banks. The influence of cyber security risks on FinTechs is economically important for traditional banks' sustainability. Simultaneously, there are particular concerns with innovations in information technology and systematic operations.

Moreover, banks depend on third-party systems to provide some digital services. Cyber-attacks and threats are considered to be challenging because of quick development in technologies. Hence, banks must consider cyber-attacks to protect their customers and clients (Al-Alawi & Al-Bassam, 2020). To resolve these challenges in banking and FinTechs, the proposed study proposes a theoretical model that evaluates the factors and recommends an effective management system. It enhances the cyber security among FinTechs and banking sectors predominantly. Furthermore, the proposed study overviews various risks in developing FinTechs and cyber security. It determines the association between cyber security and FinTechs.

**1.2 Significance of study**

As technology grows quickly, Cyber security is considered paramount in the present digital age. It covers the technologies, processes, and practices designed to guard computer networks and data from cyber threats and systems like phishing, hacking, ransomware, and malware attacks. The importance lies in maintaining the system integrations, protecting organizations and individuals from reputational damage and financial losses, and protecting sensitive information. As cyber-attack threats continue to evolve and become more sophisticated, capitalizing on robust security measures is necessary for businesses, organizations, and individuals to mitigate the risks and protect their digital assets. The priority consideration of cyber security is that companies can create trust among stakeholders, uphold the integrity and confidentiality of data in an emerging interconnecting world, and comply with regular requirements.

Cyber security is playing a vital role in banking institutions and FinTechs operations. These sectors strongly rely on digital platforms to assess financial transactions and accumulate sensitive client information. The prime focus for reducing cyber-attacks through robust cybersecurity measures. It is necessary to protect against financial fraud, reputational damage, and data breaches. Through investing in advanced cybersecurity technologies, implementing protocols, and fostering a cybersecurity awareness culture, banks and FinTechs can build trust and mitigate risks with customers. Prioritizing security not only protects the financial system's integrity but also upholds the trust and confidentiality of the financial firms.

**1.3 Problem statement**

The discourse of cyber security issues in banking and FinTechs leads to myriad challenges with long-run consequences. It revolves around the rising sophistication and cyber-attack frequency focusing on financial institutions. The industries become rewarding targets for the cruel actors seeking to abuse susceptibilities for financial gain. The evolving nature of cyber threats, comprised of phishing attacks, data breaches, and ransomware, poses crucial risks to the security and integrity of financial systems. Furthermore, the quick pace of technical advancements in banking and FinTechs further complexes the task of protecting against cyber-attacks.

Lack of awareness and Insufficient cyber security measures among the customers and employees, and the difficulty of regulatory needs exacerbated the susceptibilities of banking and FinTech companies to cyber-attacks. The latent consequences of strong cyber-attacks comprised reputational damage, financial losses, compromised reliability, and comprehensive strategies in the sectors. Addressing these issues, the proposed study attempts to provide the importance of cyber security challenges in both sectors to enhance the transactions and trust relied on by institutions and companies. Finally, it leads to the prevention of security and offers a safe environment for the customers and stakeholders.

1.4 Research question

International Journal of Core Engineering & Management
Volume-7, Issue-05, 2023 ISSN No: 2348-9510

The research questions of the present study are as follows:

- What is the risk in Fin-tech development of commercial banks?
- Illustrate the effective management system for cyber security.
- What is the association between cyber security and FinTechs?
- What are the factors inducing the rise of FinTechs and cyber security?

**1.5 Objectives of study**

1. To overview the risk in Fin-tech development of the commercial banks
2. To determine the association between the strategic approach of Fin-tech and cyber security
3. To evaluate the factors that induces the emergence of Cyber security and FinTechs
4. To recommend an effective management system in scrutinizing the impact of FinTechs variables on cyber security.

**1.6 Paper Organization**

The paper is organized in the following progressive manner. Section 1 illustrates a brief introduction regarding the cyber security challenges in FinTechs and banking institutions. It also depicts the significance of research. Section 2 describes the prevailing scholarly research works related to the proposed research. Section 3 provides a detailed analysis of cyber threats, risks, and factors and their mitigation strategies. Section 4 illustrates the discussion as well as the limitations of the study. Lastly, section 5 discusses the conclusion and future recommendations of the proposed study.

## II. LITERATURE REVIEW

This section provides various existing research to review the cyber security challenges in different regional sectors.

The existing study (Kaiwartya et al., 2017) has examined the biometrics system key features in prevailing and Islamic banking to encompass the difficulty of cyber security and offer high security and safety to the banking institutions. The results have revealed that future cyber security depends on biometrics, which has encompassed online banking, computer login, access control, and e-banking. Correspondingly, the prevailing study (Akintoye, Ogunode, Ajayi, Joshua, & Finance, 2022) has empirically investigated the impact of cyber security under the driving financial innovations of Money bank deposits in Nigeria. It has adopted a survey research and questionnaire method, and the results have shown the effectiveness in disaster recovery plans and identifying the vulnerabilities and cyber threats that are positively affected by the drive of financial innovation in money banks.

Similarly, the existing study (Stanikzai & Shah, 2021) has evaluated the effectiveness of cyber security techniques in mitigating or reducing crime and achieving potential business improvements. The findings have shown that fraud has accounted for occurrences (43%) in the ORX news dataset, disruptions (23%), and data breaches (34%). The prevailing study (Jayalath & Premaratne, 2021) has focused on examining the key areas relevant to digital infrastructure management, cyber security for FinTechs, and customer convenience. Furthermore, it has focused on customer's confidential data and privacy compliance with the industry regulations and frameworks. The findings have shown that financial platforms have become more critical. Thus, FinTech companies must consider executing reliable infrastructure when opened to the public.

The prevailing study (Ghelani, Hua, & Koduru, 2022) has examined effective mechanisms for cyber security protections in banking systems at logical and physical levels and limiting access. In addition, establishes rules for interaction, requirements, constant criteria, and suitable user authority. The findings have provided the most crucial architecture with a high possibility for easy access and the safest to protect the data from different threats. In the same way, the traditional study (Creado & Ramteke, 2020) has explored different active cyber defense methods that have been implemented through companies in the financial sector to protect and secure their cyberspace and assets. It has adopted an active cyber defense strategy and has found that active and passive defense methods are effective in threats, which has to be adopted by banks to secure cyberspace. Correspondingly, the conventional study (Varma, Nijjer, Sood, Grima, & Rupeika-Apoga, 2022) has examined how FinTechs are influenced by changes in banking and challenges, along with a specific emphasis on blockchain technology. It has performed a thematic analysis of FinTech banking industry. The prevailing study has found that FinTechs have the enormous potential to

International Journal of Core Engineering & Management
Volume-7, Issue-05, 2023 ISSN No: 2348-9510

grow and influence banking institutions. In addition, it has revealed that blockchain applications' potential is not limited to FinTechs and payment transactions. However, there has been growing interest in the blockchain technology. In parallel, the traditional study (Calliess & Baumgarten, 2020) has introduced the cyber security legal aspects and set out the key elements in the financial sector to make the European Union FinTechs sectors more cyber secure.

Similarly, the conventional study (Suseendran, Chandrasekaran, Akila, & Sasi Kumar, 2020) has analyzed the overall operations of financial technologies, challenges of FinTechs and Banking industries, and cybersecurity when associating IoT with the internet. Additionally, the usage of IoT on FinTechs in the digital environment has been mentioned precisely. Contrarily, the prevailing study (Al-Alawi & Al-Bassam, 2020) has demonstrated the advantages of applying cybersecurity and its significant effects on banking institutions. It has used an online questionnaire method to identify the risk types in Bahrain. The existing study has found that banks have been tackling cyber-attacks frequently, where 26% of financial industries have encountered online theft cases, and 23% have experienced damage to computer systems. The remaining 11% have faced hacking attempts.

Concomitantly, the conventional study (Demirkan, Demirkan, & McKee, 2020) has looked into the present and blockchain uses in business, particularly in cybersecurity and accounting. The prevailing study has suggested that blockchain technology has uses not only in accounting but also in offering trust, security, and transparency in the financial world. Correspondingly, the traditional study(Yang, Li, Zhang, Gu, & Applications, 2019) has analyzed the current strategies of cyber security and evolving technologies like biometric authentication, AI-driven anomaly detection, and advanced encryption. It has assessed the compliance needs impacts of FinTech companies and their capability to secure user data. It has been found that strengthening cyber security is a major thing for sustainability, fostering constant innovation, and protecting the future of mobile FinTechs. In parallel, the prevailing study (Saleem & Research, 2021) has identified the risks of financial technology use in offering financial services. It has examined the association between FinTech revolution and adoption and has utilized the questionnaire method in Pakistan. The findings have shown that the relationship among them has been negatively impacted by risks.

### 2.1 Research Gap

- The existing study (Ghelani et al., 2022) proposes an effective mechanism for protecting cyber security. However, it lacks a realistic evaluation of security management.
- The conventional study (Varma et al., 2022) has investigated how FinTechs are influenced by changes in banking and challenges. However, it lacks an analysis of how evolving technologies are associated with particular socioeconomic outcomes.

## III. CYBER SECURITY CHALLENGES

This section deliberates on the cyber security challenges in banking and FinTechs that encompass with risks, factors, data leakages, and outbreaks of malwares.

### 3.1 Risk of Cyber security in FinTech firms

FinTech's cyber security risks have huge economic implications for the traditional bank's sustainability. The risks are data integrity risks, malware attacks, and data leakage risks. The conventional underpinning of long-run economic improvement is dependent on financial institutions to take minimal cyber-risk in search of potentially profitable opportunities. Furthermore, the cyber security risk on FinTechs is considered the latest conventional research problem that entailed deep analysis to identify various dynamics or rising cyber security issues. The collaboration of FinTechs and banks is increased to decrease the bureaucracy and offer fine-tuned service to the clients. Such collaboration increased the cybersecurity risks for firms and traditional banks (Najaf, Schinckus, Mostafiz, & Najaf, 2020). Figure. 2 shows the main cyber security threats in FinTechs.

International Journal of Core Engineering & Management
Volume-7, Issue-05, 2023 ISSN No: 2348-9510

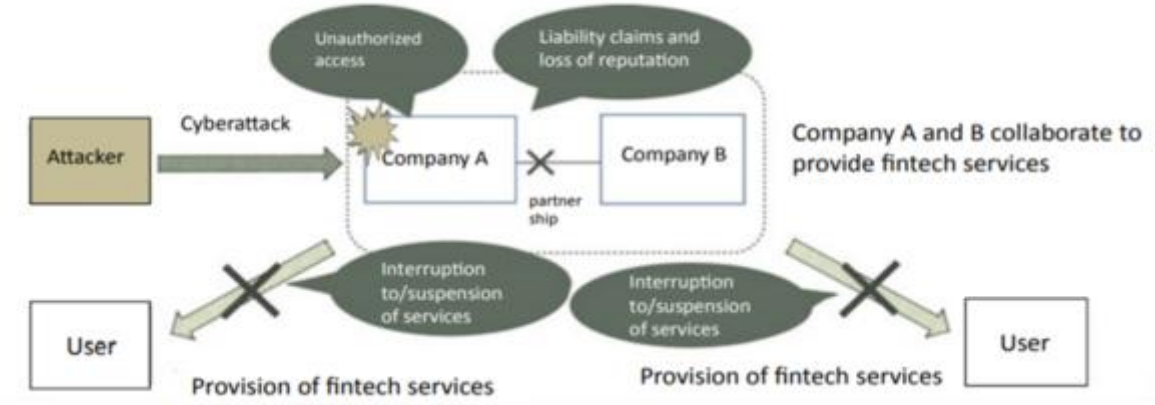


Figure. 2 Cyber Security Threat in FinTechs(Kaji, Nakatsuma, & Fukuhara, 2021)

The figure.2 deliberates the cyber security threats in FinTechs. It encompasses unauthorized access, interruption or suspension of services, loss of reputation, and liability claims. When the attacker attacks the collaborated companies, it cuts the partnership and interrupts the services to the users on both sides.

Generally, Cyber security risk is the probability of exposure from a data breach through cyber criminals or malicious insiders. From an industrial perspective, the cyber security risk is potential harm or loss caused by cyber-attacks related to a firm's critical structure. The risks and threats of cyber security to the industry are recognized. FinTech firms face the most predominant cyber threats, and this section explains the paramount cyber risks to FinTech companies. They are explained below.

**Malware:** Malware is malicious software designed to damage, disrupt, or acquire unauthorized access to the systems to steal sensitive data. It can be categorized into Ransomware, scareware, riskware, Trojan horse, zero-day, Worm, virus, spyware, and adware. These can perform vast operations like deleting, monitoring, encrypting files, stealing, and altering the registry files.

**Ransomware:** Ransomware is malware that encrypts the directories and files on the machine to make them inaccessible to the users.

**Trojan:** Trojans are known as sneaky impersonators, behaving like legitimate functions. It hides in the background and steals data from the device, a huge malware category encompassing Trojan-dropper, Trojan-spy, Trojan-banker, and Trojan-SMS.

**Denial of Service:** Denial of Service (DoS) refers to a targeted attack against a computer, network, or server to make services unavailable to the clients.

**Distributed Denial of Service:** Distributed Denial of Service (DDoS) is a targeted and lethal attack encompassing multiple compromised and attacked systems. These attacks impacted the major economies of the world. It leverages the server/client architecture to some computers to focus on particular computers with requests. So it cannot render the services to clients (Kaur, Lashkari, & Lashkari, 2021). The figure. 2 signifies the various types of cybercrime in banking sectors.

International Journal of Core Engineering & Management
Volume-7, Issue-05, 2023 ISSN No: 2348-9510

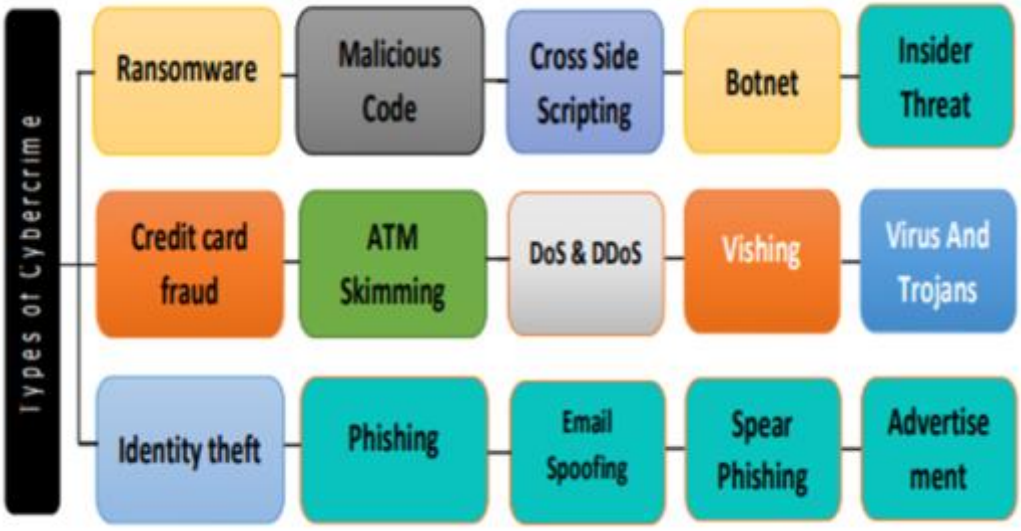


Figure 2 Types of Cyber Crime in the Banking Sector(Stanikzai & Shah, 2021)

From Figure 2, the types of cybercrime in banking institutions are deliberated. They are listed with ransomware, malicious code, cross-side scripting, botnet, vishing, ATM skimming, insider threat, DoS and DDOS, credit card fraud, identity theft, phishing, email spoofing, spear phishing, advertisement, virus, and Trojans.

Additionally, the main types of cyber security risks are tackled by financial institutions and FinTech companies as a result of cyber-attacks. The risks are loss of reputation, unauthorized access by theft, suspension or interruption of services, and liability claims. The chief reason for gaining unauthorized access to computers is to steal money or data. Thus, industries fall prey to unauthorized access, likely to suffer from information leaks or illegal money transfers. The attacks pose a risk of interruption of services, which is attained through DDOS attacks. It overwhelms the network bandwidth and makes the systems shut down through infected servers or systems with ransomware. These can lead to loss of customers, damage to reputation, and liability claims, resulting in a fall in share rates (Kaji et al., 2021).

Similarly, FinTechs are changing to the provision of traditional financial services. Risk management involves coordinated practices to control and direct an industry with regard to cyber risks. The significance of risk management in banking sectors is that AI/ ML has some potential to help risk mitigation measures, allowing banks to adopt adequate implementation and strategies. Furthermore, cyber risks include operational risks to technology and information assets, which can affect the availability, integrity of information, confidentiality, or information systems. Henceforth, it is significant to offer a safer cyberspace and to ensure cyber security (Vučinić, Luburić, & Practice, 2022).

**3.2 Data Leakages and Malware Outbreaks**

Data is known as information that can be transmitted, processed, or stored for reference and analysis. It can be presented as a combination of insight, wisdom, intelligence, and knowledge. The data breach consequences negatively impact the sustainability and reputation of the organizations or businesses. The data storage can comprise hard drives, cloud storage, network storage, flash drives, and magnetic tapes. Data leakage poses crucial risks. In a data breach event, client's confidential data like credit card numbers, personal identification, and bank account details can be exposed, leading to financial fraud and identity theft. Furthermore, regulatory bodies imposed strict data protection essentials on FinTech institutions, and non-compliance results in legal and hefty fines (Zhang et al., 2022).

Similarly, Cyber criminals are frequently select the financial sector as their prime target to steal money. For FinTech organizations, a data leak or data breach can be most disastrous due to its increased regulatory essentials brought on through cyber-attacks. The entire sector can be in peril.

International Journal of Core Engineering & Management
Volume-7, Issue-05, 2023 ISSN No: 2348-9510

Hence, every business-critical application needs to develop proactively and protect the FinTech security strategy approach. To mitigate the cyber security risks associated with data leakages, banking and FinTech sectors must invest in robust security measures such as access controls, employee training, regular security audits, and encryption. Proactive observation is necessary to promptly address and detect data breaches, improve the organization's reputation, and reduce client impacts. Ultimately, protecting privacy and integrity is paramount in maintaining credibility and trust in baking and financial institutions(Kryparos, 2018).

Malware outbreaks in FinTechs pose a significant threat to the stability and security of financial companies. The malicious software programs may steal sensitive information, disrupt operations, compromise client data, and infiltrate systems, leading to reputational damage and financial losses. The cyber criminals develop methods to exploit the susceptibilities and bypass the security measures. The most common malware types affecting FinTechs include phishing attacks, customer accounts, banking Trojans, ransomware, and targeting payment transactions and personal information. To overcome malware attacks, sectors must implement robust security measures like network monitoring, employee training, endpoint protection, and regular software updates (Zhang et al., 2022).

### 3.3 Factors affecting potential welfare and impediments of FinTech firms

Several factors include potential welfare and impediments of financial institutions. Such as market competition, technological innovation, cyber security risk, access to funding, customer adoption and trust economic conditions, and regulatory environment (Nwogugu, 2019). The specific segment of FinTech service providers united with big tech companies regarding potential contribution to social welfare. It poses heightened contestability and competition to prevailing financial sectors, however, also through information sharing and innovation among companies within the ecosystems (Cho & DP21-03, 2020). In addition, the five main factors that caused impediments to the FinTech firms, namely regulation factors, cost factors, partnership factors, technology factors, and unbanked market factors.

- **Cost factors:** Cost factors consist of acquisition costs, transaction fee costs, and distribution costs.
- **Technology factors:** Technology factors are embedded in payment services operation and offer interoperable services to unbanked essentials to be fast and convenient.
- **Regulation factor:** This factor is comprised of technology and infrastructure that are required to offer financial services to the unbanked market. These factors permeate to clear and settle the transactions by sponsoring the bank.
- **Partnership factor:** Partnership is considered a variable to factors constraining the FinTech in offering services to the market.
- **Unbanked Market Factors:** To customize the services of the unbanked to notice the market's needs is crucial. It is required to offer simplicity in understanding the boarding customer process by trusted sources like community members (Felet, 2019).

## IV. DISCUSSION

The proposed study focuses on cyber security challenges in the FinTech and banking sectors to know the difficulties of both customers and professionals. The financial threats and challenges of banking institutions in digital transactions are analyzed. This section elaborates on the challenges of cyber security in financial institutions.

The conventional study (Ghelani et al., 2022) examines the effective mechanisms for cyber security protections in banking systems at logical and physical levels and limiting access. In addition, establishes rules for interaction, requirements, constant criteria, and suitable user authority. Likewise, the prevailing study (Jayalath & Premaratne, 2021) shows financial platforms have become more critical. Thus, FinTech companies must consider executing reliable infrastructure when opened to the public. The influence of cyber security risks on FinTechs is economically important for traditional banks' sustainability.

Furthermore, the cyber security risk on FinTechs is considered the latest conventional research problem that entailed deep analysis to identify various dynamics or rising cyber security issues. The collaboration of FinTechs and banks is increased to decrease the bureaucracy and offer fine-tuned service to the clients. The prevailing study (Saleem & Research, 2021) identifies the risks of

financial technology use in offering financial services. The latent consequences of strong cyber-attacks comprised reputational damage, financial losses, compromised reliability, and comprehensive strategies in the sectors.

Congruently, the conventional study (Cho & DP21-03, 2020) assesses financial sectors' welfare and industrial implications by focusing on four sub-sectors: alternative payment systems, online capital raising platforms, alternative regulatory compliance, and robot and AI-based investment consultancy. Furthermore, effective mechanisms such as risk management and incident response management are crucial. Risk management involves coordinated practices to control and direct an industry with regard to cyber risks. Furthermore, in the prevailing study (Vučinić et al., 2022), cyber risks include operational risks to technology and information assets, affecting information availability, integrity, confidentiality, or information systems.

## V. CONCLUSION

The banking sector has witnessed several potential disruptions in FinTechs and digital technology evolution in the past years. Cyber security plays a vital role in banking institutions and FinTech operations. These sectors strongly rely on digital platforms to assess financial transactions and accumulate sensitive client information. The threats under cyber security in FinTechs and banking sectors encompass data leakages, malware outbreaks, and thefts. The challenges faced by banking and FinTech are evolving, multifaceted, and requiring potential vigilance. It requires proactive measures to protect sensitive data and maintain reliability with clients. The proposed study examines the risks, factors, and various attacks to improve understanding of cyber security threats. The increasing digitization of fiscal services has expanded the attack surface for cybercriminals, leading to a rise in sophisticated threats like malware, phishing attacks, and ransomware incidents. The present study analyzed effective cyber security strategies that comprise access control, a holistic approach, employee training programs, robust encryption protocols, and regular security audits. Collectively, collaboration between threat intelligence, data-sharing forums, and stakeholders is important in combating the threats from cyber-attacks. The present recommends the risk management system and incident response system to scrutinize the impact of FinTechs variables on cyber security.

International Journal of Core Engineering & Management
Volume-7, Issue-05, 2023 ISSN No: 2348-9510

**REFERENCES**

1. Akintoye, R., Ogunode, O., Ajayi, M., Joshua, A. A. J. u. J. o. A., & Finance. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. 10(3), 643-652.
2. Al-Alawi, A. I., & Al-Bassam, M. S. A. J. J. o. X. U. (2020). The significance of cybersecurity system inhelping managing risk in banking and financial sector. 14(7), 1523-1536.
3. Calliess, C., & Baumgarten, A. J. G. L. J. (2020). Cybersecurity in the EU the example of the financial sector: a legal perspective. 21(6), 1149-1179.
4. Cho, M. J. K. S. o. P. P., & DP21-03, M. P. N. (2020). FinTech Megatrends: An Assessment of Their Industrial and Welfare Implications.
5. Creado, Y., & Ramteke, V. J. J. o. F. C. (2020). Active cyber defence strategies and techniques for banks and financial institutions. 27(3), 771-780.
6. Demirkan, S., Demirkan, I., & McKee, A. J. J. o. M. A. (2020). Blockchain technology in the future of business cyber security and accounting. 7(2), 189-208.
7. Dunn Cavelty, M., & Wenger, A. J. C. S. P. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. 41(1), 5-32.
8. Ebrahim, R., Kumaraswamy, S., & Abdulla, Y. J. I. s. f. i. f. i. b. (2021). FinTech in banks: opportunities and challenges. 100-109.
9. Felet, C. (2019). Impediments to the provision of payment aggregator services by financial technology companies. University of Pretoria,
10. Ghelani, D., Hua, T. K., & Koduru, S. K. R. J. A. P. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking.
11. Jayalath, J., & Premaratne, S. J. I. J. o. R. P. (2021). Analysis of key digital technology infrastructure and cyber security consideration factors for fintech companies. 84(1), 128-135.
12. Kaiwartya, O., Prasad, M., Prakash, S., Samadhiya, D., Abdullah, A. H., & Abd Rahman, S. O. J. I. J. N. S. (2017). An Investigation on Biometric Internet Security. 19(2), 167-176.
13. Kaji, S., Nakatsuma, T., & Fukuhara, M. (2021). The economics of Fintech: Springer.Kalakuntla, R., Vanamala, A. B., Kolipyaka, R. R. J. H. J. o. B., & Administration, P. (2019). Cyber security. 10(2), 115-128.
14. Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). Understanding Cybersecurity Management in FinTech: Springer.
15. Kovačević, A., Putnik, N., & Tošković, O. J. I. A. (2020). Factors related to cyber security behavior.8, 125140-125148.
16. Kryparos, G. (2018). Information security in the realm of FinTech. In The Rise and Development of FinTech (pp. 43-65): Routledge.
17. Najaf, K., Mostafiz, M. I., & Najaf, R. J. I. J. o. F. E. (2021). Fintech firms and banks sustainability: why cybersecurity risk matters? , 8(02), 2150019.
18. Najaf, K., Schinckus, C., Mostafiz, M. I., & Najaf, R. (2020). Conceptualising cybersecurity risk of fintech firms and banks sustainability.
19. Nguyen, A., & Han, D. J. I. i. A. (2022). PERCEIVED TYPES, CAUSES, AND CONSEQUENCES OF FINANCIAL EXPLOITATION: NARRATIVES FROM OLDER ADULTS. 6(Suppl 1), 294.
20. Nwogugu, M. I. (2019). Earnings management, fintech-driven incentives and sustainable growth: On complex systems, legal and mechanism design factors: Routledge.
21. Saleem, A. J. I. J. o. M., & Research, C. E. (2021). Fintech revolution, perceived risks and Fintech adoption: Evidence from financial industry of pakistan. 3, 191-205.
22. Scheau, M. C., Rangu, C. M., Popescu, F. V., & Leu, D. M. J. A. U. D. Œ. (2022). Key Pillars for FinTech and Cybersecurity. 18(1).
23. Stanikzai, A. Q., & Shah, M. A. (2021). Evaluation of cyber security threats in banking systems.Paper presented at the 2021 IEEE Symposium Series on Computational Intelligence (SSCI).
24. Suseendran, G., Chandrasekaran, E., Akila, D., & Sasi Kumar, A. (2020). Banking and FinTech (financial technology) embraced with IoT device. Paper presented at the Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1.
25. Tkachenko, V., Kwilinski, A., Korystin, O., Svyrydiuk, N., Tkachenko, I. J. J. o. S., & Issues, S. (2019). ASSESSMENT OF INFORMATION TECHNOLOGIES INFLUENCE ON FINANCIAL SECURITY OF ECONOMY. 8(3).
26. Varma, P., Nijjer, S., Sood, K., Grima, S., & Rupeika-Apoga, R. J. R. (2022). Thematic Analysis of Financial Technology (Fintech) Influence on the Banking Industry. 10(10), 186.
27. Vučinić, M., Luburić, R. J. J. o. C. B. T., & Practice. (2022). Fintech, risk-based thinking and cyber risk. 11(2), 27-53.

28. Yang, W., Li, J., Zhang, Y., Gu, D. J. J. o. I. S., & Applications. (2019). Security analysis of third-party in-app payment in mobile applications. 48, 102358.
29. Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D.-P., Ghorbani, A. A. J. I. J. o. I., & Security C. (2022). Data breach: analysis, countermeasures and challenges. 19(3-4), 402-442.