Review

Cybersecurity & Data Privacy in Fintech

Rajath Karangara * and Otilia Manta *

Posted Date: 11 April 2024

doi: 10.20944/preprints202401.2194.v2

Keywords: Fintech; Cybersecurity; Data Privacy; Information Security; Regulatory Compliance

Review

Cybersecurity & Data Privacy in Fintech

Rajath Karangara [1,*] and Otilia Manta [2,3]

[1] American Express, Florida, United States of America (R.K); email: rajathk2003@yahoo.co.in
[2] Romanian Academy, Victor Slăvescu" Centre for Financial and Monetary Research, Bucharest, 050711, Romania (O.M.).
[3] Romanian American University, Bucharest, 012101, Romania (O.M.); email: otilia.manta@icfm.ro
* Correspondence: rajathk2003@yahoo.co.in

Abstract: With the fintech industry growing at an unprecedented rate, it is critical to protect cybersecurity and ensure data privacy. The research presented here thoroughly examines the challenges faced by financial technology companies, highlighting the growing risks posed by malware, phishing, and network vulnerabilities. As essential components of a proactive defense plan, the report promotes strong cybersecurity measures like frequent security assessments, encryption, and stringent access controls. The findings highlight how important it is for fintech companies to give cybersecurity equal importance with open and honest data privacy policies to win customers. To protect the industry from cybersecurity risks regulatory compliance, intrusion detection systems, and collaborative information sharing are considered essential components. The article advises businesses to include cybersecurity and data privacy into their core business operations and customer relations, highlighting these factors' critical role in sustaining success in the rapidly evolving fintech industry.

Keywords: fintech; cybersecurity; data privacy; Information Security; regulatory compliance

1. Introduction

The rapid expansion of the fintech sector has revolutionized the landscape of digital financial services, offering consumers unprecedented convenience and accessibility (Gai et al., 2018; Claessens & Cornelli, 2018). However, this remarkable growth has also brought forth a plethora of cybersecurity and data privacy challenges that warrant thorough investigation (Yong Xu et al, 2024). Given that fintech companies handle sensitive financial data, they have become prime targets for cybercriminals seeking to exploit vulnerabilities in their systems (Woods A., 2022). Consequently, the imperative to safeguard confidential financial information has become increasingly paramount (Hassan, 2020; Yermack, 2017).

As fintech continues to disrupt traditional financial services, it is crucial to critically assess the implications of this transformation on cybersecurity and data privacy (Milian E.Z. et al, 2019); Cocco et al., 2017). The growing reliance on digital platforms and online transactions underscores the need for robust security measures and regulatory frameworks to protect against cyber threats (Sangwan, V. et al, 2020; Arner et al., 2016). Moreover, the evolving nature of fintech innovations, such as blockchain technology and AI-driven solutions, introduces new complexities and vulnerabilities that must be addressed (Catalini & Gans, 2016).

This research seeks to fill gaps in existing literature by providing a comprehensive analysis of the intricate intersection between cybersecurity, data privacy, and fintech (Barberis N., 2018). By examining the challenges and opportunities inherent in this convergence, it aims to offer insights and recommendations for policymakers, regulators, industry practitioners, and researchers alike (Miroshnychenko I. et al, 2017; Cumming et al., 2018). Ultimately, this study contributes to the ongoing dialogue on enhancing security and trust in the fintech ecosystem, fostering innovation while safeguarding the integrity of financial systems (Chen et al., 2012; Cha D.et al., 2019).

 doi:10.20944/preprints202401.2194.v2

Objectives: the overarching objectives of this study are multifaceted, aimed at providing a comprehensive analysis of cybersecurity within the fintech industry:

- ✓ To meticulously identify and analyse the myriad cybersecurity threats confronting fintech companies, encompassing both traditional and emerging risks.
- ✓ To delve into the intricate regulatory landscape governing the fintech sector, discerning its nuances and assessing its profound impact on cybersecurity practices.
- ✓ To critically evaluate the efficacy of existing cybersecurity measures implemented by fintech organizations, gauging their effectiveness in mitigating threats and safeguarding sensitive financial data.
- ✓ To formulate practical and actionable recommendations tailored to bolster cybersecurity and enhance data privacy standards within the dynamic fintech ecosystem.

***Significance*:** the significance of this study resonates across various dimensions, underscoring its pivotal role in shaping discourse and fostering advancements within the fintech cybersecurity domain:

- ✓ By shedding light on the evolving cybersecurity risks within the financial industry, this study illuminates the shifting threat landscape and underscores the imperative for proactive risk management strategies.
- ✓ Through an in-depth exploration of the regulatory framework, this research elucidates the intricate interplay between regulatory mandates and cybersecurity practices, offering valuable insights into compliance requirements and governance considerations for fintech entities.
- ✓ By offering actionable suggestions for enhancing cybersecurity posture, this study empowers fintech companies to fortify their defences and proactively mitigate cyber threats, thereby bolstering resilience and trust in the digital financial ecosystem.
- ✓ As a scholarly contribution, this research enriches the existing body of knowledge on the convergence of fintech, cybersecurity, and data privacy, advancing understanding and informing future research endeavours in this burgeoning field.

Research Questions: to address the objectives, the study will seek answers to the following research inquiries:

- ✓ What are the predominant challenges and vulnerabilities confronting fintech organizations in terms of cybersecurity, and how have these threats evolved over time?
- ✓ How does the regulatory landscape, including compliance requirements and regulatory frameworks, influence cybersecurity practices and risk management strategies within the fintech sector?
- ✓ To what extent are the existing cybersecurity measures adopted by fintech companies effective in mitigating cyber risks and safeguarding sensitive financial information?

What actionable recommendations can be proposed to enhance data privacy and cybersecurity resilience within the fintech industry, considering the evolving threat landscape and regulatory dynamics? This study investigates the relationship between data privacy, cybersecurity, and fintech. The research employed a literature review approach to gather relevant information and insights from various academic and professional sources related to cybersecurity and data privacy in the fintech industry. We have gathered relevant academic literature and industry reports from credible sources.

This research delves into the intricate relationship between data privacy, cybersecurity, and the burgeoning field of financial technology (fintech). To achieve a comprehensive understanding, the study adopts a literature review approach, synthesizing insights from diverse academic and professional sources pertaining to cybersecurity and data privacy in the fintech landscape.

The methodology employed involved a meticulous search strategy, meticulously curated to gather pertinent academic literature and industry reports from reputable sources. Utilizing keywords such as "fintech," "cybersecurity," "data privacy," "cyber threats," "regulatory compliance," and "artificial intelligence," the search was tailored to capture the latest developments within the past five years, with a preference for peer-reviewed journals to ensure scholarly rigor and credibility.

In adhering to inclusion criteria, emphasis was placed on selecting studies that directly addressed the nexus of cybersecurity and data privacy within the fintech sector, published in

 doi:10.20944/preprints202401.2194.v2

esteemed and credible outlets. Conversely, exclusion criteria were applied to filter out studies tangential to the research focus or published in sources lacking credibility.

Subsequently, the amassed data underwent a meticulous thematic analysis, a rigorous process aimed at identifying recurrent themes and patterns embedded within the literature. This analytical approach facilitated a nuanced comprehension of the predominant challenges, emerging solutions, and prospective trajectories within the realm of fintech cybersecurity and data privacy. By systematically distilling and synthesizing the findings, the study endeavors to provide actionable insights and contribute to advancing knowledge in this critical domain.

The collected data was then analyzed using a thematic analysis approach. This involved identifying recurring themes and patterns within the literature, allowing for a comprehensive understanding of the field's key challenges, solutions, and future directions.

Literature Review

Cybersecurity and Data privacy in the fintech industry have emerged as critical issues that demand attention. The rapid growth of fintech has raised concerns about the security and protection of sensitive financial data. The increasingly heavy reliance on digital platforms and mobile applications for financial transactions has created vulnerabilities that threat actors can exploit. The World Bank and CCAF report highlights that cybersecurity risks are the biggest concern for financial regulators in the fintech industry. Furthermore, the implementation of financial insurance and the understanding of cyber risks pose challenges for fintech companies.

“FinTech”, a contraction of “Financial technology”, refers to technology enabled financial solutions. It is often seen today as the new marriage of financial services and information technology (Arner, D. at all, 2016). In (Gai, K., at all, 2020), the authors investigate the definition of Fintech and measure the extent of the impact of Fintech variables on the Cybersecurity as the dependent variable. (Cukier, K., at all, 2018) a major theme in this book is that “big data” will become the dominant scientific paradigm, and change society—and it may yet. Guidelines set out the EBA’s view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. Competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010 to whom Guidelines apply should comply by incorporating them into their practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where Guidelines are directed primarily at institutions (European Banking Authority, 2018). Special consideration is given to how blockchain-based identity and access management systems can address some of the key challenges associated with IoT security (Kshetri, N., 2017). Consumers, increasingly aware of their privacy rights, may seek alternative products and services without appropriate protections (International Association of Privacy Professionals, 2019). The Council is charged with identifying risks to the financial stability of the United States; promoting market discipline; and responding to emerging risks to the stability of the United States' financial system (Financial Stability Oversight Council, 2020). For example, in the paper (Smith, A. N., & Smith, B. L., 2018) they investigate the definition of Fintech and measure the extent of the impact of Fintech variables on Cybersecurity as the dependent variable. Beyond individual organizations, cyber risk is a systemic challenge and cyber resilience a public good. Every organization is a steward of information they manage on behalf of others. And every organization contributes to the resilience of their immediate customers, partners, and suppliers and the overall shared digital environment (World Economic Forum, 2019). This study (Apostu, S. A., at all, 2022) may also help policymakers and regulators to structure and improve their policies toward investing in financial markets, as cryptocurrencies require multiple risk-mitigation approaches for investors and financial markets. As researchers and practitioners alike seek to identify new ways to solve business challenges, inspire financial innovation, and create and seize new opportunities, insurers around the world are increasingly teaming up with insurtechs, and other tech startups (Manta O, at all, 2023). There has been an increased recognition that more attention needs to be paid to AI, the internet of things, environmental, social, and governance (ESG), sustainability, adoption, and intelligent automation (Tong L, at all, 2022). Also in the specialized literature, we identified the work (Brooks C. J., et all,

 doi:10.20944/preprints202401.2194.v2

2018), which offers clear and comprehensive details on cyber security, with a direct orientation towards current challenges, namely:

- How to secure the infrastructure.
- How to secure and control devices.
- How to secure of local and global networks, as well as securing and protecting the perimeter.

This scientific work deals with these challenges and demonstrates to us through the analyzed scenarios, those vulnerabilities (Brooks C. J., et all, 2018), that each system user may face in their daily professional life. In the digital age, individual autonomy should prevail, and this aspect must be carefully protected through clear tools and mechanisms. (Becker, M., 2019) starts from the privacy debates, and through the aspects mentioned by the author helps us how to protect personal autonomy in the digital age, an essential aspect especially in the context of fintech financial instruments. As also presented by (Yuchong Li et all, 2021)), cyber security "tracks real-time information about the latest IT data". It is obvious that at the global level, especially in the context of AI, researchers at the international level propose tools, various methods, models to prevent and limit cyber-attacks, but above all to limit the damage generated by these attacks.

The rapidly evolving fintech industry has witnessed a surge in cybersecurity and data privacy concerns, prompting extensive research and diverse perspectives on addressing these challenges. The world bank and CCAF identify the need for increased collaboration between insurers and insurtechs to drive financial innovation and address the evolving landscape of risks, such as AI, IoT technologies, ESG factors, sustainability, and intelligent automation. (Contributors, 2023). Existing research explores the multifaceted nature of cybersecurity in fintech, its impact on the cybersecurity landscape and the need for proac-tive defense strategies. However, opportunities exist to delve deeper into the methodologi-cal approaches employed within these studies. Critically examining the assumptions, limitations, and potential biases inherent in the reviewed literature can offer a more nu-anced understanding of the field and pave the way for future research directions. Cybersecurity and data privacy concepts and definitions

Defining some key concepts is important to understand the challenges and considerations surrounding cybersecurity and data privacy in the fintech world.

Threat landscape: The Fintech sector is continuously experiencing a wide range of evolving and diverse threats that pose significant risks to the security and privacy of sensitive data. These include cyber-attacks, data breaches, compliance issues with regulations, and new technologies introducing vulnerabilities.

Risk management: It includes the systematic identification, analysis, evaluation, and reduction of potential vulnerabilities and threats to guarantee a strong security infrastructure. Strict protocols for privacy management involve in-depth data protection within complex financial processes by methodically identifying risks, analyzing vulnerabilities, and evaluating threats to ensure effective security measures., and maintaining strict privacy protocols for sensitive data within fintech organizations. (Uddin et al., 2020)

Encryption: Converting sensitive data into unreadable code to prevent unauthorized access using encryption techniques and algorithms. This helps in ensuring that only authorized individuals or systems with the proper decryption key can access and understand the information, thus safeguarding it from potential security breaches.

Authentication: The process of verifying the identity of users or devices to ensure only authorized access to sensitive information and systems, often through multifactor authentication and security protocols. This includes confirming identities through biometric data, passwords, tokens, smart cards, or other secure methods while considering potential threats such as phishing attacks and social engineering tactics. (Varshney et al., 2020)

Security breach: Unauthorized access refers to gaining entry to sensitive data without proper authorization, while disclosure involves releasing this information to unauthorized individuals. Alteration pertains to any unauthorized changes made to the data, and destruction indicates the intentional or accidental elimination of sensitive data.

 doi:10.20944/preprints202401.2194.v2

Compliance: Ensuring that fintech organizations strictly adhere to a comprehensive set of regulatory requirements and industry standards, meticulously designed to safeguard customer information and uphold the highest levels of data privacy. (Suryono et al., 2020)

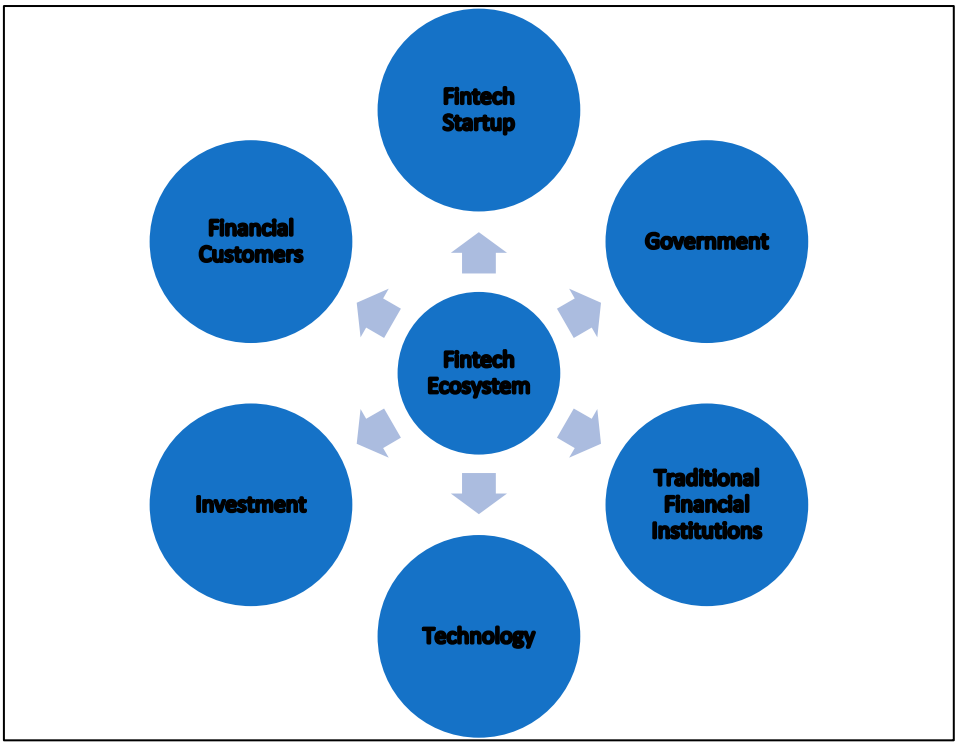

Figure 1. Ecosystem for Fintech. *Source: own processing.*

The figure depicts the interdependencies and relationships that exist within the fintech industry. Fintech companies create cutting-edge financial solutions and are recognized as important participants in the ecosystem. The end users utilizing these products are financial customers. The links to investments indicate the financial backing necessary for fintech projects to expand. Technology is a crucial component that emphasizes the need for advanced IT systems. The integration of traditional financial institutions represents the changing dynamic between fintech innovators and established finance organizations. Another crucial component is the government, which demonstrates the regulatory framework and its role in forming the fintech landscape.

Cybersecurity and Data Privacy Solutions

Cybersecurity threats keep evolving rapidly, requiring fintech companies to adapt and implement robust security measures constantly. The implementation of these measures is crucial for protecting against evolving threats. Some of the measures include:

- Encryption: Encrypting sensitive data in transit and at rest using solid algorithms like AES and RSA can significantly increase its security (Kavitha et al., 2022). Encryption helps to ensure that even if the data is accessed, it cannot be understood without the proper decryption key.
- Authentication: Implementing multi-factor authentication (MFA) protocols beyond traditional passwords can further strengthen access security. It may include biometric authentication, one-time passwords, or hardware tokens.
- Security Assessments: Regularly conducting penetration testing and vulnerability scanning helps identify and address security gaps before attackers can exploit them. Security assessments can also include risk assessments and security audits to evaluate the effectiveness of existing security measures.

 doi:10.20944/preprints202401.2194.v2

Furthermore, emerging technologies like artificial intelligence (AI) and blockchain offer promising avenues for enhancing fintech security. AI-powered systems can analyze vast amounts of data to detect and prevent malicious activities in real-time. At the same time, blockchain technology can offer secure and tamper-proof data storage and sharing mechanisms. However, It is crucial to balance adopting these technologies with considerations for user privacy, responsible development, and ethical implications.

Common Cyber Security Threats for the Fintech

Phishing and social manipulation attacks are among the main reasons for security breaches due to human error. According to IBM's 2022 report on the Cost of a Data Breach, these attacks can also be very costly, with an average impact of USD 4.91 million for phishing and USD 4.10 million for social engineering. In such cases, attackers try to deceive users to obtain sensitive information like login credentials or banking details through email. Clicking on any compromised links or attachments in phishing emails can result in installing malicious software on the targeted computer system or lead users to a fraudulent webpage designed to collect login credentials. ((Oraca) & (Craciun), n.d)

Another significant risk financial technology companies face is the presence of malware and ransomware attacks. Malware pertains to harmful software designed to disturb or obtain unauthorized entry into computer systems. Such attacks can jeopardize user data, disrupt services, or facilitate unlawful access to financial systems. Attackers utilize malware to infiltrate systems and gain unauthorized access to information before deploying ransomware that encrypts the company's data. To prevent public exposure or avoid complete deletion of the company's database in some instances, threat actors demand payment in exchange for releasing it.

Due to the valuable customer and intellectual property information, it holds, ransomware groups find the financial services industry highly attractive. Furthermore, FinTech platforms are vulnerable to various malware, including viruses, ransomware, and spyware. The risk of exposing this data on the dark web and the subsequent harm to reputation and business prospects often forces many financial services organizations to give in to ransom demands even if official recommendations go against such practices.

Distributed Denial of Service (DDoS) Attacks are another threat that targets the resources of a FinTech platform, rendering it inaccessible to legitimate users. By flooding the system with a massive volume of traffic or requests, attackers disrupt services, cause financial losses, and damage the reputation of the targeted platform. To address these cybersecurity risks, the financial technology industry must prioritize the implementation of robust cybersecurity frameworks and standards.

 doi:10.20944/preprints202401.2194.v2

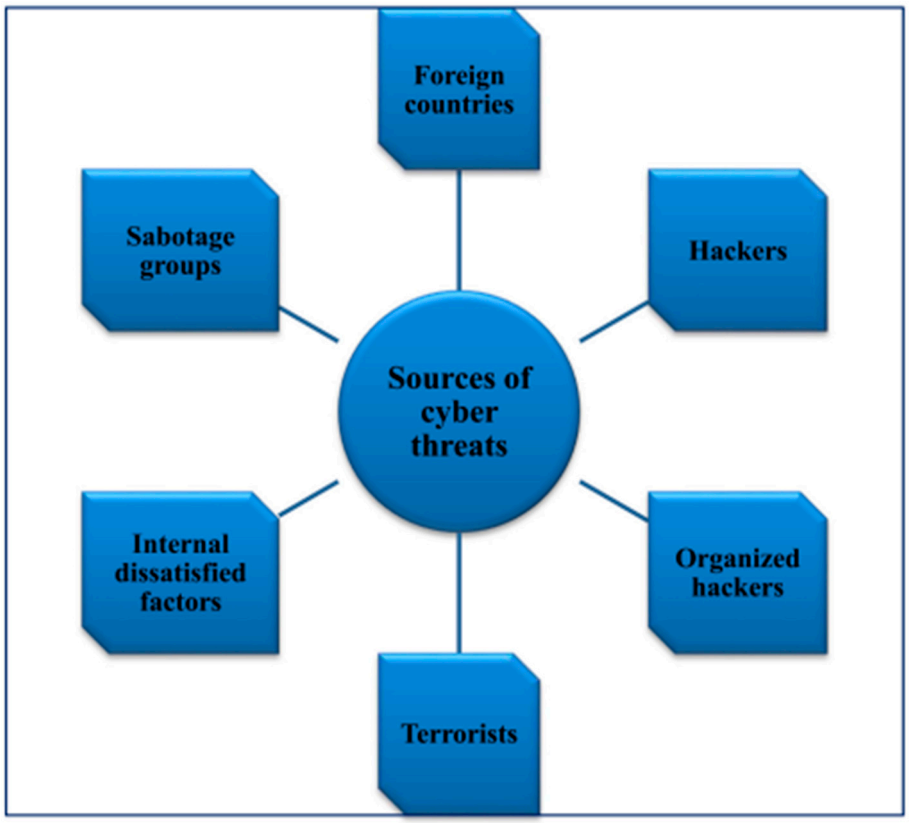

Figure 2. Sources of cyber threats. Source: (Yuchong Li, et all, 2021).

As seen in the figure above, the source of cyber-attacks is different, and very often being distributed randomly, it isn't very easy to identify the person or persons who generated the respective cyber-attack.

A few recent studies highlight the increasing risks and challenges faced by the FinTech industry in terms of cybersecurity. For instance, the Decentralized Finance (DeFi) Platform Nomad Bridge Exploit resulted in a loss of $11 million worth of cryptocurrency due to a smart contract vulnerability (Challenges of using artificial intelligence, 2024). The incident was that a vulnerability in the Nomad bridge, which allowed users to transfer funds be-tween different blockchain networks, was exploited by a malicious actor who drained the funds. The regulatory landscape was such that the Defi platform could not recover the stolen funds. The Nomad Bridge exploit exposed the security risks inherent in DeFi protocols and the need for stricter measures to ensure user asset safety and transparency within the DeFi ecosystem.

Another instance is the social engineering attack on Binance users, where Binance, a leading cryptocurrency exchange, experienced a breach resulting in the theft of over $40 million worth of Bitcoin. (Contributors, 2023). Hackers gained unauthorized access to user accounts through phishing techniques and were able to steal funds from unsuspecting users. While Binance is subject to regulations in certain jurisdictions, the global nature of cryptocurrency makes it challenging to enforce consistent security measures across all platforms and jurisdictions. The incident underscores the importance of user education and awareness to prevent falling victim to phishing attacks in the context of cryptocur-rency transactions.The two recent cases above highlight the evolving nature of cybersecurity threats in the fintech industry, particularly about cryptocurrency platforms and decentralized finance protocols. While regulations are continuously being developed to address these issues, fintech companies must stay proactive in implementing strong cybersecurity measures and educating users about potential risks to mitigate cybercrime threats in the financial technology industry.

 doi:10.20944/preprints202401.2194.v2

Solutions

To address the challenges mentioned above, fintech companies must implement appropriate cybersecurity measures (Creado & Ramteke, 2020). Companies must develop a clearly defined cybersecurity plan aligning with their business goals. This plan should include specific objectives, risk evaluations, strategies for handling incidents, and initiatives to raise employee awareness. It should also consider emerging risks and changing technologies to guarantee ongoing security measures.

Enterprises must prioritize implementing robust access controls to prevent unauthorized entry to sensitive data and systems. This involves enforcing strong authentication methods, like multifactor authentication, for verifying user identities, and establishing role-based access controls to ensure that employees have suitable access privileges according to their roles and duties.

Encryption serves as a crucial security measure for safeguarding data against unauthorized access. FinTech companies must apply encryption to protect data during transmission and when stored on their systems. Utilizing secure encryption protocols like Transport Layer Security can help ensure data security in transit, while employing robust encryption algorithms is necessary for securing data at rest. ((Oraca) & (Craciun), n.d)

Regular security evaluations, like penetration testing and vulnerability scanning, are useful for uncovering potential weaknesses in systems. Experts must carry out these assessments to identify vulnerabilities, evaluate the efficacy of security measures, and promptly address any identified weaknesses.

A well-prepared and thoroughly practiced incident response plan is essential in minimizing harm and swiftly restoring services during a cybersecurity incident. FinTech companies must create detailed response plans that define roles, escalation procedures, communication protocols, and recovery processes. Regular testing and simulation exercises are also necessary to verify the effectiveness of these plans.

It is essential to regularly apply security patches and updates to software, operating systems, and network infrastructure. This helps to address known vulnerabilities and protects against potential exploitation by cybercriminals.

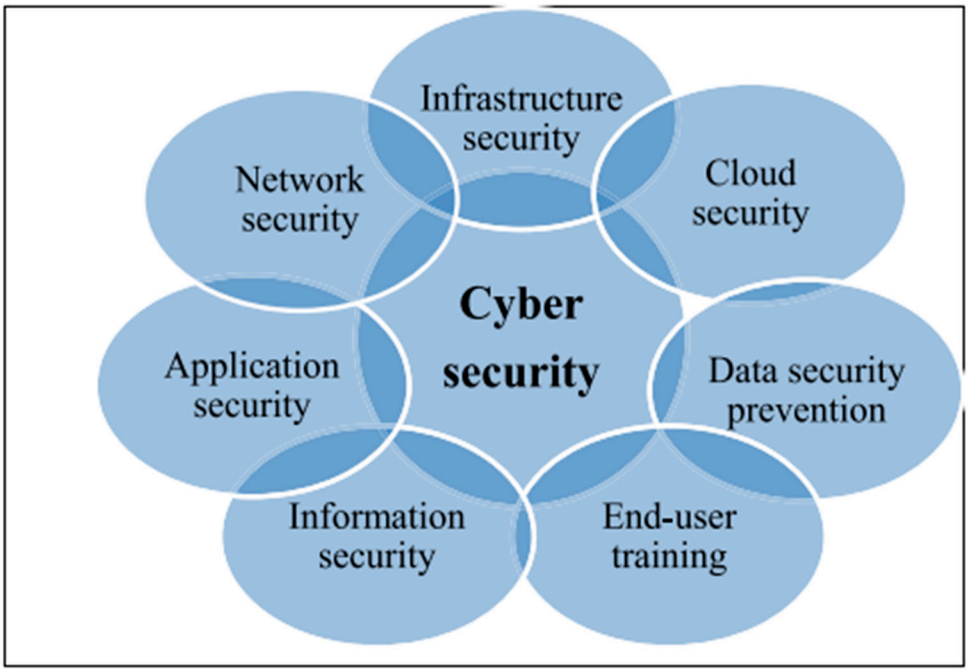

Figure 3. Security triangle (CIA). Source: (Yuchong Li, et all, 2021).

 doi:10.20944/preprints202401.2194.v2

To ensure cyber security at the level of institutions involved in offering FinTech digital financial services, we appreciate that all those involved in the activity process and for a good protection and management of financial data must flow, it is essential to know at the individual and institutional level what are the types of cyber. The figure above shows the different types of cyber security (Yuchong Li, et all, 2021).

Additionally, Fintech organizations should closely monitor and stay informed about the latest data protection and privacy regulation updates, ensuring compliance with local and international laws such as the General Data Protection Regulation and the Payment Card Industry Data Security Standard.

Lastly, companies should develop a strong culture of security within their organizations. Fintech organizations should prioritize cybersecurity and data privacy from the top down, fostering a culture of security awareness and ensuring that all employees are trained on best practices for handling sensitive data and identifying potential threats.

2. Materials and Methods

To gather information on cybersecurity and data privacy in the fintech industry, a multi-step approach was followed ((Oraca) & (Craciun), n.d). This included thoroughly reviewing relevant literature, industry reports, and regulatory guidelines. The sources mentioned in the prompt were consulted to gain insights into the potential threats faced by FinTech companies and the best practices for implementing cybersecurity measures. Results showed that cybersecurity risks were a major concern for financial regulators, with concerns ranging from operational risks to consumer protection. Fintech companies need to proactively address cybersecurity risks to protect sensitive financial data and maintain the trust of their customers. The findings revealed that cybersecurity and data privacy are crucial for fintech companies.

3. Results and Discussion

The study's results highlighted key points regarding cybersecurity and data privacy in the fintech industry. The study is a call to action for fintech companies to prioritize cybersecurity as a fundamental aspect of their business.

Fintech companies face many cyber threats, including phishing and social engineering attacks, malware and ransomware attacks, and network vulnerabilities. Phishing and social engineering attacks are often directed at unsuspecting employees who may inadvertently compromise sensitive information. Malware and ransomware attacks can cripple fintech operations, leading to financial losses and reputational damage. Additionally, network vulnerabilities pose a significant threat to the confidentiality and integrity of financial data. Fintech companies need to implement robust cybersecurity measures and adhere to data privacy regulations to mitigate these risks. The following data shows the data violation incidents in the US from 2015 to 2022.

 doi:10.20944/preprints202401.2194.v2

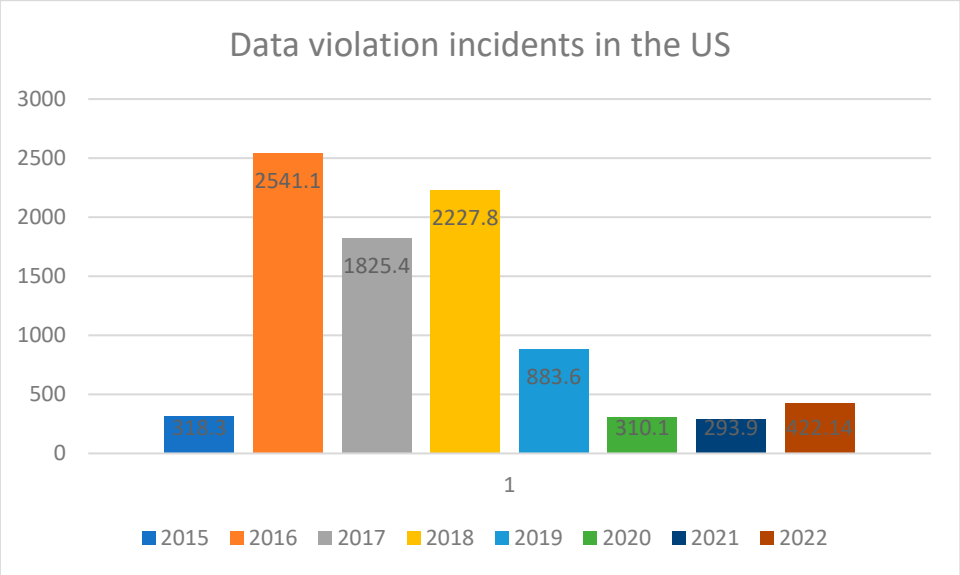

Figure 4. Data violation incidents in the US. *Source: own processing.*

One of the essential best practices is to regularly conduct comprehensive security assessments and penetration testing to identify and address vulnerabilities in their systems. This proactive approach can help preempt potential cyber threats and safeguard sensitive financial information. Furthermore, fostering a culture of cybersecurity awareness and providing regular training to employees can significantly reduce the risk of falling victim to social engineering attacks. Strong authentication measures, encryption protocols, and secure access controls are imperative to protect financial data from unauthorized access. (Arner, D. W., et all, 2016).

Regulatory issues and lack of customer trust further compound FinTech companies' challenges in ensuring cybersecurity and data privacy. Regulatory issues such as the General Data Protection Regulation and the Payment Card Industry Data Security Standard place additional compliance burdens on fintech companies. Non-compliance with these regulations can result in severe penalties and reputational damage. Moreover, the lack of trust among customers due to concerns about the security of their financial information underscores the urgency for fintech companies to invest in robust cybersecurity infrastructure and transparent data privacy practices.

Implementing best practices such as intrusion detection systems, threat intelligence feeds, and comprehensive cybersecurity programs can significantly enhance the cybersecurity posture of fintech companies. These measures protect sensitive financial data and foster trust among customers, leading to increased adoption of fintech services. Intrusion detection systems and threat intelligence feeds can help detect and respond to potential cyber threats in real time, minimizing the impact of attacks. Additionally, establishing solid partnerships with trusted cybersecurity providers can ensure continuous monitoring and prompt incident response, further strengthening the overall security of fintech systems. (IAPP, 2019)

Collaboration and information sharing within the industry are crucial for combating cyber threats and avoiding emerging risks. Creating platforms and networks for information sharing, such as cybersecurity forums and industry associations, can facilitate the exchange of best practices, threat intelligence, and cyber incident response strategies. (Gai et al., 2018) By pooling resources, knowledge, and expertise, fintech companies can collectively augment their cybersecurity capabilities and strengthen the overall resilience of the entire industry. In today's rapidly changing world, the significance of accurate weather forecasts cannot be overstated.

Similarly, the significance of cybersecurity and data privacy cannot be overstated in the booming fintech world. The following table shows the highest number of victim losses in the United States in 2022. The data is considered in millions of US Dollars.

 doi:10.20944/preprints202401.2194.v2

Table 1. Cybercrime and victim losses. *Source: own processing*.

Category	Loss in $ Million
Investment	$ 3,311.74
Business email Compromise	$ 2,742.35
Tech Support	$ 806.55
Personal Data breach	$ 742.44
Confidence fraud	$ 735.88
Real estate	$ 396.93
Non-payment/ non-delivery	$ 281.77
Credit card/ Check fraud	$ 264.15
Government impersonation	$ 240.55
Identity theft	$ 189.21
Spoofing	$ 107.93
Advanced fee	$ 104.33

Industry-wide cybersecurity standards and regulations must also be established to ensure consistent and robust cybersecurity practices among fintech companies. These standards should address critical areas such as data encryption, access controls, authentication mechanisms, incident response protocols, and regular security audits. (Tyagi, 2022) Furthermore, adopting Explainable Artificial Intelligence techniques in credit card fraud detection can help address concerns surrounding the opacity of AI models. Additionally, fintech companies should prioritize cybersecurity as a fundamental aspect of their business. This includes allocating adequate resources in terms of budget and personnel to develop and implement comprehensive cybersecurity programs.

4. Challenges and Future Directions

To address the challenges mentioned above, fintech companies must implement appropriate cybersecurity measures (Creado & Ramteke, 2020). Companies must develop a clearly defined cybersecurity plan aligning with their business goals. This plan should include specific objectives, risk evaluations, strategies for handling incidents, and initiatives to raise employee awareness. It should also consider emerging risks and changing technologies to guarantee ongoing security measures.

Enterprises must prioritize implementing robust access controls to prevent unauthorized entry to sensitive data and systems. This involves enforcing powerful authentication methods, like multifactor authentication, for verifying user identities and establishing role-based access controls to ensure that employees have suitable access privileges according to their roles and duties (RX Advanced Technologies LTD, 2024).

Encryption serves as a crucial security measure for safeguarding data against unauthorized access. FinTech companies must apply encryption to protect data during transmission and when stored on their systems. Utilizing secure encryption protocols like Transport Layer Security can help ensure the security of data in transit while employing robust encryption algorithms is necessary for securing data at rest (Oraca M.U. et al., 2023) (Petrosyan A., 2023).

Regular security evaluations, like penetration testing and vulnerability scanning, help uncover potential weaknesses in systems. Experts must carry out these assessments to identify vulnerabilities, evaluate the efficacy of security measures, and promptly address any identified weaknesses.

A well-prepared and thoroughly practiced incident response plan is essential in minimizing harm and swiftly restoring services during a cybersecurity incident. FinTech companies must create detailed response plans that define roles, escalation procedures, communication protocols, and recovery processes. Regular testing and simulation exercises are also necessary to verify the effectiveness of these plans.

 doi:10.20944/preprints202401.2194.v2

It is essential to regularly apply security patches and updates to software, operating systems, and network infrastructure. This helps to address known vulnerabilities and protects against potential exploitation by cybercriminals.

Additionally, Fintech organizations should closely monitor and stay informed about the latest data protection and privacy regulation updates, ensuring compliance with local and international laws such as the General Data Protection Regulation and the Payment Card Industry Data Security Standard.

While significant progress has been made in addressing cybersecurity challenges in the fintech industry, the industry's dynamic nature necessitates continuous research and innovation. Emerging trends like quantum computing and the widespread adoption of IoT devices introduce new threats that require proactive measures.

Future Research Efforts Should Focus on:

Investigating the potential impact of quantum computing on existing encryption methods used in fintech and exploring the development and implementation of post-quantum cryptography solutions.

Developing advanced detection and prevention techniques to combat social engineering attacks targeting individuals and organizations within the fintech ecosystem.

Conducting research on securing IoT devices used in financial transactions and mitigating their potential vulnerabilities to ensure the secure integration of these technologies within the fintech landscape.

It is crucial for academia, industry, and regulatory bodies to collaborate in addressing these emerging challenges. Continuous research, knowledge sharing, and the development of robust cybersecurity frameworks are essential to ensure the secure and sustainable growth of the fintech industry.

5. Conclusions

With the rapidly expanding fintech sector, protecting cybersecurity and data privacy is critical to retaining customer trust and promoting long-term success. Fintech businesses are encouraged to make it a top priority to establish advanced cybersecurity security measures, thorough data privacy guidelines, and an effective security culture within the organizations they operate. Navigating the intricacies of the digital landscape requires keeping up with legislative changes.

The industry needs to acknowledge and manage the risks associated with inherent cyber-security in addition to these recommended practices. Fintech businesses must consider cybersecurity and data privacy as core components of their business operations and cus-tomer relationships to fully realize the potential for innovation and growth.

The limited availability of data on incidence statistics after 2020 is acknowledged in our study. However, to find conclusive data on cyberattacks and their financial impact on the fintech sector, we commit to continue our research using scientific databases and collabo-rating with regulatory bodies in the future. This commitment aims to further assist fintech companies in prioritizing cybersecurity and data privacy, building customer trust, and protecting sensitive information.

Finally, our research emphasizes how critical cybersecurity and data privacy are to the long-term sustainability of the financial sector and customer trust. Important actions in-clude putting strong cybersecurity security measures in place, taking a proactive approach to counter emerging threats and keeping an eye on developments in fields like post-quantum cryptography and explainable AI integration.

Furthermore, it has been suggested that responsible growth in fintech requires exploring ethical issues and regulatory frameworks related to AI. Another important area for pro-gress is the safe integration of IoT devices into the finance ecosystem.

In the long run, promoting cooperation between regulatory bodies, the industry, and ac-ademia becomes critical. This cooperative effort has been identified to be a major force be-hind innovation and ongoing cybersecurity practice improvement in the fintech sector. The fintech sector can ensure

 doi:10.20944/preprints202401.2194.v2

an efficient and sustainable future through the prioritization of research, the development of resilient solutions, and constant monitoring.

Author Contributions: Conceptualization, R.K. and O.M..; methodology, R.K..; validation, R.K. and O.M..; formal analysis, R.K. and O.M..;.; investigation, R.K. and O.M..; resources, R.K. and O.M..; data curation, R.K. and O.M..; writing—original draft preparation, R.K..; writing—review and editing, R.K. and O.M..;.; visualization, R.K. and O.M..;.; supervision, R.K. and O.M..;.; project administration, R.K. and O.M..; funding acquisition, O.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data used in the research article can be found in the URL https://www.statista.com/statistics/234987/victim-loss-cyber-crime-type/

Acknowledgments: many special thanks to the editorial team of the FinTech Journal and the valuable team of reviewers.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The Evolution of FinTech: A New Post-Crisis Paradigm? Georgetown Journal of International Law, 47(4), 1271-1320.
2. Apostu, S. A., Panait, M., Vasa, L., Mihaescu, C., & Dobrowolski, Z. (2022). NFTs and Cryptocurrencies—The Metamorphosis of the Economy under the Sign of Blockchain: A Time Series Approach. Mathematics, 10(17), 3218.
3. Barberis Nicholas, 2018, Handbook of Behavioral Economics: Applications and Foundations 1, North-Holland, Volume 1,2018, Pages 79-175, ISSN 2352-2399,ISBN 9780444633743, ttps://doi.org/10.1016/bs.hesbe.2018.07.001.
4. Becker, M., 2019, Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. Ethics Inf Technol 21, 307–317 (2019). https://doi.org/10.1007/s10676-019-09508-z
5. Brooks Charles J., Christopher Grow, Philip Craig, Donald Short, 2018, Cybersecurity Essentials, ISBN:9781119362395, John Wiley & Sons, Inc.
6. Catalini, Christian and Gans, Joshua S., Some Simple Economics of the Blockchain (April 20, 2019). Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16, Available at SSRN: https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598
7. Cha D., C. Pae, S.-B. Seong, J.Y. Choi, H.-J. Park, (2019), Automated diagnosis of ear disease using ensemble deep learning with a big otoendoscopy image database, EBioMedicine, 45 (2019), pp. 606-614
8. Chen, L., Wang, W., Nagarajan, M., Wang, S., Sheth, A., 2012. Extracting diverse sentiment expressions with target-dependent polarity from twitter. In: Proceedings of the International AAAI Conference on Web and Social Media, vol. 6, no. 1, pp. 50–57.
9. Claessens, Stijn and Frost, Jon and Turner, Grant and Zhu, Feng, Fintech Credit Markets Around the World: Size, Drivers and Policy Issues (September 1, 2018). BIS Quarterly Review September 2018, Available at SSRN: https://ssrn.com/abstract=3288096
10. Creado, Y., & Ramteke, V. (2020, May 2). Active cyber defense strategies and techniques for banks and financial institutions. https://doi.org/10.1108/jfc-01-2020-0008
11. Cocco, L., Pinna, A., & Marchesi, M. (2017). Banking on Blockchain: Costs Savings Thanks to theBlockchain Technology. Future Internet, 9(3), 25. doi:10.3390/fi9030025
12. (3) (PDF) FinTech in Banks: Opportunities and Challenges. Available from: https://www.researchgate.net/publication/344646568_FinTech_in_Banks_Opportunities_and_Challenges [accessed Mar 19 2024].
13. Cukier, K., & Zhu, H. (2018). Big Data, Big Risks: Toward Sustainable Cybersecurity in Financial Technology. Journal of Cybersecurity, 4(1), 1-17.
14. Cumming Sean P., Chris Searle, Janie K. Hemsley, Finlay Haswell, Hannah Edwards, Sam Scott, Aleks Gross, Desmond Ryan, Jeff Lewis, Paul White, Andrew Cain, Siobhan B. Mitchell, Robert M. Malina, (2018), Biological maturation, relative age and self-regulation in male professional academy soccer players: A test of the underdog hypothesis, Psychology of Sport and Exercise,Volume 39, 2018, Pages 147-153, ISSN 1469-0292, https://doi.org/10.1016/j.psychsport.2018.08.007.
15. European Banking Authority. (2018). Guidelines on the Security Measures for Operational and Security Risks of Payment Services Under Directive (EU) 2015/2366 (PSD2). Retrieved from https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2263108/1f74ebf0-c7b2-4e89-ade0-16ebea24cc7d/EBA-GL-2018-

 doi:10.20944/preprints202401.2194.v2

07%20%28Guidelines%20on%20security%20measures%20for%20operational%20and%20security%20risks%20of%20payments%20services%20under%20PSD2%29.pdf

16. Financial Stability Oversight Council. (2020). Annual Report. Retrieved from https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1085
17. Gai, K., Qiu, M., & Sun, X. (2018, February 1). A survey on FinTech. Journal of Network and Computer Applications, 103, 262-273. https://doi.org/10.1016/j.jnca.2017.10.011
18. Gai, K., Qiu, M., & Sun, X. (2020). Blockchain Cybersecurity in Financial Technology Applications: A Case Study of Ant Financial. Journal of Information Security and Applications, 50, 102417.
19. International Association of Privacy Professionals (IAPP). (2019). The Growing Global Focus on Privacy: 2019 Privacy Governance Report. Retrieved from https://iapp.org/resources/article/the-growing-global-focus-on-privacy-2019-privacy-governance-report/
20. Hasan, Rashedul, Mohammad Kabir Hassan and Sirajo Aliyu.(2020) "Fintech and Islamic Finance: Literature Review and Research Agenda." International Journal of Islamic Economics and Finance (IJIEF) (2020): n. pag.
21. Kshetri, N. (2017). Can blockchain strengthen the Internet of Things? IT Professional, 19(4), 68-72.
22. Manta, O., Folcut, O., & Militaru, L. (2023). ARTIFICIAL INTELLIGENCE, INTEGRITY, AND OPPORTUNITY IN INSURTECH. Journal of Information Systems & Operations Management, 17(1), 97-110.
23. Milian Eduardo Z., Mauro de M. Spinola, Marly M. de Carvalho, (2019), ,Fintechs: A literature review and research agenda, Electronic Commerce Research and Applications, Volume 34, 2019, 100833, ISSN 1567-4223, https://doi.org/10.1016/j.elerap.2019.100833.
24. Miroshnychenko Ivan, Barontini Roberto, Testa Francesco, 2017, Green practices and financial performance: A global outlook, Journal of Cleaner Production, Volume 147, 2017, Pages 340-351, ISSN 0959-6526, https://doi.org/10.1016/j.jclepro.2017.01.058.
25. Oraca, M U., & Craciun, L F. (n.d), 2023, The Rise of FinTech and the Need for Robust Cybersecurity Measures
26. Petrosyan A., 2023, Leading cyber-crime victim loss categories U.S. 2022, https://www.statista.com/statistics/234987/victim-loss-cyber-crime-type/
27. R K. (2023, October 11). Examining The Role of Fintech in Financial Inclusion and Its Impact on Financial Services to Underbanked Population in India. https://doi.org/10.36948/ijfmr.2023.v05i05.7473
28. RX Advanced Technologies LTD, 2024, ResilientX Security is the leading provider of cutting-edge cyber security solutions for Security testing, Posture Management, Security rating and Risk monitoring, https://resilientx.com/blog/ibm-cost-of-a-data-breach-report-2023-what-we-learn-from-it/
29. Sangwan, V., Prakash, P., & Singh, S. (2020). Financial technology: A review of extant literature. Studiesin Economics and Finance, 37(1), 71–88. doi:10.1108/SEF-07-2019-0270
30. (3) (PDF) FinTech in Banks: Opportunities and Challenges. Available from: https://www.researchgate.net/publication/344646568_FinTech_in_Banks_Opportunities_and_Challenges [accessed Mar 19 2024].
31. Smith, A. N., & Smith, B. L. (2018). FinTech: Addressing Cybersecurity Risks. Journal of Technology Research, 9, 1-16.
32. Suryono, R R., Budi, I., & Purwandari, B. (2020, December 21). Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review. Information, 11(12), 590-590. https://doi.org/10.3390/info11120590
33. Tong L, Yan W and Manta O (2022) Artificial Intelligence Influences Intelligent Automation in Tourism: A Mediating Role of Internet of Things and Environmental, Social, and Governance Investment. Front. Environ. Sci. 10:853302. doi: 10.3389/fenvs.2022.853302
34. Uddin, H., Ali, H., & Hassan, M K. (2020, August 18). Cybersecurity hazards and financial system vulnerability: a synthesis of literature. Risk Management, 22(4), 239-309. https://doi.org/10.1057/s41283-020-00063-2
35. Varshney, S., Munjal, D., Bhattacharya, O., Saboo, S., & Aggarwal, N. (2020, December 16). Big Data Privacy Breach Prevention Strategies. 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC). https://doi.org/10.1109/isssc50941.2020.9358878
36. World Economic Forum. (2019). Advancing Cyber Resilience: Principles and Tools for Boards. Retrieved from http://www3.weforum.org/docs/WEF_Advancing_Cyber_Resilience_Principles_and_Tools_for_Boards_2019.pdf
37. Woods A., 2022, https://www.startupdaily.net/podcasts/suds-with-adviser-ratings-founder-angus-woods-on-the-rise-of-fintech-the-great-tech-jobs-crisis-paying-advisors-and-mental-health-for-kids/
38. Yermack, David, Corporate Governance and Blockchains (November 28, 2016). Review of Finance, Forthcoming, Available at SSRN: https://ssrn.com/abstract=2700475 or http://dx.doi.org/10.2139/ssrn.2700475

 doi:10.20944/preprints202401.2194.v2

39. Yong Xu, Ling Yuan, Hyoungsuk Lee, Sabrine Baire, Joanna Nakonieczny, Xin Zhao, Fintech Development and Firm Technological Innovation Efficiency: Empirical Findings in China, IEEE Transactions on Engineering Management, 10.1109/TEM.2023.3239499, 71, (3881-3891), (2024).
40. Yuchong Li, Qinghui Liu, 2021, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Energy Reports, Volume 7, Pages 8176-8186, ISSN 2352-4847. https://doi.org/10.1016/j.egyr.2021.08.126.
41. Contributors, F. (2023, July 10). The Challenges and Opportunities of Data Privacy and Security in the Fintech Ecosystem. https://www.financemagnates.com/fintech/data/the-challenges-and-opportunities-of-data-privacy-and-security-in-the-fintech-ecosystem/
42. Kavitha, A., Rao, B S., Akhtar, D N., Rafi, D S M., Singh, P., Das, S., & Manikandan, D G. (2022, June 30). A Novel Algorithm to Secure Data in New Generation Health Care System from Cyber Attacks Using IoT. International journal of electrical & electronics research, 10(2), 270-275. https://doi.org/10.37391/ijeer.100236
43. Challenges of using artificial intelligence. (2024, January 1). https://www2.deloitte.com/us/en/pages/consulting/articles/challenges-of-using-artificial-intelligence.html