JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 05 Issue 01
2023

Research Article
https://doi.org/10.56979/501/2023

Evolution of Cybersecurity in Fintech, A Scoping Review of Literature

Mohsin Asad Gill[1*], Muhammad Ahmad[2], Summaia Aziz[3], Muhammad Talha Tahir Bajwa[2], and Awais Rasool[2]

[1]School of Business, University of Southern Queensland, Australia.
[2]Department of Computer Science, University of Agriculture Faisalabad, Pakistan.
[3]Department of Computer Science, Foundation University School of Science and Technology (FUSST), Pakistan.
[*]Corresponding Author: Mohsin Asad Gill. Email: mag_gill@hotmail.com.

Received: February 19, 2023 **Accepted:** May 12, 2023 **Published:** June 05, 2023.

Abstract: In an embryonic digital world, corporations, institutions and individual assets and information are at constant risk of cybersecurity threats. Cyber security threat modelling for protection against cybercrime is a process development in parallel to the advancements of digital technologies. Races of technological advancements are also growing in cybercrime at the same time. The culprits of cybercrime continually found new ways to do fraud through Fintech companies. Financial technology users must be aware of the potential awareness and threats of using, then they would be able to recognize and prevent such situations of fraud. The increasing use of cryptocurrency is also a major factor in increasing the risk of data stealing and crimes. The aim of the study includes exploring the potential use of cybersecurity in Fintech and exploring the scope, Evolution of cybersecurity in the Fintech industry. The study is based on scoping literature review and follows the Prisma framework for adjusting data. Clusters were designed after a review related to the scope and analysis of selected literature which focused on the development of cybersecurity in Fintech. It is concluded that there is a wide demanding scope to use cyber security networks to avoid security threats and malicious attacks from outside data thieves.

Keywords: Cybersecurity, Fintech, Scoping Review, Evolution.

1. Introduction

The influx of technology advancements in the financial sector is referred to as "FinTech," a term that has grown in popularity over the last three to four years. According to Ng and Kwok (2017), Skan, Dickerson, and Masood (2015), among others, these innovations can be in the form of externally produced goods or services. Credit card processing, internet banking, and digital currencies are a few examples of recently released products and services that are changing the market (Callen-Naviglia and James, 2018). Internal technological advancements made by a financial institution may include, but are not limited to, the development of cloud-based apps and the upgrading of legacy systems.

Businesses, investors, and consumers are all increasingly resorting to FinTech to stay competitive, grow market share, and offer services at cheap or no cost (Leong & Sung, 2018). Therefore, the following FinTech trends are anticipated for 2018: automated financial decisions and actions (such as autopay, financial apps), FinTech acquisitions by large banks, advanced identity validation within financial services, automation of fraud and risk, FinTech expansion into business-to-business lending, advanced know your customer (KYC) products, and the definition of the monetary system provided by The Evolution of FinTech Callen-Nathanson. The expansion and development of FinTech in the United States' financial and finance systems is depicted in Figure 1.

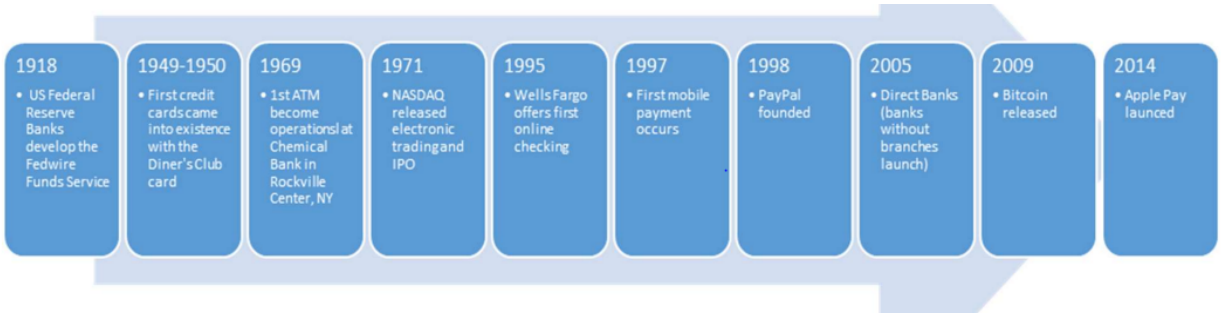

Figure 1. The evolution of FinTech within the Monetary System of the U.S. (CallenNaviglia, 2017)

Cyber Security, with new potential for both the global economy and people worldwide, the internet and IT have revolutionized the world. Modern society cannot function without the Internet and IT, but this dependency has also made it easier for new types of cybercrime and terrorism to emerge from a wide range of sources (Spidalieri & Kern, 2014).

According to Wang et al. (2015) and Whitley (2009), cybersecurity refers to a system or tool that shields for-profit businesses, public institutions, banks, and other financial institutions from hostile attacks intended to intentionally harm electronic assets. This is required due to the significance of technological advancement and the increasing reliance on smart devices across all industries, particularly in the financial sector and in the delivery of services over the Internet. Despite the benefits of increased connectedness, fraud and abuse are now more common than ever (Jain et al., 2023). People are becoming increasingly vulnerable to cyberattacks including phishing, blackmail, fraud, and social media fraud as the world's population becomes more reliant on contemporary technology (Stevens, 2018). Cyberspace and the infrastructure that supports it are incredibly poorly safeguarded, making them vulnerable to a wide range of physical and electronic attacks. Actors who pose these threats prey on their adversaries' technological and national security weaknesses in an effort to steal data and money, disrupt, destroy, or just cause disruption (khan & Malaika, 2021).

The study conducted on scoping review of literature, Scoping review relates to the type of review which focuses on the potential size of available literature, expanded empirical research aims to clarify the nature of the research scope (Grant & Booth, 2009). In this study, the researcher wanted to explore the crucial use of cyber security in the Fintech industry. Nowadays, it's a need of every company to do advanced measures against security threats. The objectives and research questions were also relates to explore the scope of cybersecurity in Fintech.

2. Objectives

To explore the potential application of cyber security in the Fintech industry.
To investigate the evolution of cyber security in Fintech through literature studies.
To explain why cyber security is important in the Fintech industry.
To explore the potential scope of cyber security in the Fintech industry.

3. Research Questions

What is the potential use of cyber security in Fintech?
What are the advancements used to provide protection from cyber threats to the Fintech industry?
What is the scope of cyber security applications and importance in Fintech?

4. Methods

The study relates to the evolution of cyber security in Fintech, for the purpose of literature review, scoping literature review was selected to do the rigorous review of quality based articles. Moreover, Prisma scoping review framework was used for further procedure of selecting valuable literature. Initially, for identification of data, google scholar was used where Scopus journal articles are easily available with full access. Data search included articles which were published between the periods of 2020 to 2023. Other indexed journal and articles were identifies related to the study variables; cyber security and Fintech. Some studies were excluded as of biased assessments or risk factor. In the next step, articles were included and

excluded because of their eligibility and ineligibility criteria. Then in the final step 28 articles were selected for the inclusive purpose of scoping review. Prisma provides a sequence of doing analysis with a flow, how to follow a method. Most of the researchers used Prisma check list for meta-analysis and systematic review related learning and challenges about Fintech (Dawood et al., 2022; Malibari et al., 2023)

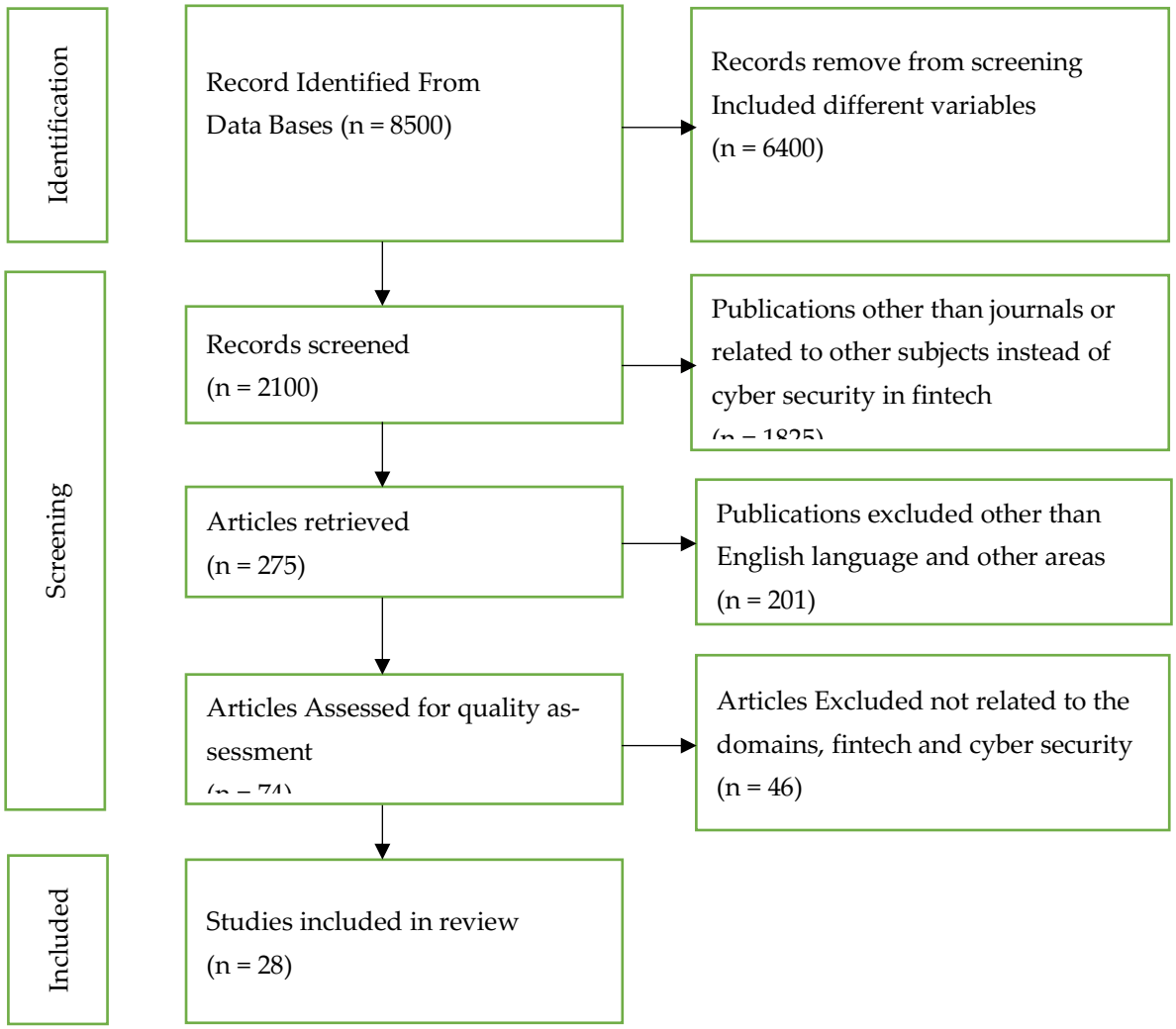

Figure 2. Prisma Framework to Select Literature for Scoping Review

5. Results

Through the screening process of data, minimal data were utilized for review. After a thorough review, some clusters were generated to explore and clarify the scope of cybersecurity in Fintech.

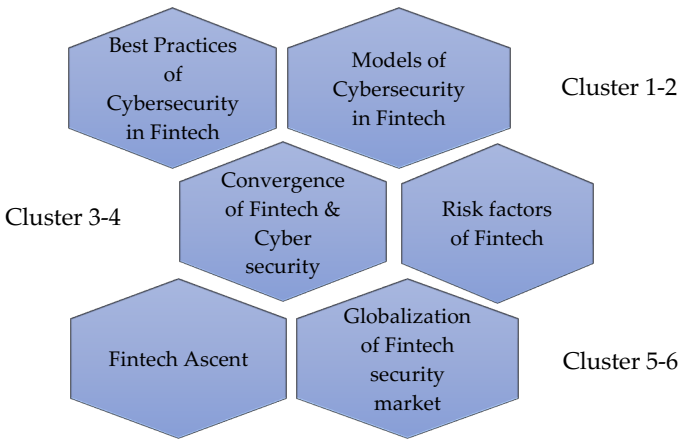

Figure 3. Clusters developed through Scoping Review

6. Cluster 1: Laws Governing Cyber Security in the Financial Technology Sector & Some Best Practices

Money is such a sensitive topic, therefore it seems sense that the financial sector is heavily regulated. The act of holding money and offering banking services also requires holding personal data. The security of set data and important client information may still be subject to state privacy laws, according to a Benzinga report that was released in late 2022 (Kaur, 2022). It's a good thing that regulatory agencies with authority over financial services, like the Securities and Exchange Commission, the Federal Trade Commission, and the Consumer Financial Protection Bureau, have tightened their regulations in recent years to make it clear that fintechs need to adhere to rigorous cybersecurity standards. Because the aforementioned does not stop firms from finding gray areas within which to operate, consumers should take extra precaution when dealing with a company that has no history (Despotovi et al., 2022). The recent collapse of a cryptocurrency company, which affected millions of people and raised additional cash, may also be a signal for regulators to look more closely at businesses that operate in a similar field in order to help protect consumers and the general public in the future. Although there is still a long way to go until solid cyber security standards are implemented across the entire business, it does seem that more attention has recently been devoted to legislation around consumer protection in fintechs, with much more to come (Zouros, 2022).

7. Cluster 2 : Models for Reducing Cyber Risk in The Financial Technology Sector

Cyber scams that have emerged as a result of the growth of digital data include extortion, distributed denial of service assaults, and credit card fraud. Cyberattacks have increased in frequency recently. Understanding the different kinds of cyber risks and the causes of cyber accidents is crucial in order to reduce these occurrences (Kaur et al., 2021). The global FinTech sector is exposed to cyber threats from numerous threat categories. Cyber-attacks are launched for a variety of reasons, including political, economic, and religious ones. For the purpose of eliminating cyber risks, threat modeling is crucial. The structural method used in FinTech threat modeling puts an emphasis on attacks, attackers, software, and assets. FinTech institutions can be protected using threat modeling tools as STRIDE, Trike, VAST, and PASTA (Kaur et al., 2021). The financial regulator adopts a strategic approach that makes use of Fintech potential while embracing cyber risk exposures by putting in place thorough risk-based processes to support institutionalization of cybersecurity among regulated firms through strategic controls (Ng & Kwok, 2017).

8. Cluster 3 : Convergence of Financial Technology & Cyber Safety

Hackers have been targeting the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system, and their attacks are becoming more and more sophisticated. Bank organizations all throughout the world rely on the SWIFT system to transfer sensitive data, such as bank transactions or malware assaults. The potential of data-leakage attacks on sensitive financial information given by clients, such as credit card numbers and login credentials, rises as a result of third-party fintech agreements between banks (Singh et al., 2021; Kaur et al., 2021). Mobile devices are becoming more and more crucial to fintech financial services. If mobile devices without powerful encryption algorithms are utilized for fintech services, there may be issues with the integrity of the financial data delivered via the variety of fintech interfaces. Time: (Vimal Mani, 2019). A robust financial ecosystem is made possible by the cloud. A financial ecosystem can benefit from specialized services offered by cloud computing, including payment gateways, digital wallets, and safe online transactions (Hossain et al., 2022). Thanks to cloud computing, the procedure of making a payment, for instance, is streamlined and quick. Banks and financial services cannot afford to jeopardize the security of their customers' financial data or violate their customers' privacy. Inadequate cloud security measures could lead to the compromise or alteration of this private data (Singh et al., 2021).

9. Cluster 4: The Risk Fintech Poses to Cybersecurity

Implementing fintech entails cybersecurity threats due to integration problems including compatibility and out-of-date technologies. Risks to data privacy could result from the integration of old banking systems with fintech. Fintech companies are frequently the target of hackers due to the massive amounts of client data that they acquire, particularly extremely personal data (Al Duhaidahawi et al., 2020). Groups

that were formerly financially excluded now have simple access to basic banking services thanks to developments in financial technology. Due to their lack of cybersecurity awareness, these new bank customers may be more vulnerable to cyberattacks. Application programming interfaces (APIs) established specifically to let banks communicate with fintech platforms are referred to as API banking (Najaf et al., 2021). Open application programming interfaces (APIs) make it possible for outside developers to create software specifically for the banking industry. Due to its complexity and technological connections, the numerous interconnected systems that make up a fintech ecosystem make it an alluring target for hackers. Due to the nature of the data transferred, there are more cybersecurity concerns connected with the transfer of data elements across the interfaces necessary for fintech implementation with banks, financial service providers, and fintech enterprises (Rehman et al., 2023).

10. Cluster 5: Fintech's Ascent

As a result of the advent of globalization and digitization, which has transformed the financial services industry, many small and large enterprises alike have developed online platforms to assist financial transactions (Najaf et al., 2021). The creation of Fintech 3.5 was made possible by the rise of Fintech 3.0, which dismantled traditional hurdles for regulated financial institutions (Setiawan & Maulisa, 2020). People are abandoning the antiquated financial system and embracing cutting-edge tools like Bitcoin and digital wallets, which makes Fintech 3.5 conceivable. In the two time periods, consumers' financial situations were different (Arner et al., 2015). Fintech 3.0 has been implemented in developed countries since they have better banking infrastructure and network coverage.

Fintech 3.0 is revolutionary due to the way it integrates cybersecurity into its service platforms as well as the way it employs and implements technology. Blockchain, which employs a distributed, encrypted ledger to securely communicate data between users upon request, is one of the most well-known Fintech 3.5 cybersecurity technologies (Ratecka, 2020). This is crucial for both bitcoin trading and fighting money laundering. Additional advances that have appeared in the modern era include biometric alternatives, device-based cryptosystems, and two-factor authentication. Fintech 3.5 has thus marked a pivotal moment in the execution of cybersecurity activities by urging the improvement of everything from fundamental security procedures like password setting to cutting-edge cyber obstacles like ethical hacking (Al Duhaidahawi et al., 2020). 2019 marks the beginning of the FinTech 5.0 era. Modern financial markets, a circular economy, innovative growth, Smart Cities, the incorporation of cloud computing into virtual systems, big data technology, and the Internet of Things are characteristics of this period. Financial independence, effective marketing, and original thought are traits of the contemporary era (Mah et al., 2022).

Era	Date	Events	5 P's of marketing	Transition Causes
FinTech 1.0	1866-1967	Industrial Revolution	People->products	Fall of slave trade
FinTech 2.0	1967-2008	Internet/digital process	Products->Place (Markets)	End of cold war/rise of decolonization
FinTech 3.0	2008-2013	Smart Phones, Social media platforms and new financial market services	Place-> Price (Online markets)	2008 financial crisis
FinTech 4.0	2013-2019	Industry 4.0/Machine learning/ Emerging markets	Price-> Promotions (innovative Online & Paperless systems)	COVID-19
FinTech 5.0	2019-Date	Advance financial markets, circular economies, development of innovations, smart cities, Cloud base systems, Big data, and internet of things.	Promotion->Smart contracts (advancements in Online & Paperless systems)	-

Figure 4. Evolution of Fintech (Adopted from (Mah et al., 2022))

11. Cluster 6: Globalization of the Fintech security market

The ongoing global instability brought on by the conflict in Ukraine and Russia has prompted internet giants and financial companies to beef up their cybersecurity defenses. Businesses all over the world are supporting more dispersed workforces, which adds to the lack of cyber talent (Al Duhaidahawi et al.,

2020). This situation has been exacerbated by the widespread use of cloud computing and the rising cost of cyberattacks as they become more aggressive and challenging to defend against. Google has bought Mendicant, a well-known cybersecurity company. The sale reportedly cost an amazing US$5.4 billion, making it Google's second-largest acquisition ever and a glaring example of how important protecting their systems from current threats is to the firm. Fintech security is reaching the highest peak in the developing current digitalized era (Despotović et al., 2023).

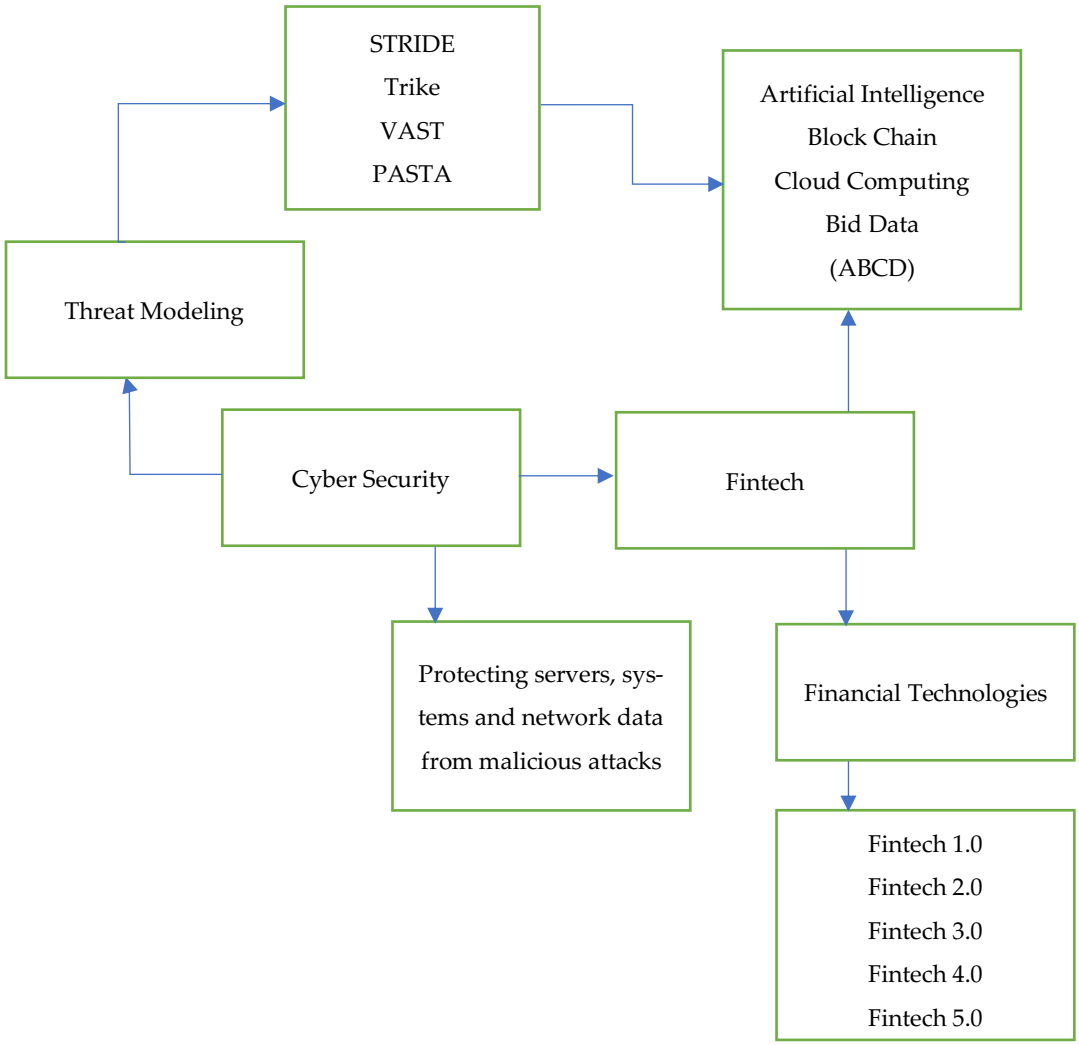

Figure 5. Evolution of Cyber security in Fintech

12. Discussion

The growth of fintech is one of the best things that has ever happened to humanity; it has decreased global dependence by enabling creative people to use their skills more effectively through more advanced services (Khan & Malaika, 2021).

Fintech includes technologically enabled breakthroughs in business models and digital technology. These changes could lower barriers between industries, encourage strategic disintermediation, change the way that well-established companies deliver their services, stimulate the creation of new business models, and make financial services more accessible to a larger population (Kakinuma 2022).

"The future of Fintech is promising, and it would be a shame to see its activities cut short by pitfalls that could have been avoided"19, with cybercrime being the most dangerous of these roadblocks. Because of this, FinTech professionals should always remember that no one is totally protected from cyberattacks. FinTech companies may have to keep this nightmare truth in mind when conducting daily transactions in

an increasingly vulnerable digital world (Despotovi et al., 2023) because, as Robert Mueller once said, "there are only two types of companies: those that have already been hacked and those that will be."

Investment in FinTech has grown significantly since the global financial crisis of 2008 (Skan, Dickerson, and Masood, 2015; Ng and Kwok, 2017). To continue serving their consumers and expand their companies, financial institutions work to innovate or develop new products and services (Ng & Kwok, 2017). The regulatory and compliance landscape has had to adapt as a result of technological advancements in American banking, to be more particular and to focus on the US. As the fintech industry grew, it brought technical innovations to a field that had grown fixated on rules and regulations. For instance, the emergence of digital currencies has brought attention to the dubious effectiveness of current legal and regulatory systems. The regulatory system already in place is enough for monitoring and managing virtual currencies. However, in an effort to regulate virtual currencies, the state of New York created a new regulatory framework in 2015 dubbed BitLicense. The BitLicense in New York is a ground-breaking piece of legislation. Based on the outcomes of BitLicense—both favorable and negative—further efforts to regulate FinTech goods and services may be made (Callen-Naviglia, 2017; Hughes, 2014). The risks of cybercrime are becoming more and more prevalent in the financial industry as a result of the quick speed of technological advancement and the growing use of digitalized financial products and services. According to Pascu (2017), there were 9% more data breaches in 2017 than there were in 2016. As a result, from 58% in 2016 to 78% in 2017, firms in the financial sector boosted their IT security budgets. Along with the growth of FinTech, cybersecurity is receiving more attention (Jain et al., 2023).

With the growth of Internet-connected devices and the increase in mobile phone use at home and at work, cybersecurity is one of the most discussed topics currently. Knowing how to secure yourself online is crucial in today's society (Zouros, 2022). The prevention of unauthorized access to computer systems, networks, devices, software, or data is one definition of cyber security. Additionally, before a network is even implemented, the process of defending its data from intruders like viruses and unauthorized users starts during the design phase. This is due to the possibility that a weak application could provide an outsider access to private data that was supposed to be protected (Marican et al., 2022; Jain et al., 2023).

A few examples of traditional crimes committed in cyberspace include the creation and distribution of child pornography, the use of children in exploitation schemes, banking and financial fraud, intellectual property infringement, and other traditional crimes with serious human, economic, and legal repercussions (Jain et al., 2023). Because of this, experts and researchers have worked hard to develop smart technologies like artificial intelligence and other methods to detect and defend against cyberattacks before they happen (Marican et al., 2022). To detect and identify dangerous apps, deal with their effects, and develop protocols to demonstrate the user's personality to the software, clever programmes and skilled programmers were used (Grant & Booth, 2009). Five people were trained in them and examined how and how to attack during this time period after reports of attack incidents were gathered from 2012 to 2018 with the aim of introducing people, protecting their files, and determining who is carrying out the attack through the use of language processors and personal files (Zouros, 2022). It should be noted that a significant portion of cyber threats have been acquired through what we have identified as two different types of risks, the first on the user's end and the second on the server end, where data were stored (Marican et al., 2022).

13. Conclusions

In the Fintech industry, security and privacy of data are vital trepidations. It’s the responsibility of the company to provide full security to the user's personal information, which information is very sensitive. The study was conducted to explore the need and scope of cybersecurity in Fintech companies. In the 21st century, everyone is surrounded by technology so they need security as well for protection from fraud. The use of cyber security is also advancing in Fintech. Scoping review method was adopted to explore the cybersecurity crucial scope in Fintech. It is concluded that there is a wide demanding scope to use cyber security networks to avoid security threats and malicious attacks from outside data thieves. In the past years, Fintech is growing fast, uses using technologies like Fintech 1.0 and Fintech 5.0 were utilized to provide service to its users. For this, they were using some cyber threat modeling including STRIDE and others, which are famous, recognized ones. The evolution of cyber security is getting on its peak in every finance-providing company.

14. Recommendations

Recommending ahead that Fintech companies can invest in cyber security networks to ensure the security and privacy of customers' services, their statistical data, financial resources and personal information. Future researchers should focus on its security setup development and bringing awareness among the customers on how they can avoid data thefts. Furthermore, researchers might conduct a scoping review of Fintech's technological advancements. It can also be measured security reviews and security breaches through, evaluations, and regular testing procedures to avoid risks. Additionally, transparent privacy policies should be given to the customers, the outlets providing information on how to use, collect and share data ensuring privacy.

References

1. Al Duhaidahawi, H. M. K., Zhang, J., Abdulreda, M. S., Sebai, M., & Harjan, S. (2020). The financial technology (fintech) and cybersecurity: Evidence from Iraqi banks. International Journal of Research in Business and Social Science (2147-4478), 9(6), 123-133.
2. Arner, D. W., Barberis, J., & Buckley, R. P. (2015). The evolution of Fintech: A new post-crisis paradigm. Geo. J. Int'l L., 47, 1271.
3. Callen-Naviglia, J., & James, J. (2018). FINTECH, REGTECH AND THE IMPORTANCE OF CYBERSECURITY. Issues in Information Systems, 19(3).
4. Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and Cyber Security in Fintech. In Digital Transformation of the Financial Industry: Approaches and Applications (pp. 255-272). Cham: Springer International Publishing.
5. Hossain, M. J., Rifat, R. H., Mugdho, M. H., Jahan, M., Rasel, A. A., & Rahman, M. A. (2022, November). Cyber Threats and Scams in FinTech Organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh. In 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) (pp. 190-195). IEEE.
6. Jain, R., Kumar, S., Sood, K., Grima, S. and Rupeika-Apoga, R., 2023. A Systematic Literature Review of the Risk Landscape in Fintech. Risks, 11(2), p.36.
7. Kakinuma, Y. (2022). Financial literacy and quality of life: a moderated mediation approach of fintech adoption and leisure. International Journal of Social Economics, 49(12), 1713-1726.
8. Khan, M. A., & Malaika, M. (2021). Central Bank Risk Management, Fintech, and Cybersecurity. International Monetary Fund.
9. Leong, K., & Sung, A. (2018). FinTech (Financial Technology): What is it and how to use technologies to create business value in fintech way?. International Journal of Innovation, Management and Technology, 9(2), 74-78.
10. Mah, P. M., Skalna, I., Muzam, J., & Song, L. (2022). Analysis of natural language processing in the fintech models of mid-21st Century. Journal of Information Technology and Digital World, 4(3), 183-211.
11. Malibari, N., Katib, I. and Mehmood, R., 2023. Systematic Review on Reinforcement Learning in the Field of Fintech. arXiv preprint arXiv:2305.07466.
12. Marican, M.N.Y., Abd Razak, S., Selamat, A. and Othman, S.H., 2022. Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. IEEE Access.
13. Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech firms and banks sustainability: why cybersecurity risk matters?. International Journal of Financial Engineering, 8(02), 2150019.
14. Naviglia, J. C. (2017). The Technological, Economic and Regulatory Challenges of Digital Currency: An Exploratory Analysis of Federal Judicial Cases Involving Bitcoin (Doctoral dissertation, Robert Morris University).
15. 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.
16. 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.
17. Ratecka, P. (2020). FinTech—definition, taxonomy and historical approach. Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej w Tarnowie, (1 (45)), 53-67.
18. Rehman, F. U., Attaullah, H. M., Ahmed, F., & Ali, S. (2023). Data Defense: Examining Fintech's Security and Privacy Strategies. Engineering Proceedings, 32(1), 3.
19. Skan, J., Dickerson, J., & Masood, S. (2015). The Future of Fintech and Banking: Digitally disrupted or reimagined. Accenture, London.
20. Spidalieri, F., & Kern, S. (2014). Professionalizing cybersecurity: A path to universal standards and status. Newport, RI: Pell Center for International Relations and Public Policy, Salve Regina University.
21. Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. Politics and Governance, 6(2), 1-4.
22. Vimal Mani, C. I. S. A. (2019). Cybersecurity and Fintech at a Crossroads.
23. Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and software-defined networking. Computer Networks, 81, 308-319.
24. Setiawan, K., & Maulisa, N. (2020, March). The Evolution of Fintech: A Regulatory Approach Perspective. In 3rd International Conference on Law and Governance (ICLAVE 2019) (pp. 218-225). Atlantis Press.
25. Kaur, G., Habibi Lashkari, Z., Habibi Lashkari, A., Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Cybersecurity Risk in FinTech. Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends, 103-122.
26. Dawood, H., Al Zadjali, F., Al Rawahi, M., Karim, S., & Hazik, M. (2022). Business trends & challenges in Islamic FinTech: A systematic literature review. F1000Research, 11.
27. Singh, G., Gupta, R., & Vatsa, V. (2021, November). A framework for enhancing cyber security in fintech applications in india. In 2021 International Conference on Technological Advancements and Innovations (ICTAI) (pp. 274-279). IEEE.
28. Schatz, D., Wall, J., Schatz, D., & Wall, J. (2017). Security and law towards a more representative definition of cyber security towards a more representative definition of cyber security. Journal of Digital Forensics, 12(2), 1306396.
29. Kaur, G., Habibi Lashkari, Z., Habibi Lashkari, A., Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Cybersecurity Threats in FinTech. Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends, 65-87.

30. Kaur, G., Habibi Lashkari, Z., Habibi Lashkari, A., Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Cybersecurity Vulnerabilities in FinTech. Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends, 89-102.
31. Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. Health information & libraries journal, 26(2), 91-108.
32. Zouros, E., 2022. Cybersecurity in Fintech Companies.