المجلة العربية للعلوم الإنسانية والاجتماعية
Arab Journal for Humanities and Social Sciences

Impact factor isi 1.304

العدد العشرون / آب 2023

Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review.

Ahmed Abdulrhman B. Alodhiani

Saudi Federation for Cybersecurity, Programming and Drones, Riyadh, Saudi Arabia.

aodyanidata@gmail.com

Abstract:

This research aims to identify the threats posed by cybercrime to the fintech sector, as well as the preventative measures taken by the industry in the form of cybersecurity. This study employs a systematic literature review approach to analyzing previously published publications on cybercrime and cybersecurity in the financial technology industry. The survey found that cybercrime issues in the fintech industry include lax cybercrime rules, theft of data and information, and infringement of intellectual property. Proactive measures strengthened legislation, and establishing a trustworthy cybersecurity framework or system may all be used to combat cybercrime in the fintech industry.

This study's findings may serve as a resource for academics, practitioners, regulators, and fintech players interested in learning more about the evolution of cybercrime and cybersecurity in the financial technology sector. While this study does an excellent job of summarizing and expanding upon the research findings in each chosen article, it needs to analyze the connections between the pieces. Broadening the scope of the article under evaluation, using other literature review techniques, or doing more empirical research are all viable options for recommending additional studies to corroborate the findings of the current one.

Keywords: Cybercrime, cybersecurity, financial technology, fintech regulation, intellectual property theft.

الملخص:

تهدف هذه الدراسة إلى تحديد تحديات الجرائم الإلكترونية التي تواجه صناعة التكنولوجيا المالية بالإضافة إلى الإجراءات الاستباقية في شكل الأمن السيبراني للتغلب على هذه التحديات. تستخدم هذه الدراسة طريقة مراجعة منهجية للأدبيات من مقالات مختلفة تناقش الجرائم الإلكترونية والأمن السيبراني في التكنولوجيا المالية والتي تم نشرها في قواعد بيانات موثوقة على الإنترنت. تشير النتائج إلى أن مشاكل الجرائم الإلكترونية في التكنولوجيا المالية تتكون من لوائح الجرائم الإلكترونية غير الصارمة ، وسرقة البيانات والمعلومات ، وسرقة الملكية الفكرية التي تؤثر على سمعة التكنولوجيا المالية. يمكن تنفيذ الأمن السيبراني كمحاولة للتصدي للجرائم الإلكترونية في التكنولوجيا المالية من خلال الإجراءات الاستباقية ، وتعزيز اللوائح ، وإنشاء إطار أو إجراء موثوق للأمن السيبراني. تعد الآثار المترتبة على هذا البحث بمثابة مرجع إضافي للأكاديميين والممارسين والمنظمين والجهات الفاعلة في مجال التكنولوجيا المالية فيما يتعلق بالتطور السريع للجرائم الإلكترونية والأمن السيبراني في التكنولوجيا المالية. يتمثل الحد من هذه الدراسة في أنها تقدم فقط نظرة عامة وتوضح نتائج الدراسات السابقة بدلاً من تقديم تحليل إضافي للعلاقة بين المقالات التي تمت مناقشتها. التوصيات لمزيد من البحث لزيادة نطاق المقالات المدروسة أو تطبيق طرق مراجعة الأدبيات الأخرى أو إجراء بحث تجريبي لتأكيد نتائج هذه الدراسة.

الكلمات المفتاحية: الجرائم الإلكترونية، الأمن السيبراني، التكنولوجيا المالية، تنظيم التكنولوجيا المالية، سرقة الملكية الفكرية.

Introduction:

Financial technology, or FinTech for short, is an emerging business that uses technology to enhance financial operations and compete with more conventional means of delivering financial services. This innovation makes banking and other financial services available to more people, as seen by the rise of cellular banks, mobile phone-based investing services, and digital currencies like Bitcoin. Companies in the financial technology sector include start-ups, incumbent banks, and IT firms to improve or replace traditional financial services. As Peters et al. (2015) point out, many modern financial institutions use financial technology solutions and technologies to advance their service offerings and strengthen their market standing. Thus, we conclude that developments in financial technology work hard to enhance the efficiency of the financial system for all public and private sectors, enterprises, and consumers, but also increase the likelihood of financial risks and losses. To foster financial innovation and accelerate the growth of these services, policymakers, titles, and rules aim to safeguard all parties involved (Philippon, 2016; Shah et al., 2018).

By capitalizing on technological advancements in the financial sector, a new generation of financial technology companies has developed in recent years, changing the landscape of financial markets throughout the globe. Given the rate of change, it is crucial to implement measures that ensure the financial technology revolution is used for the good of society and the economy while protecting consumers and the financial system.

Changes in technology throughout time have allowed finance to flourish and expand. Fintech advancements over the last decade have made various financial services more accessible to consumers in the fields of payments, loans, insurance, savings, and investing, and at a scale and speed never before seen (Kim et al., 2015). However, this practice raises several questions about the security of customers' personal information, as well as the likelihood that machine learning and artificial intelligence will be employed for risk management in the banking industry (Kareem et al., 2020)., Consumers may fall victim to fraud if it is feasible for them to do so inadvertently, unexpectedly, or unaware of what they are getting into. As a result, businesses with the know-how to cope with cutting-edge technology, the ability to offer electronic financial services, and the means to thwart cyber-attacks are tasked with accelerating the transition to cloud computing.

Most importantly, although the new world is ripe with possibilities, it also poses several known and unknown threats at various levels, beginning with people (Sinan Abdullah Harjan et al., 2019). Non-bank online lenders have been on the rise recently, making it easier to get a loan when needed. However, with this convenience comes the added responsibility of industry watchdogs who must ensure the safety of their clients in a system that can quickly become overwhelming (Sadakowski & Sobieraj, 2017). Industry watchers debate how well third-party service providers adhere to standards and implement crucial security safeguards using electronic means since they now dominate service provision through electronic management. Consumer-focused innovations like POS terminals and payment processing are getting a lot of attention, and they're expected to improve the shopping experience overall. Here, worries emerge concerning the influence of the dominant service providers' market dominance on consumers who lack the knowledge to make informed decisions (Sinan A. Harjan et al., 2015). Simultaneously, unique Cryptocurrencies have evolved to facilitate payments in a manner distinct from conventional monetary systems. While this method promotes anonymity, it also raises serious issues about money laundering and consumer safety. Crowdfunding, currency offerings, and new ways to trade stocks and manage assets are all examples of how Fintech provides novel and effective means to raise individual capital. This, in turn, increases the bar for protecting investors, leading to the passage of several pieces of legislation meant to regulate and mitigate the dangers posed by the financial technology sector (Firmansyah & Anwar, 2019; Hayder M. Kareem et al., 2019).

As a result of these changes, the prevalence and sophistication of cyberattacks are both on the rise. It is crucial to define the type of threat and understand the risks associated with Cybersecurity and its effects on financial services. Those who specialize in attack operations work to improve their methods to develop rapidly and faster than security teams can, resulting in more sophisticated ways. This was true even before the advent of e-crime, and it only increased as the frequency and severity of assaults increased and as regulators were kept more apprised of the situation. Knowing the ever-evolving nature of the threats faced by financial institutions is crucial for enhancing design, service delivery, risk management, and staff training because hackers will always find a way in. This blog aims to lighten the current climate and the reactions of financial institutions, including banks and insurers. We can't undertake a deep dive, but we'll provide enough information so chief financial officers will reevaluate how they're doing CybersecurityCybersecurity.

The rise of financial technology, or Fintech, is a hallmark of the 21st century. These apps and programs have changed the banking and personal business industries as technology and the need for convenience have advanced. Although financial technology is not new, it has come under increasing cyberattacks in recent years. Cyberattacks in the financial technology sector have been prevalent since the late 2000s (Sadakowski & Sobieraj, 2017) but have increased since 2017.

The expansion of "financial technology" firms and the radical shifts they have wrought in monetary theory and practice across the board, from the nature of banking to how capital is created and on to the very heart of currency itself. In the age of technology-enabled funding, these shifts need a radical rethinking of financial regulation. This is especially true (Magnuson, 2018).

As technological progress is present across all industries, including finance, financial technology is poised to take the helm of the financial services industry shortly. Therefore, as financial technology grows significantly, more robust, Cybersecurity measures are required. Thus, all of the advantages of modern financial technology are recovered. This calls for advanced planning across various domains, including cyber governance, improved familiarity with Internet technology, analysis of security facts, and the formation of security partnerships. For instance, they are building trust factors and guaranteeing dependable security partnerships between the different parts of the financial system. While innovations like Clear from Fintech have been helpful, they cannot be implemented at the cost of the security and longevity of financial institutions or the rights of their customers.

A literature analysis on technical problems and the anticipation that has been carried out by Fintech so far is required to deepen the knowledge of academics, practitioners, regulators, and Fintech players. A literature study of cybercrime and CybersecurityCybersecurity in Fintech is intended to offer a snapshot of the evolving nature of these two topics. Previous studies examined Fintech (Li & Xu, 2021; Milian et al., 2019), and the general difficulties encountered by Fintech (Adeyoju, 2019; Suryono et al., 2020) served as the basis for this investigation. This study aims to catalog existing research on cybercrime and CybersecurityCybersecurity in financial technology (Fintech) and outline its historical and future evolution for the benefit of interested parties and potential researchers (Kitchenham & Brereton, 2013; Xiao & Watson, 2019).

To get findings that apply to all of the articles chosen for this study, the researchers had to choose, gather, extract, and analyze the reports per the research questions. Cybercrime and CybersecurityCybersecurity in Fintech are broad topics; this study's findings provide an overview that can be used as a reference for theories, frameworks, and research models, enhancing our ability to understand and prepare for cybercrime threats and paving the way for new avenues of inquiry.

Problem statement:

Financial institutions are the most susceptible to the dangers posed by these threats; the primary issue is that huge hazards have also emerged with the recent growth and high capabilities of financial and banking services. In addition, these services are accompanied by vicious assaults, for which institutions need to make adequate preparations. Consequently, the oversight of financial operations and regulatory authorities must be responsible for supervising oversight mechanisms following the development of electronic financial processes and the hazards of these developments.

Based on the explanations that came before, we may formulate the research questions as follows:

- What difficulties does the financial technology industry confront in terms of cybercrime?
- What role does cybersecurity play in anticipating cybercrime risks within the finance industry?

Research objectives:

The purpose of this research is to understand the reality of financial technology and how it affects cybersecurity by understanding the effect of cybercrime, obstacles, and hazards associated with financial technology and how they affect cybersecurity.

- To explore the difficulties that fintech companies are having with cybercrime
- To find out how cybersecurity in fintech companies are preparing for cybercrime threats

Literature review:

Financial Technology (FinTech)

Fintech, an innovative approach to financial services that seeks to rival traditional services in style, employs technology to enhance economic activities. This involves utilizing smartphones and tablets to access financial and banking services for all operations, including borrowing and investment (Lin, 2015; Schueffel, 2018). Multidisciplinary in nature, the topic at hand amalgamates the domains of finance, technology management, and innovation management. Leong (2018) highlights the efforts to enhance financial services through technical solutions tailored to various work scenarios. Additionally, integrating Cryptocurrencies in financial transactions has become increasingly accessible to the general public. Companies specializing in modern technologies strive to improve traditional financial services and transform them into technology-based entities.

Consequently, the term financial technology has gained significant attention among researchers. Therefore, it is crucial to comprehend financial technology to ensure coherence in texts within this emerging field of study. According to Schueffel (2018), one of the systematically researched definitions of fintech suggests that it involves using technology to provide financial services in a new and innovative manner. This definition acknowledges that banks have been developing their activities since ancient times and cannot be excluded from the realm of technology. Thus, fintech can serve as a source of inspiration for scientific health research.

In contrast, these financial institutions have dedicated considerable effort towards developing digital advocacy systems over an extended period, as well as creating novel financial services. During its inception, the concept of an Automated Teller Machine (ATM) was a groundbreaking innovation. Following the proliferation of the Internet during the 1990s, financial institutions have established online banking platforms for their customers, while MasterCard has implemented cutting-edge technologies to facilitate online transactions (Nikkel, 2020).

Simultaneously, the fintech industry is experiencing rapid growth. Several industries compete to provide services that align with contemporary advancements, facilitating seamless service transfer for consumers. This is evident in social networking programs and other online service providers like Amazon (Wulan, 2017).

Fintech's application by financial services providers in international stock exchanges, as identified by specialized institutions in the market and through legal frameworks established by the Financial Supervision Authority, will be more appealing and have a more significant impact on consumers in areas where these industries have grown significantly in recent years, in addition to providing means to guarantee that customers receive on services in online trading platforms (Micu, 2016).

The researchers didn't stop there; some of them also tried to understand the extent to which technology is permitted in Islamic law, so long as it complies with the provisions of this law; they also talked about the difficulties of Islamic finance in Indonesia and Singapore; they collected data by sending out surveys to a sample of businesses via online social media; and they concluded, among other things, that IoT has a bright future. Therefore, regulators of these operations must move in a constructive direction to support Islamic finance, and the academic community must investigate the application of Islamic financial technology and strike a balance between theory and practice (Firmansyah & Anwar, 2019).

Cybersecurity

In light of the widespread use of the Internet, smart and mobile devices, it has become imperative to prioritize cybersecurity measures in our contemporary era. This applies to individuals, organizations, and even at the state level. Cybersecurity has emerged as a prominent topic recently, and acquiring knowledge in this field has become necessary. Cybersecurity can be defined as safeguarding electronic systems, networks, devices, programs, or data from theft or damage, thereby ensuring information security (Schatz et al., 2017). It is essential to exercise caution against malicious attacks and electronic attempts to compromise and steal systems, given that the entire process is computerized and relies on smart devices. This is necessary to prevent electronic attacks and malicious attempts that may destroy or disrupt systems or networks at large (Von Solms & Van Niekerk, 2013). In addition to safeguarding computer networks against intrusive and opportunistic entities, including targeted attackers and malware, it is imperative to prioritize maintaining programs and hardware to prevent potential threats. This is because compromised applications can grant access to protected data. It is crucial to note that implementing a successful security concept should commence during the initial design phase before deployment. The significance of technological advancement and the growing dependence on smart devices in various industries, particularly in financial businesses and online service provision, has led to the need for protective measures against hostile attacks aimed at causing intentional harm to private organizations, government agencies, banks, and other financial institutions, given that the assets of the electronic environment require safeguarding (Wang et al., 2015 & Whitley, 2009). Cybersecurity has emerged as a significant global challenge in today's interconnected world. Notwithstanding its benefits, the growing interconnectedness has resulted in an escalated susceptibility to theft, fraudulence, and exploitation.

The increasing reliance of individuals worldwide on contemporary technology has rendered them susceptible to various forms of cyber-attacks, including but not limited to corporate security breaches, phishing, blackmail, fraud, and social media fraud (Stevens, 2018). The susceptibility of cyberspace and its underlying infrastructure to various electronic and material risks have resulted in significant insecurity. Adversaries, including non-state and state actors, exploit the vulnerabilities of their opponents to steal information and funds and to acquire the capacity to impede, dismantle, or merely jeopardize the adversary's ability to provide essential services. The realm of cyberspace has witnessed the perpetration of a multitude of conventional criminal activities, such as the creation and dissemination of child pornography, the exploitation of minors, fraudulent schemes targeting financial institutions, infringement of intellectual property rights, and various other offenses. These transgressions carry substantial ramifications in terms of their impact on individuals, the economy, and the legal system in the online domain (Ayofe & Irwin, 2010).

Consequently, experts and scholars have made significant efforts to implement intelligent technologies, including artificial intelligence and other analytical tools, to address cyber-attacks preemptively (Kang & Kang, 2016; Rieck et al., 2011). The utilization of intelligent software and skilled programmers for identifying and categorizing harmful software, devising strategies to mitigate their effects, and establishing authentication protocols to verify the user's identity to the program, has been documented (AL-Maksousy, 2018). The objective of this study was to establish measures for identity verification and file protection, as well as to identify the perpetrators of cyber-attacks based on their modus operandi and attack patterns. To achieve this, a corpus of attack incident reports spanning the years 2012 to 2018 was compiled, and a team of five experts was trained to analyze these reports and discern the methods and techniques employed by the attackers. The study focused on using language processors and personal files to aid in identifying and tracking cyber criminals. Notably, a significant proportion of cyber threats have been acquired (Noor et al., 2019). This indicates that two types of risks are particularly prominent: those originating from the user and the server where data is stored (Davis, 2017).

Since addressing Cybersecurity risks is crucial in modern practice, numerous studies and models have been developed. Henrique's model was the first of its kind, and it analyzed Cybersecurity risks by considering the timing of data dissemination, data modification, and data loss or damage. E-commerce was shown to be more susceptible to cyber security threats than other sites, and the findings revealed that using the two models had significant positive effects (Henriques de Gusmo et al., 2018). The focus of Munk's research is understanding the security and governance methods given in the European area. Therefore, the Cybersecurity policies and governance models produced by the European Union and NATO may be comprehended by approaching the diagnosis from the dogmatic and mental governance viewpoint. The Copenhagen and Paris schools, each emphasizing a different facet of the security agenda, were utilized to diagnose tactics and forms of governance. Two case studies—on cyber security and cyber terrorism, respectively—were used to create the study's underlying analytic approach. The study's findings include the need for proactive governance and organizational practices that would significantly reduce cyber-attacks; the complexity of the contractual system; the existence of legislative gaps; the importance of various forms of government; the importance of transparency and accountability; and so on (Munk, 2015). After the Securities Commission issued instructions to disclose Cybersecurity risks, Lee conducted a study on the topic. The purpose of the study was to learn more about the factors that influence the declaration of Cybersecurity risks and the factors that have become recognized as indicators of the presence of these risks over time. Here, we discover that, unless disclosed, the correlation between Cybersecurity incidents and reported Cybersecurity risks become negligible. The study concludes that the decision of the Securities and Exchange Commission confirms the disclosure of security risks Cyber. However, corporations may feel pressured by the US Securities and Exchange Commission's disclosure rule to report Cybersecurity risks regardless of their severity (Li et al., 2018). More and more businesses are investing in better protecting and securing their data. It is essential to pay attention to employee behavior within the organization and how it relates to their performance, as well as cyber behaviors that are positive with organizational citizenship behaviors and potentially harmful cyber behaviors And related to negative business behaviors because employees within organizations continue to pose the greatest threat to Cybersecurity despite efforts to secure the information infrastructure. Cybersecurity behavior prediction and internal threat mitigation are included in this study's findings (Christine Dreibelbis, 2016). While considerable research has been done on the topic, it isn't easy to track down new information on how technologies have been used in the past. As a result, the authors of this research suggest using a fuzzy inference system (FIS) to spot cyber threats (Alali et al., 2018).

The safeguarding and preservation of cyberspace necessitate the prioritization of cybersecurity measures and law enforcement capabilities. The role of law in attaining Internet security objectives is pivotal, as it encompasses investigating a broad spectrum of cyber offenses, including but not limited to theft, fraud, child exploitation, and the apprehension and prosecution of the perpetrators. The ministries of interior and justice in various nations are tasked with prioritizing implementing criminal investigations and effective measures to impede and discourage cybercriminal activities. This involves prioritizing recruiting and training technical experts, devising standardized approaches, and exchanging best practices and tools related to large-scale electronic response. Professionals with expertise in criminal investigation and network security possess a comprehensive knowledge of the technologies utilized by malicious entities and the targeted vulnerabilities. These experts actively respond to and investigate cyber incidents (Borghard & Lonergan, 2017).

Meanwhile, Dawson has directed attention toward the escalating apprehensions regarding critical infrastructure, which is becoming increasingly susceptible to sophisticated electronic penetration, thereby giving rise to novel risks. The integration of information technology with physical infrastructure operations poses a heightened risk of large-scale or high-impact events that can cause damage or disrupt services critical to the economy and daily life of millions of individuals. Given the potential consequences of electronic events, it is essential to consider the associated risks. The augmentation of security and resilience in cyberspace has become a crucial aspect of national security for several nations. This has led to a concentrated effort on the part of stakeholders to examine the impact of education, technology, and politics on the domain of Cybersecurity. The research culminated in the creation of training environments designed to impart knowledge on actual Cybersecurity incidents and the establishment of a pervasive educational framework aimed at instructing individuals on Cybersecurity principles and Policies that promote secure usage of contemporary systems while also examining their impact on both national and global security (Dawson, 2017).

The task of safeguarding cyberspace is notably challenging owing to various factors, including the capacity of malicious agents to conduct operations from any location globally, the presence of interconnections between cyberspace and tangible systems, and the intricacy of mitigating vulnerabilities and ramifications within intricate information networks.

Cybersecurity risk of fintech firms

In recent years, there has been a marked improvement in the cooperation between conventional banks and fintech companies. Collaboration is being pursued to better service quality, agility, inventive thought, and digital infrastructure. It's controversial because it makes conventional banks more susceptible to cyberattacks from fintech companies, such as ransomware, data leaks, and breaches in data integrity. Cybersecurity risk in the financial technology industry is a new frontier in basic research requiring more investigation into its underlying dynamics. Cyber-breach by fintech businesses raises the amount of risk and fraud exposure for conventional banks (Ng & Kwok, 2017b). That's why fintech companies must comply with every country's data protection laws.

According to Lewis & Baker (2013), cybercrime has increased since fintech companies became widely available to consumers. They also note that because cyberattacks hit financial institutions in diverse ways, quantifying the monetary harm each one causes is challenging. Cybercrime, therefore, poses a threat to the credibility of financial organizations as well as to their bottom lines. Furthermore, Kopp et al. (2017) state that fintech companies lose clients, reputation, revenue, brand, equity value, and operational expenses due to cyber-breach. According to Fitch (2017), a rating organization specializing in the financial technology industry, cybercrime may significantly impact the financial performance of both fintech businesses and their partner firms. Experts in cyber risk say that the cybersecurity risk of fintech businesses is greater than that of conventional banks, and the International Organization of Securities Commission's Committee on Payments and Market Infrastructures (IOSC-CPMI) agrees. It suggests that partner companies have serious concerns about the long-term viability of fintech companies due to their cybersecurity practices.

However, the financial performance of alliance institutions might be weakened by the seriousness of fintech cybersecurity risk, which is particularly crucial for partner financial institutions and the capital market. Traditional banks see fintech relationships as essential to pursuing profit prospects, yet 71% of institutions have expressed worries about the cybersecurity dangers associated with fintech businesses (Digital News Asia, 2018). Data integrity risk, data leakage risk, and malware assaults are at the forefront of partner companies' cybersecurity worries and represent the most crucial inflection points for future growth. Financial technology companies often need more resources than their traditional counterparts. Therefore, fintech businesses cannot invest as much in cybersecurity due to limited funds, endangering the long-term viability of their partner banks.

Components of cybersecurity risk

In this research, we provide a comprehensive literature review of cybersecurity threats in fintech and their effects on the financial institutions with whom fintech firms engage. So far, we have argued that the economic viability of banks is negatively impacted by the increase in cybersecurity threats that followed their connection with fintech businesses. The susceptibility of the fintech cybersecurity system is also shown in the literature to affect company development and institutional performance. When compared to other financial organizations, banks are more vulnerable to cyberattacks. According to a consensus among practitioners and academic experts, economic epidemics caused by cyber incidents are positively correlated with the operational risk of banking institutions. Researchers in both the academic world and the financial technology industry are attempting to figure out what led to an increase in cyber events after fintech partnerships with banks and what can be done to lessen the impact of future attacks. We explore the background of fintech cybersecurity in the following publications.

A. *Malware Attacks*

Hackers worldwide often attack the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system. Financial organizations primarily use the SWIFT system to protect money transfer data. Recent malware assaults on the SWIFT system, as reported by India's second-largest bank, showed a significant degree of skill on the part of the hackers. Banks' heightened susceptibility to cyber assaults follows their embrace of fintech alliances. According to a new SWIFT survey study, cybercriminals use weaknesses in the fintech industry to target specific banks that have established a regulatory sandbox with fintech companies. According to a recent study, hackers are targeting more fintech companies and the companies with whom they work (Austin & Bloggs, 2018). McAfee predicts that by the end of 2020, the total number of malware assaults will have surpassed 700 million (McAfee, 2019). Due to fintech businesses' poor cybersecurity, conventional banks are now an easy target after the joint venture.

B. Data Leakages

Banks also confront the problem of data leaking in the realm of cybersecurity and malware assaults. Statistics leakage attacks have escalated since partnerships with financial companies were formed, according to published statistics (Ozili, 2018). User passwords and credit card details are examples of financial data. Financial technology companies consistently confront the challenge of data leaking. Since all fintech services are digital, they are more susceptible to data revealing than traditional banks (Yalcin, 2018). After financial institutions partner with fintech businesses, the banks must provide sensitive customer data to the fintech service providers. This leaves the fintech companies vulnerable to data breaches. One of the most exciting developments in the fintech environment is cloud computing, but proper cloud security measures are necessary to protect sensitive information. In sum, emerging research suggests that fintech companies face cybersecurity risks due to leaking sensitive financial data.

C. Data Integrity Risk

The use of mobile internet banking and other fintech services is crucial. A powerful, compact encryption technology is required for fintech services to function correctly on a mobile device. According to recent studies (Subashini & Kavitha, 2011), data reliability differs significantly amongst mobile money apps. Cloud computing is also a key enabler in the finance sector. Payment methods include digital wallets, gateways, and internet transactions. Cloud computing makes online payments simple and quick, but it may be difficult for fintech companies to keep customer financial data safe and private. The robust encryption process of such sensitive information necessitates high cloud security. The data collected by fintech apps also seems dubious and varies significantly across samples (Anton-Diaz, 2018). In a nutshell, the cybersecurity risk for financial companies comes from problems with data integrity.

Cybercrime and Cybersecurity

Cybercrime is criminal activities that target computer systems or internet networks, intending to unlawfully obtain data and financial resources and disseminate malicious software code. These actions are considered illegal within information and communication technology and are viewed as a modified form of traditional criminal behavior. (Shekar & Prabha, 2020; Aravazhi, 2020). According to Irfan et al. (2018), cybercrime refers to the deliberate actions of individuals who seek to compromise organizational networks through the theft of sensitive data and documents and the unauthorized access of bank accounts to transfer funds to their accounts. The investigation of such offenses necessitates the expertise of a cybercriminal with a comprehensive understanding of cybercrime, a fusion of criminology, psychology, sociology, computer science, and cybersecurity (Choi & Lee, 2018). The rapid development of cybercrime can be attributed to various factors, including the easy accessibility and study of cybercrime tools, methods, and media on the Internet. Additionally, the proliferation of technological advancements in processing speed, data processing and analysis, internet bandwidth, and other internet network activities have contributed to this phenomenon. Furthermore, the affordability of access to these resources has also played a role in the growth of cybercrime. Singh and Rajput (2019) assert that adding information to sources or servers is typically done manually.

Many cybercriminal activities are frequently employed by offenders, as documented by Cascavilla et al. (2021) and Maigida et al. (2019). One such activity is email spoofing, which involves the falsification of email headers. The email messages exhibited characteristics suggesting they originated from a trustworthy and credible sender. Typically, these modes are employed in spam or phishing endeavors. The recipient may perceive the email as originating from a credible entity and proceed to access its contents.

To "hack" is to access a computer network to obtain sensitive information illegally. The proliferation of viruses or other forms of malware is the dissemination of a set of computer instructions that may perform harmful actions. Viruses and other forms of malware interrupt the regular operation of the system's applications and introduce other performance issues. Email, instant messaging, file sharing, multimedia, the web, and other electronic media are potential vectors for distributing malicious software and viruses. Phishing refers to the fraudulent attempt to acquire sensitive information online, such as a user's password, credit card number, or login credentials. Emails and IMs sent to victims are spoofed to commit this cybercrime. The hacker will create a link that appears just like the legitimate website but will take the victim to a spoof page. Stalking is following or spying on a victim via electronic methods, such as the Internet or other forms of electronic communication. Harassment, hate speech, and cyberdefamation are all forms of cyberspace stalking. Repeatedly intimidating, threatening, or harassing someone via phone calls, texts, and other forms of communication is a hallmark of stalking. When someone's good name is sullied online, it's called "defamation," It can happen to anybody and any business. To defame someone is to make false remarks about them or their interaction with the intent to harm their reputation. Website scripting refers to a typical computer or system security flaw that cybercriminals may exploit in the form of code or script injection. Website attackers use script flaws to access targeted servers administratively (Aravazhi, 2020).

Cybersecurity, including preventative measures against cyberattacks and corrective steps after cybercrime, is essential for proactively countering this growing threat. Cybersecurity must meet several conditions, including availability, confidentiality, integrity, authentication, and accountability (Humayun et al., 2020; Rabii et al., 2020). The ability and availability of necessary information or data to be accessible at any moment by authorized parties are what we mean when discussing availability. To maintain confidentiality, information must be shielded from prying eyes. When data in a system has integrity, no unauthorized modifications may compromise that data. Analyzing a user to determine whether or not they are who they claim to be is called authentication. Responsibility, willingness, openness, and responsiveness are all aspects of accountability that users must take on as part of their usage of the system (Singh & Rajput, 2019).

Cybercrime on Fintech

Cybercrime that commonly occurs in information and communication technology can also attack fintech. The effects of cybercrime acts are disguised via the process of cyberlaundering, which entails many steps of conversion (placement), stacking (layering), and integration (Wibawa, 2017). Criminals often employ cryptocurrencies for cyberlaundering (Mabunda, 2018). Legalizing illicit funds is an effective strategy for combating cyber-money laundering (Karlov, 2018).

Fintech attacks are a broad category that includes many different kinds of cybercrime. Hackers often access sensitive information by bypassing multi-factor authentication or application connection protection. A Trojan horse for mobile banks that breaks into the financial system by targeting its encryption algorithm. Ransomware is malicious software that locks users' files and requests payment to unlock them. Magecarting is a cybercrime that aims to steal money using online shopping carts (Nikkel, 2020). The growth of technology and the acceleration of networks through time provide additional hazards associated with cybercrime. To eliminate new dangers, such as those posed by cybercrime, fintech development represents an evolution of the profession that requires both technological and ethical capabilities (Ng & Kwok, 2017).

Cybersecurity compliance in the financial industry is affected by hacking, phishing, and malware (Kwarto & Angsito, 2018). Most personal information and credit card data are kept and processed through e-commerce and online payment systems, making them prime targets for cybercriminals (Aravazhi, 2020). Users' inability to foresee cybercrime reduces their confidence in e-commerce (Batmetan et al., 2018). Other research suggests that misalignment with rules and inadequate consumer protection against cybercrime have slowed the growth of e-commerce. Both government officials and company owners agree that stringent measures must be implemented to protect against cybercrime and that law enforcement agencies must be vigilant to new trends in this area (Fahlevi et al., 2019). Model to Encounter Cyber Assaults (MECA) is one approach to cybersecurity that may be used to defend against cybercrime assaults on fintech (Cyriac & Sadath, 2019).

Traditional digital forensic techniques are insufficient for detecting and investigating cybercrime in fintech organizations. Due to the dynamic nature of data interchange in public server storage spaces, cybercrime using public clouds, often employed by fintech organizations, necessitates high-level digital forensic investigations (Baror & Venter, 2019). Public servers cannot be frozen as they are in conventional digital forensics. The cybersecurity infrastructure of a financial startup must be properly planned from the beginning. Data recovery in the case of cybercrime also requires dependable detection and investigation tools to complement the cybersecurity measures that have been put in place.

Methodology:

The present investigation employs a method of systematic literature review accompanied by research inquiries. What are the challenges of cybercrime that the fintech industry encounters? What is the fintech industry's approach toward cybersecurity in predicting and mitigating cybercrime risks? This paper aims to present a comprehensive account of the evolution of the primary obstacles encountered by the financial technology (fintech) industry in the shape of cybercrimes and the proactive measures implemented by fintech to mitigate these criminal activities. The present study will restrict its search for published articles from 2016 to 2021 in light of the extensive discourse surrounding fintech as a novel financial innovation over the past half-decade. The present study identifies, evaluates, and interprets research findings about a specific research topic to answer the research questions at hand (Jesson et al., 2011).

The search for relevant articles commenced on the Google Scholar portal. Subsequently, it extended to esteemed online databases, including ScienceDirect, Elsevier, ACM Digital Library, ABI/Inform Complete, Academic Search Complete, IEEE Xplore, SSRN, Springer, Emerald, Taylor & Francis, World Scientific, and IGI Global. The search query employed was "cybercrime cybersecurity fintech." However, the search did not yield satisfactory results, prompting the need for further exploration. Additionally, a protocol review was conducted by formulating research inquiries, which involved the classification of keywords based on population strategies, interventions, comparisons, results, and contextual factors of the acquired articles.

The inclusion and exclusion criteria were determined based on the research questions to avoid any subjective influence from the researchers during the article selection process. Moreover, Mendeley software is utilized to organize the selected articles effectively. The methodology employed to extract and synthesize data involves using thematic analysis and meta-analysis, as posited by Bown and Sutton (2010).

The research process comprises three main stages: planning, implementing, and reporting. These stages are further subdivided into eight distinct steps, which include formulating the research problem, developing and validating the review protocol, conducting a comprehensive literature search, screening the relevant literature, evaluating the quality of the literature, extracting data, analyzing and synthesizing the data, and finally, reporting the research findings. The works of

Uman (2011) and Xiao and Watson (2019) are referenced in the following text. Please refer to Figure 1 for further details:

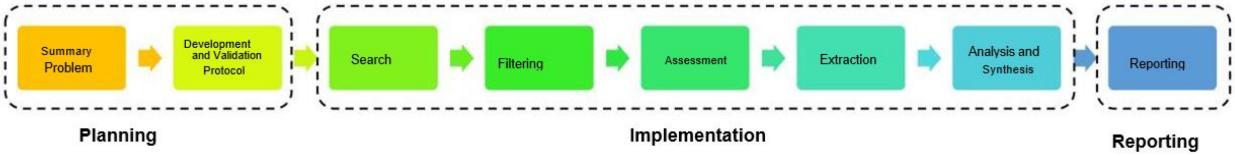

Figure 1. Systematic Literature Review Method

The procedure of scrutinizing, refining, and evaluating articles to ascertain their alignment with the research objectives is executed by examining the themes expounded in each article. The selected papers are subjected to extraction and analysis, guided by research inquiries, to comprehensively understand cybercrime in the fintech industry and the corresponding cybersecurity measures to mitigate this threat.

Results and discussion:

A. Article Selection

A search query using "cybercrime cybersecurity fintech" on Google Scholar yielded 1,320 results. A fine selection of articles was then conducted from these results, utilizing reputable online databases such as Science Direct, Elsevier, ACM Digital Library, ABI/ Inform Complete, Academic Search Complete, IEEE Xplore, SSRN, Springer, Emerald, Taylor & Francis, World Scientific, and IGI Global. The findings of the article selection indicate that 35 articles from diverse online databases align with the subject matter of cybercrime and cybersecurity in fintech. The year of publication, research methodology, and sub-topics are also consistent with this theme.

B. Article Classification

The data in Table 1 indicate a noticeable rise in published articles on cybercrime and cybersecurity in fintech from 2017 to 2021. This trend reflects an overall increase in article publications during this period. The distribution of articles published in online databases with comparable topics is diverse, with a significant proportion of articles published on SSRN, as indicated in Table 2.

Table 1. Classification of Articles by Year of Publication 2017

2017	2
2018	3
2019	5
2020	9
2021	12
Amount	**31**

Table 2. Classification of Articles Based on Online Sources

Online Resources	
Elsevier	5
Emerald	3
IEEE Xplore	3
IGI Global	2
Springer	5
SSRN	4
Taylor & Francis	5
World Scientific	4
Amount	**31**

Classification of articles based on topics that discuss cybercrime threats in fintech and anticipate cybersecurity to overcome it as shown in Table 3 below:

Table 3. Classification of Articles Based on Research Types

Topic	Publishers
Fintech's Anticipation of Cybercrime and Threats	(Adeyoju, 2019; Boitan & Marchewka Bartkowiak, 2021; Corbet & Gurdgiev, 2017; Cyriac & Sadath, 2019; Faya & Ogbuefi, 2019; Huang & Madnick, 2020; Kaur et al., 2021; Malladi et al . , 2021; Mehrotra & Menon, 2021; Milian et al., 2019; Namchoochai et al., 2020; Ng & Kwok, 2017)
Opinions on the effectiveness of fintech in preventing and combating cybercrime	(Asante-Offei & Yaokumah, 2021; Ogbanufe & Kim, 2018)
Cybercrime's effects, root causes, methods, and forensic analysis in the financial technology sector	(Al-Harrasi et al., 2021; Nikkel, 2020; Vedral, 2021)
Securing financial technology infrastructure requires regulation to foresee cybercrime.	(Amstad, 2019; Bagby & Packin, 2020; Bagby & Reitter, 2019; Laidlaw, 2021; Ojo & Nwaokike, 2019; Teigland et al., 2018)
Methodologies and infrastructure for cyber security risk assessment	(Bouveret, 2019; Chari, 2020; Creado & Ramteke, 2020; Lubin, 2021; Najaf et al., 2021; Noor et al., 2019; Santucci, 2018; Singh & Rajput, 2019; Uddin et al., 2020; Yousef & Hafeez-Baig, 2021)

Cybercrime problem in Fintech

Cybercrime is the biggest threat to the financial technology industry, and it is evolving in response to advances in ICT (Al-Harrasi et al., 2021; Vedral, 2021). Inadequate cybercrime control regulations on fintech, the loss, alteration, or disclosure of data and information, and the theft of intellectual property all contribute to a loss of public confidence in the sector (Adeyoju, 2019; Boitan & Marchewka- Bartkowiak, 2021; Corbet & Gurdgiev, 2017; Cyriac & Sadath, 2019; Faya & Ogbuefi, 2019; Huang The following is a description of these challenges:

- Regulation: Since rules are typically slow to adapt to information and communication technology advancements, fintech faces regulatory and operational challenges. However, some countries still do not support fintech in their countries because they believe it has the potential to undermine conventional financial stability. This is a global challenge that involves other countries around the world. The internationally applicable legislation is needed due to the worldwide influence of fintech (Laidlaw, 2021). Regulation of cybercrime in the financial technology industry is still, in some circumstances, applying cybercrime legislation that is generic, leading to the less-than-optimal application of these regulations. Regulation must also be fluid to keep up with the rapid changes in the financial technology industry. (Bagby & Packin, 2020; Bagby & Reitter, 2019; Faya & Ogbuefi, 2019; Ojo & Nwaokike, 2019; Teigland et al., 2018).

- Data and Information: Because cybercrime threats are always more advanced than fintech's cybersecurity, fintech's cybersecurity needs to be updated to deal with all types of cybercrime threats, which undergo rapid development over time and thus increase the risk of data loss, modification, or leakage. (Akhta et al., 2021).
- Intellectual Property Theft: The proliferation of creative technology has led to the theft of intellectual property rights, including patents, copyrights, and trade secrets. These thefts of intellectual property rights started as cybercrime assaults on victims in the financial technology industry. (Al-Harrasi et al., 2021).
- Public Trust: The public's faith in financial technology has suffered as a direct result of the concerns that have been outlined above. If data or information were to leak due to cybercrime assaults against fintech companies, it would be difficult to regain the public's confidence. (Asante- Offei & Yaokumah, 2021; Ogbanufe & Kim, 2018).

Cybersecurity Anticipation in Fintech

- Fintech is especially susceptible to cybercrime because of its fast growth; as a result, the industry must establish certain safeguards to prevent data breaches and financial losses. Implementing solid cybersecurity measures from the outset of a fintech business's inception is the most excellent way to safeguard its data and information. Some preventative measures against cybercrime aimed at the financial technology sector include:

- **Proactive Action:**

Fintech and the government as policymakers in implementing regulations should take the following proactive steps to combat cybercrime: a. Create a comprehensive cybersecurity framework that incorporates prevention, detection, monitoring, information sharing, financial and technological literacy, and recovery plans (Chang et al., 2018; Faya & Ogbuefi, 2019).

1. To deal with the cybercrime threats posed by global data usage, we need a b: comprehensive data security and information access architecture.
2. Legislative and regulatory monitoring to make sure fintech is using certain practices.
3. They are educating consumers of fintech to raise their consciousness about the significance of cybersecurity.

- **Fintech:**

Regulations To mitigate the risks of operating in a constantly evolving industry, fintech businesses need adaptable rules and regulations. According to Fahlevi et al. (2019), legislation should support innovation and creativity throughout comprehensive and systematic fintech development. Ensure that business actors, consumers, and supervisory authorities have a clear foundation on how to behave and act in compliance with relevant legislation; the regulations also give legal certainty for any cybercrime activities that are harmful to fintech. The growth of financial technology must be supported entirely by rules, which must also adhere to the values of upholding national dignity. (Amstad, 2019; Bagby & Packin, 2020; Bagby & Reitter, 2019; Laidlaw, 2021; Ojo & Nwaokike, 2019; Teigland et al . , 2018).

- **Technical Steps in Implementing Cybersecurity in Fintech:**

Several technical measures can be taken to combat cybercrime in the fintech industry, including the development of trustworthy cybersecurity frameworks and procedures (Creado & Ramteke, 2020; Najaf et al., 2021; Singh & Rajput, 2019; Uddin et al., 2020), the mapping of risks that are susceptible to cybercrime (Bouveret, 2019; Chari, 2020; Lubin, 2021; Santucci, 2018 Appropriate cybersecurity measures, including the following steps, are required due to the possibility of cybercrime that exploits cybersecurity holes in fintech (Aravazhi, 2020):

1. Protect and monitor all network-connected devices using a multi-layered security architecture, including wireless access points, and restrict user access as needed.
2. Manage and restrict internal user access to files or data to that which is strictly necessary to complete assigned tasks.
3. Protect and safeguard all intended system users and administrators.
4. Verification of harmful software like viruses, trojans, malware, etc. Regularly scanning for spyware, adware, bots (software robots), and other dangerous e. applications using an antispyware tool is a must.
5. Educate users to be cautious and secure while using online services.

Conclusion:

Due to the fast expansion of information and communication technology, cybercrime is a requirement that will continue to exist, which is why dependable and efficient cybersecurity is required to cope with it. Theft of data, information, and intellectual property, which can potentially damage the image of the fintech industry, are some of the issues posed by cybercrime. To reduce the impact of the threat posed by cybercrime, it is necessary to implement cybersecurity measures, such as taking preventative measures, tightening rules, and developing a cybersecurity framework or system that is dependable, effective, and efficient.

1. References:

Adeyoju, A. (2019). Cybercrime and Cybersecurity: FinTech's Greatest Challenges. SSRN Electronic Journal, 1–5. https://doi.org/10.2139/ssrn.3486277.

Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. Computers and Security, 74, 323–339. https://doi.org/10.1016/j.cose.2017.09.011

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2021). Towards Protecting Organisations' Data by Preventing Data Theft by Malicious Insiders. International Journal of Organizational Analysis, 20–21. https:// doi.org/10.1108/IJOA-01-2021-2598.

AL-Maksousy, H. H. L. (2018). Applying Machine Learning to Advance Cyber Security: Network Based Intrusion Detection Systems. Doctor of Philosophy (PhD), dissertation, Computer Science, Old Dominion University, DOI: 10.25777/8w8w- sa92.

Amstad, M. (2019). Regulating Fintech: Objectives, Principles, and Practices. Asian Development Bank Institute Working Paper Series 1016, 1–13. https://doi.org/10.2139/ssrn.3541003.

Anton-Diaz, P. (2018). New Data Security Study of Fintech Apps Highlights Vulnerabilities | Center for Financial Inclusion. Retrieved April 4, 2020, from New Data Security Study of Fintech Apps Highlights Vulnerabilities," Center for Financial Inclusion, 5 September 2018 website: https://www.centerforfinancialinclusion.org/new-data-security-study-of-fintech- apps-highlights-vulnerabilities

Austin, J., & Bloggs, J. (2018). Big Data Outsourcing and Identity Verification in Fintech Credit Assessment: A Case Study of a Microloans Platform in China. Australasian Conference on Information Systems.

Ayofe, A. N., & Irwin, B. (2010). Cyber Security: Challenges And The Way Forward. Georgian Electronic Scientific journal, Computer Science & Telecommunications, 29(6). Https://Www.Researchgate.Net/Publication/265121167_Cyber_Securıty_Challenges_And_The_Way_Forward.

Bagby, J. W., & Packin, N. G. (2020). RegTech and Predictive Lawmaking: Closing the RegLag between Prospective Regulated Activity and Regulation. Michigan Business & Entrepreneurial Review, 10(2), 127–177. https://doi.org/10.36639/mbelr.10.2.regtech.

Bagby, J. W., & Reitter, D. (2019). Anticipatory FinTech Regulation: On Deploying Big Data Analytics to Predict the Direction, Impact and Control of Financial Technology. SSRN Electronic Journal, 1–59. https://doi.org/10.2139/ ssrn.3456844.

Boitan, I. A., & Marchewka-Bartkowiak, K. (2021). Fostering Innovation and Competitiveness with Fintech, RegTech, and SupTech. IGI Global. USA: Hershey PA.

Borghard, E. D., & Lonergan, S. W. (2017). The Logic of Coercion in Cyberspace. Security Studies, 26(3), 452–481. https://doi.org/10.1080/09636412.2017.1306396

Bouveret, A. (2019). Cyber Risk for the Financial Services Sector. Journal of Financial Transformation, 49, 78–85.

Bown, M. J., & Sutton, A. J. (2010). Quality Control in Systematic Reviews and Meta-analyses. European Journal of Vascular & Endovascular Surgery, 40(5), 669–677. https://doi.org/10.1016/j.ejvs.2010.07.011

Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen Co-Production of Cyber Security: Self-Help, Vigilantes, and Cybercrime. Regulation and Governance, 12(1), 101– 114. https://doi.org/10.1111/rego.12125.

Chari, K. (2020). Fraud Risk in Digitized Fintech Ecosystem: Troubling Trends, Issues and 1–8. Approaches Mitigateto Risk. SSRN Electronic https://doi.org/10.2139/ssrn.3680456

Christine Dreibelbis, R. (2016). It’ s More Than Just Changing Your Password: Exploring the Nature and Antecedents of Cyber- Security Behaviors, University of South Florida. http://scholarcommons.usf.edu/etdhttp://scholarcommons.usf.edu/etd/6083

Corbet, S., & Gurdgiev, C. (2017). Financial Digital Disruptors and Cyber-Security Risks: Paired and Systemic. Forthcoming in Journal of Terrorism & Cyber Insurance, 1(2), 1–20. https://doi.org/10.2139/ssrn.2892842.

Creado, Y., & Ramteke, V. (2020). Active Cyber Defence Strategies and Techniques for Banks and Financial Institutions. Journal of Financial Crime, 27(3), 771–780. https://doi.org/10.1108/JFC-01-2020-0008.

Cyriac, N. T., & Sadath, L. (2019). Is Cyber Security Enough-A Study on Big Data Security Breaches in Financial Institutions. 2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019, 380–385. https://doi.org/10.1109/ISCON47742.2019.9036294

Davis, J. J. (2017). Machine Learning and Feature Engineering for Computer Network Security. Thesis. https://eprints.qut.edu.au/106914/1/Jonathan_Davis_Thesis.pdf

Dawson, M. (2017). Hyper-connectivity : Intricacies of national and international cyber securities Hyper-connectivity : Intricacies of national and international cyber securities . London Metropolitan University Maurice Dawson Submitted in partial fulfillment of the award of Doctor of Philosophy by Prior. January. https://www.researchgate.net/publication/314230510_Hyper-connectivity_Intricacies_of_national_and_international_cyber_securities

Digital News Asia. (2018). Cyber-security the biggest barrier to fintech and banking sector partnerships in Asia. Digital News Asia. Retrieved from: https://www.digitalnewsasia.com/digital-economy/cyber-security-biggest-barrier-fintech-and-banking-sector-partnerships-asia

Faaeq, M. K., Thabit, T. H., & Harjan, S. A. (2015). Technology Innovation Usage in Public Services Among Employees in Republic of Iraq. In 7th International Conference on Information Technology, Al-Zaytoonah University of Jordan, Amman, Jordan.

Faya, M., & Ogbuefi, N. (2019). Cybersecurity in the Age of FinTech and Digital Business. Cyber Secure Nigeria 2019 Conference, 6–10. https://ssrn.com/abstract=3606866

Firmansyah, E. A., & Anwar, M. (2019). Islamic Financial Technology (Fintech): Its Challenges and Prospect. Atlantis Press is a professional publisher of scientific. 216(Assdg 2018), 52–58. https://doi.org/10.2991/assdg-18.2019.5

Fitch. (2017). [Press Release] Fitch: Cyber Risk Is a Growing Threat to Financial Institutions. Retrieved from https://www.fitchratings.com/site/pr/1022468

Harjan, Sinan Abdullah, Teng, M., Shah, S. S. H., & Mohammed, J. H. (2019). Political Connections and Cost of Debt Financing: Empirical Evidence from China. International Journal of Economics and Financial Issues, 9(1), 212. DOI: https://doi.org/10.32479/ijefi.7561.

Hayder M. Kareem, A.-D., Zhang, J., Abdulreza, M. S., Harjan, S. A., & Shah, S. S. H. (2019). the Role of Financial Inclusion and Competitive Advantage: Evidence From Iraqi Islamic Banks. International Journal of Economics and Financial Issues, 9(3), 193–199. https://doi.org/10.32479/ijefi.8080

Henriques de Gusmão, A. P., Mendonça Silva, M., Poleto, T., Camara e Silva, L., & Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. International Journal of Information Management, 43(January), 248–260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008

Huang, K., & Madnick, S. (2020). Cyber Securing Cross-border Financial Services: Calling for a Financial Cybersecurity Action Task Force. Working Paper CISL# 2020-08, 1–10. https://doi.org/10.2139/ssrn.3570140.

Jesson, J. K., Matheson, L., & Lacey, F. M. (2011). Doing Your Literature Review: Traditional and Systematic Techniques. SAGE Publications. California: Thousand Oaks.

Kang, M. J., & Kang, J. W. (2016). Intrusion detection system using deep neural network for in-vehicle network security. PLoS ONE, 11(6), 1–17. . https://doi.org/10.1371/journal.pone.0155781

Kareem, H. M., Duhaidahawi, A., Zhang, J., Abdulreza, M. S., & Sebai, M. (2020). An efficient model for financial risks assessment based on artificial neural networks; Evidence from Iraqi Banks (2004-2017), Journal of Southwest Jiaotong University. https://doi.org/10.35741/issn.0258-2724.55.3.8. 55(3).

Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends. In Springer. Switzerland AG. http://www.springer.com/series/16360.

Kim, Y., Park, Y.-J., Choi, J., & Yeon, J. (2015). An Empirical Study on the Adoption of "Fintech" Service: Focused on Mobile Payment Services. December, Advanced Science and Technology Letters, 114(26), 2015, 136–140, https://doi.org/10.14257/astl.2015.114.26

Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). Cyber risk, market failures, and financial stability. International Monetary Fund

Laidlaw, E. (2021). Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows. SSRN Electronic Journal, 1–81. https://doi.org/10.2139/ssrn.3790936

Leong, K. (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. https://doi.org/10.18178/ijimt.2018.9.2.791

Lewis, J., & Baker, S. (2013). The economic impact of cybercrime and cyber espionage. McAfee.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. International Journal of Accounting Information Systems, 30(June), 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

Lin, T. C. W. (2015). Infinite Financial Intermediation. Wake Forest Law Review, 50(643), Temple University Legal Studies Research Paper No. https://ssrn.com/abstract=2711379

Magnuson, W. (2018). Regulating fintech. Vanderbilt Law Review, Available at: https://scholarship.law.vanderbilt.edu/vlr/vol71/iss4/271 (4), 1167–1226.

Malladi, C. M., Soni, R. K., & Srinivasan, S. (2021). Digital Financial Inclusion: Next Frontiers— Challenges and Opportunities. CSI Transactions on ICT, 9(2), 127–134. https://doi.org/10.1007/s40012-021-00328-5.

McAfee. (2020). Study: $100 Billion Lost Annually to Cyber Attacks | 2013-07-22 | Security Magazine. Retrieved from https://www.securitymagazine.com/articles/84549-study-100-billion-lost-annually-to-cyber-attacks

Mehrotra, A., & Menon, S. (2021). Second Round of FinTech - Trends and Challenges. 2nd International Conference on Computation, Automation and Knowledge Management, ICCAKM 2021, 243–248. https://doi.org/10.1109/ICCAKM50778.2021.9357759.

Micu, A. (2016). Financial Technology (FinTech) and its Implementation on the Romanian Non-Banking Capital Market. SEA – Practical Application of Science, IV(11), 379–384.

Milian, E. Z., Spinola, M. de M., & Carvalho, M. M. d. (2019). Fintechs: A Literature Review and Research Agenda. Electronic Commerce Research and Applications, 34(100833), 1– 21. https://doi.org/10.1016/j.elerap.2019.100833.

Munk, T. H. (2015). Cyber-Security in the European Region: Anticipatory Governance and Practices. PQDT- The University of Manchester (United Kingdom) & Ireland, 287. . https://search.proquest.com/docview/1784057545?accountid=9645

Najaf, K., Mostafiz, M. I., & Najaf, R. (2021). Fintech Firms and Banks Sustainability: Why Cybersecurity Risk Matters? International Journal of Financial Engineering, 08(02), 2150019. https://doi.org/10.1142/S2424786321500195.

Namchoochai, R., Kiattisin, S., Darakorn Na Ayuthaya, S., & Arunthari, S. (2020). Elimination of FinTech Risks to Achieve Sustainable Quality Improvement. Wireless Personal Communications, 115, 3199–3214. https://doi.org/10.1007/s11277-020-07201-9.

Ng, A. W., & Kwok, B. K. B. (2017a). 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. https://doi.org/10.1108/JFRC-01-2017-0013

Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. Forensic Science International: Digital Investigation, xxxx, 200908. https://doi.org/10.1016/j.fsidi.2020.200908

Nikkel, B. (2020). Fintech Forensics: Criminal Investigation and Digital Evidence in Financial Technologies. Forensic Science International: Digital Investigation, 33, 200908. https://doi.org/10.1016/j.fsidi.2020.200908.

Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Generation Computer Systems, 96, 227–242. https://doi.org/10.1016/j.future.2019.02.013

Noor, U., Anwar, Z., Amjad, T., & Choo, K. K. R. (2019). A Machine Learning-based FinTech Cyber Threat Attribution Framework Using High-level Indicators of Compromise. Future Generation Computer Systems, 96, 227–242. https://doi.org/10.1016/j.future.2019.02.013.

Ogbanufe, O., & Kim, D. J. (2018). Comparing Fingerprint-based Biometrics Authentication Versus Traditional Authentication Methods for e-Payment. Decision Support Systems, 106, 1–14. https://doi.org/10.1016/j.dss.2017.11.003.

Ojo, O., & Nwaokike, U. (2019). Disruptive Technology and the Fintech Industry in Nigeria: Imperatives for Legal and Policy Responses. Gravitas Review of Business and Property Law, 9(3), 1–19. https://doi.org/10.2139/ssrn.3306164

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. Borsa Istanbul Review, 18(4), 329–340.

Peters, G. W., Panayi, E., & Chapelle, A. (2015). Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. SSRN Electronic Journal, 3(3). https://doi.org/10.2139/ssrn.2646618

Philippon, T. (2016). The Fintech Opportunity. National Bureau Of Economic Research, 8(3), 6–10. http://www.nber.org/papers/w22476

Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Automatic analysis of malware behavior using machine learning. Journal of Computer Security, 19(4), 639–668. https://doi.org/10.3233/JCS-2010-0410

Sadłakowski, D., & Sobieraj, A. (2017). The development of the FinTech industry in the Visegrad group countries. World Scientific News, 85, 20-28. https://doi.WSN% 2085%20 (2017)%2020-28.pdf

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). https://doi.10.1080/ 09636412.2017.1306396

Schueffel, P. mname. (2018). Taming the Beast: A Scientific Definition of Fintech. SSRN Electronic Journal, April. https://doi.org/10.2139/ssrn.3097312

Shah, S. S. H., Xinping, X., Khan, M. A., & Harjan, S. A. (2018). Investor and manager overconfidence bias and firm value: Micro-level evidence from the Pakistan equity market. International Journal of Economics and Financial Issues, 8(5), 190.

Sharma, N. (2019). Banking and FinTech (Financial Technology) Embraced with IoT Device. 197–211. Advances in Intelligent Systems and Computing, 1042, https://doi.org/10.1007/978-981-32-9949-8_15.

Singh, P., & Rajput, R. S. (2019). Cybersecurity Analysis in the Context of Digital Wallets International Journal of Advanced Studies of Scientific Research, 4(3), 522–525.

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. Politics and Governance, 6(2), 1–4. https://doi.org/10.17645/pag.v6i2.1569

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11.

Teigland, R., Siri, S., Larsson, A., & Puertas, A. M. (2018). The Rise and Development of FinTech: Accounts of Disruption from Sweden and Beyond. Routledge. New York: Third Avenue.

Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and Financial System Vulnerability: A Synthesis of Literature. In Risk Management (Vol. 22, Issue 4). Palgrave Macmillan UK. https://doi.org/10.1057/s41283-020-00063-2.

Uman, L. S. (2011). Systematic Reviews and Meta-Analyses. Journal of the Canadian Academy of Child Adolescent. Psychiatry, 57–59. https://wawnwd.ncbi.nlm.nih.gov/pmc/articles/PMC3024725/. 20(1),

Vimal, M. (2019). Cybersecurity and Fintech at a Crossroads. Retrieved from: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/cybersecurity-and-fintech-at-a-crossroads

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers and Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

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. https://doi.org/10.1016/j.comnet.2015.02.026

Whitley, E. A. (2009). Informational privacy, consent and the “control” of personal data. Information Security Technical Report, 14(3), 154–159. https://doi.org/ 10.1016/j.istr .2009.10.001

Wulan, V. R. (2017). Financial technology (fintech) a new transaction in future. Journal Electrical Engineering and Computer Sciences, 2(1), 177–182. Corpus ID: 170052661.

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. Journal of Planning Education 1–20. https://doi.org/10.1177/0a7n3d94R5e6sXe1a7rc7h2,3971.39(1),

Yalcin, F. G. (2018). Finans Sektörü 300 Kat Daha Fazla Saldırıya Uğruyor | Fintechtime. Retrieved from http://fintechtime.com/tr/2018/10/finans-sektoru-300-kat-daha-fazla-saldiriya-ugruyor/

Yusif, S., & Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. Journal of Applied Security Research, 16(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995.