Published: 31 December 2024

Cybersecurity and Fintech Studies in Academic Discussion

Hasna Maliha[1]
[1]*SMART Indonesia, Indonesia*

This study aims to see the development of research on the topic of "Cybersecurity and Fintech" and research plans that can be carried out based on journals published on the theme. This research uses a qualitative method with a bibliometric analysis approach. The data used is secondary data with the theme "Cybersecurity and Fintech" which comes from the Dimension database with a total of 351 journal articles. Then, the data is processed and analyzed using the VosViewer application with the aim of knowing the bibliometric map of "Cybersecurity and Fintech" research development in the world. The results of the study found that there were 5 clusters with the most used words being security, system, company, model, threat, innovation, regulation, financial inclusion, banking, market, and cryptocurrency. Then, the research path topics related to Cybersecurity and Fintech are Data Security in Fintech Adoption, Big Data for Cybercrime Mitigation in Fintech, Information Security in the Fintech Ecosystem, Fintech cloud innovation for security, and Technological Innovation in Financial Markets.

Keywords: Cybersecurity, Fintech, Research Map, Bibliometric

OPEN ACCESS
ISSN 2775-4251 (Online)

*Correspondence:
Hasna Maliha
hasliha@gmail.com

Received: 3 October 2024
Accepted: 1 December 2024
Published: 31 December 2024

Citation:
(2024) Cybersecurity and Fintech Studies in Academic Discussion. Journal of Islamic Economic Literature. 5.2.

INTRODUCTION

The origins of fintech date back to the late 19th century with foundational technologies such as the first transatlantic cable and electronic funds transfer systems. These early innovations laid the foundation for subsequent developments in financial services infrastructure. Subsequently, significant growth occurred in the aftermath of the 2008 financial crisis. The crisis highlighted inefficiencies in the traditional banking system, which paved the way for innovative solutions. The term "fintech" began to gain traction when technology companies started providing alternatives to conventional banking services, such as peer-to-peer lending and mobile payment platforms (Putri et al., 2023; Pham et al., 2024). The introduction of smartphones and high-speed internet further accelerated this shift, enabling app-based banking solutions and contactless payments that appeal to a tech-savvy consumer base. These technologies facilitate the development of new financial products and services that are more accessible and user-friendly (Anyfantaki, 2016; Iman, 2020).

Fintech has been instrumental in breaking down geographical barriers to financial services. Fintech provides access to banking and investment opportunities for underserved populations who may not have access to traditional banking systems. By enabling online loan applications and digital payment processes, fintech increases market access for micro, small and medium enterprises (MSMEs), which drives economic growth in these sectors (Kumalasari & Farida, 2024). This democratization of financial services is important to promote financial literacy and inclusion across different demographics.

The integration of technology into financial services has also resulted in improved operational efficiency. Fintech companies utilize automation and advanced algorithms to streamline processes such as loan approvals and customer service interactions, which reduces the time and costs associated with these operations. For example, the use of big data analytics enables more accurate credit scoring and risk management, leading to faster decision-making and lower operational costs (Iman, 2020; AlMomani & Alomari, 2021).

Nonetheless, financial technology (fintech) presents challenges that affect its growth and integration into the financial landscape. One of the main challenges relates to cybersecurity. As fintech relies heavily on digital platforms for transactions and data storage, it has become increasingly vulnerable to cyberattacks. The rise of online financial transactions has raised concerns about data privacy and security breaches. Fintech companies must implement robust cybersecurity measures to protect sensitive customer information and maintain trust in their services (Suryono et al., 2020; Junaidi et al., 2023). The potential for significant financial losses due to cyber incidents poses a critical challenge for fintech development.

There are several types of cybersecurity threats, especially in the fintech industry, including data theft, unauthorized access to sensitive customer data, leading to identity theft and fraud; lax cybersecurity regulations that can make fintech companies vulnerable, making them attractive targets for cybercriminals; and theft of proprietary technology or algorithms posing significant risks to fintech innovation and competitiveness (Alodhiani, 2023; Bae & Hong, 2023). On the other hand, the integration of advanced technologies such as cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) has given rise to new vulnerabilities. For example, cloud services have become a focal point of attacks due to their widespread adoption in the financial sector (Ali & Qassem, 2023; Bae & Hong, 2023). In addition, as personal data is increasingly consolidated with platforms, the risk of large-scale data breaches increases (Bae & Hong, 2023).

Cyberattacks can cause huge financial losses to fintech companies through direct theft, regulatory fines, and reputational damage. Organizations may also incur increased insurance premiums and legal fees following a breach (Aksoy, 2023). Cybersecurity incidents can also erode consumer trust, hindering the adoption of innovative financial solutions. Lack of trust can significantly impact user engagement and retention (Alexandri et al., 2023). To combat such threats, it is important for fintech companies to develop a robust cybersecurity framework. Utilizing AI for threat detection and response can significantly improve security measures. Recent studies have shown that machine learning models can effectively reduce system vulnerabilities while improving detection time (Bhaskaran, 2024; Bae & Hong, 2023).

The intersection of cybersecurity and financial technology (FinTech) presents significant challenges and opportunities for research. Despite the growing body of literature available, there are still some important gaps that need to be addressed to increase understanding and improve practice in this domain. Most research focuses primarily on the point of view of FinTech companies, ignoring insights from consumers and regulators. This

lack of comprehensive analysis may hinder the development of a robust cybersecurity framework that addresses the needs and concerns of all parties involved (AlBenJasim et al., 2024). Therefore, it is important to see the extent of the current development of *Cybersecurity and Fintech* through research, and one method that can be used to see the development of research is bibliometrics using VosViewer. The method is able to create and display author journal maps and research paths based on co-citation data or keyword maps based on shared incident data.

Some research that examines related to *Cybersecurity and Fintech* is Mustapha et al (2023) investigating the complex and evolving cybersecurity landscape in the fintech mobile application ecosystem. This research explains that cybersecurity threats in the fintech mobile application ecosystem cover a broad spectrum, including data breaches, malware attacks, phishing schemes, and identity theft. Fintech apps are often prime targets for malicious actors seeking financial gain because fintech deals with handling sensitive financial data and transactions. To address such threats, this research examines 's current cybersecurity strategies and emerging technologies, such as advanced encryption, biometric authentication, and AI-driven anomaly detection. Furthermore, regulatory frameworks and industry standards play an important role in shaping cybersecurity practices in fintech

Sahid et al (2023) explored the growth of research paradigms related to "FinTech agility" literature with bibliometric analysis. The results revealed significant differences between authors, publication influence, and keyword occurrence between WOS and combined databases. This research also highlights the importance of incorporating database approaches in bibliometric studies and demonstrates the importance of "FinTech Agility" in the rapidly growing FinTech sector. The agility of financial technology companies, or the ability to adapt quickly, is the foundation of their success and innovation. Lavanya & Rajkumar (2024) examined the cybersecurity landscape in the banking industry with bibliometric analysis. The results revealed a pattern of increase in article production in 2019 and 2023 and the average article citations peaked in 2018. In today's banking sector, there has been a significant increase in the utilization of digital technologies and devices. The importance of digital security is a major concern for all individuals. Cybersecurity is of utmost importance in safeguarding the information and data provided by customers.

Jain et al (2024) analyzed the adoption of Fintech in the banking sector with bibliometric analysis. The digital revolution has crossed the threshold of the banking sector worldwide. Financial Technology (Fintech) has moved away from the essence of the traditional banking system and has replaced this physical system with a revolutionary new app-based banking system. In today's era, customers want innovative services that are quick and easy to handle, which is why Fintech is gaining importance in today's market and triggering disruptions to the traditional banking concept. In the race of providing innovative services to customers between bankers and Fintech companies, the real winner is the customer.

Sahabuddin et al (2023) investigated how FinTech evolved over time in research using bibliometric analysis. The study revealed a trend of increasing annual publications, a shift in focus on financial inclusion, a dominance of authors from the US, and an increasing number of international collaborations and publications from various sources, indicating FinTech as an active field with potential for further scientific enrichment. Bajwa et al (2022) conducted a meta-literature review that examined the past, present, and possible future trends of Fintech research by bibliometric analysis. The analysis revealed 4 major research clusters related to Bitcoin and digital currencies, crowdfunding, mobile payments, and blockchain. The results highlighted the most influential aspects of the FinTech literature, such as leading countries, institutions, journals, authors, and articles.

Idayani et al (2024) examined how cyber risks will affect the use of fintech. The results showed that cyber-related risks can be categorized based on the type of crime. Overall, the user acceptance measurement model for Fintech serves to assist developers and companies in understanding, predicting, and improving user acceptance of Fintech solutions, as well as informing effective strategy development and product improvements. Thottoli (2024) discussed the tactical role of financial technology (FinTech) in accounting and auditing with bibliometric analysis. This research identifies the tactical role of fintech especially in the field of accounting and auditing professionals. Fintech is still in its infancy, with ongoing development and implementation taking place particularly in auditing. The findings also confirm that FinTech can generate confluence between different research areas, including accounting, auditing, business finance, economics, management, and business fields.

This research was conducted to complement existing research and fill the gaps of previous research and to expand the literature related to *Cybersecurity and Fintech* through the research path. In particular, the purpose of this research is to see the development of "*Cybersecurity and Fintech*" research published by journals with this theme and see future research opportunities by formulating a research agenda.

METHOD

In this research, various scientific journal publications related to the theme "*Cybersecurity and Fintech*" around the world are used as data sources. The data is collected by searching for Dimension database indexed journal publications using the keywords "*Cybersecurity and Fintech*". After that, scientific articles or journals that are relevant to the research theme will be selected based on the publication data that has been collected. Journals equipped with DOI are the criteria in the filtering process and data processing using software. There were 351 journal articles published from within the research theme "*Cybersecurity and Fintech*". The development of publication trends related to the research topic was analyzed using VOSviewer software, which can generate bibliometric maps and allow for more detailed analysis.

In order to build the map, VOSviewer uses the abbreviation VOS which refers to Visualizing Similarity. In previous studies, the VOS mapping technique has been used to obtain bibliometric visualizations which are then analyzed. Furthermore, VOSviewer is able to create and display author journal maps based on co-citation data or keyword maps based on co-incidence data. Therefore, this research will analyze journal maps related to "*Cybersecurity and Fintech*", including author maps, and keywords which are then analyzed for research paths that can be carried out in the future through clusters on *keyword mapping*.

This research uses a descriptive qualitative approach with meta-analysis and descriptive statistical literature study based on 351 journal publications that discuss the theme of "*Cybersecurity and Fintech*". Meta-analysis is a method that integrates previous research related to a particular topic to evaluate the results of existing studies. Furthermore, the qualitative method used in this research is also referred to as a constructive method, where the data collected in the research process will be constructed into themes that are easier to understand and meaningful. The sampling technique used in this research is purposive non-probability sampling method, which aims to fulfill certain information in accordance with the desired research objectives. Studies using bibliometric analysis in research on other topics for example can be seen in Khalifah et al., (2024), Mi'raj & Ulev (2024), Napitupulu, et al., (2024); Yenice et al., (2022), Rusydiana (2021), Rusydiana et al., (2023), Ozdemir & Selçuk (2021), and also Laila et al., (2021).

RESULT AND DISCUSSION

Research Map

The figure 1 describes the trend of keywords that appear in research on the theme "*Cybersecurity and Fintech*" and the larger shapes are the most used words in journal publications on the theme "*Cybersecurity and Fintech*". As for the mapping, the keywords that appear most in the publication "*Cybersecurity and Fintech*" include security, system, company, model, threat, innovation, regulation, financial inclusion, banking, market, and cryptocurrency which are then divided into 5 clusters, as follows.

Cluster 1: Data Security in Fintech Adoption

This cluster contains 30 keyword items, namely access, adoption, banking, banking sector, collaboration, consumer protection, country, data privacy, digital banking, disruption, economic growth, financial inclusion, financial industry, financial stability, fintech innovation, fintech solution, innovation, insight, integration, light, mobile banking, operational efficiency, policymaker, practice, regulation, regulatory compliance, smes, stakeholder, technological advancement, transformation. A number of relevant studies include research from Nayak et al (2021) analyzing the effect of data security and consumer trust on fintech. This study confirms that customer trust (CT), data security (DS), added value (VA), user design interface (UI), are influenced by the intention to adopt fintech. There is insufficient evidence to conclude that promotion affects the intention to adopt fintech.

Ramaswamy et al (2024) empirically investigated the role of consumer trust and data security in fintech adoption. The findings of this study highlight a strong relationship between consumer trust and adoption of fintech services. Users who perceive a higher level of trust in fintech platform integrity and data security are more likely to use fintech services. This research also highlights the important role of data security measures that fintech companies are expected to practice. Olaiya et al (2024) discussed various encryption techniques required to secure financial

information in fintech applications. The main methods described in this study include symmetric encryption, asymmetric encryption, and hybrid encryption techniques. In addition, the functionality of end-to-end encryption (E2EE) is discussed in terms of protecting the privacy of data as it is transmitted, which is crucial for protecting sensitive financial activities such as mobile banking and digital payments. The research also concluded that Fintech security is expected to be shaped by new developments in encryption technology, including post-quantum cryptography, integration of artificial intelligence for adaptive security measures, and privacy-protecting solutions.

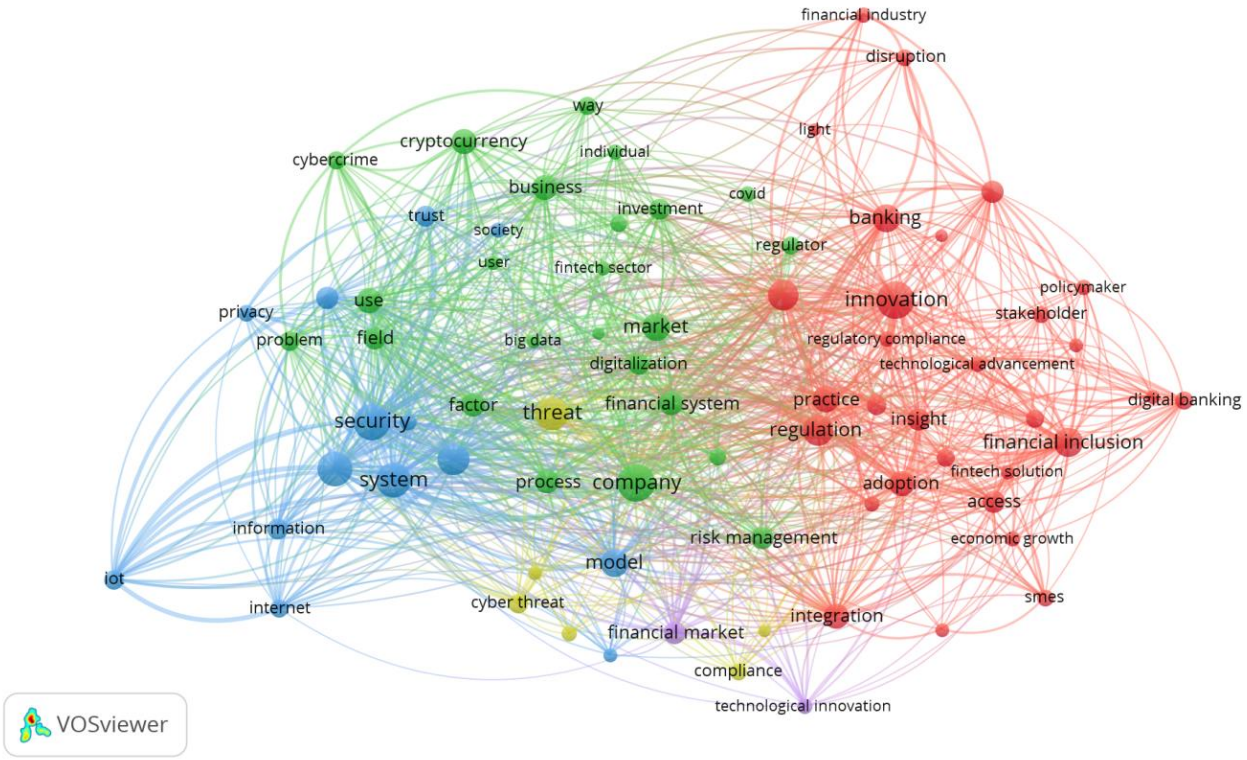

Figure 1. Research cluster

Singh et al (2021) examined a framework for improving cybersecurity in fintech applications in India. Fintech is currently among the most rapidly growing sectors in terms of business growth and job creation. The broader objective of Fintech is to cater to the unmet financial needs of certain demographic groups that are not the main focus markets in the mainstream financial services model. The research emphasizes the importance of data protection and the urgent need for measures to be taken by all stakeholders for the sustainable growth of the Fintech sector.

Munasinghe et al (2024) present a research model to assess the position of Fintech in the context of open banking, especially from the customer's perspective on data security and privacy issues. This research explains, the use of Fintech for open banking is gradually increasing as it allows consumers to share their data with third-party providers and access their products and services. Due to a lack of trust in data security and privacy, there is a reluctance to consent to sharing personal data and a fear of losing control of the data hoarded during open banking. Stewart & Jürjens (2018) empirically analyzed the main factors influencing the adoption of financial technology (FinTech) innovations in Germany, highlighting the important role of data security, customer trust, and user interface design. . The research findings suggest that FinTech providers need to better communicate the value and benefits of their services to drive adoption.

Zhang et al (2023) empirically investigated the effect of perceived ease of use (PEU), perceived usefulness (PU), data security (DAS) on Fintech service adoption intention through Fintech promotion (FP), and customer trust (CT). The regression results show that DAS, PEU, PU, FP, CT have a positive and significant influence on the adoption intention of Fintech Services. PEU, DAS, PU also have a positive and significant influence on CT. In addition, customer

perceptions of DAS and PEU also have a positive and significant influence on customer perceptions of the importance of FP. In contrast, FP has an insignificant influence on CT and PU also has an insignificant influence on FP.

Cluster 2: Big Data for Cybercrime Mitigation in Fintech

This cluster has 24 keyword items, namely big data, business, company, covid, cryptocurrency, cybercrime, digital technology, digitalization, digitization, factor, field, financial system, fintech sector, individual, investment, knowledge, market, problem, process, regulator, risk management, use, user, way. The topic of Big Data for Cybercrime Mitigation in Fintech discusses the utilization of big data technology to identify, prevent, and mitigate cybercrime threats in the fintech sector. Not enough research has been explored on the topic, among the relevant research is reviewing cybersecurity issues and mitigation measures in FinTech. The main findings of this research identified privacy concerns, data breaches, malware attacks, hacking, insider threats, identity theft, social engineering attacks, distributed denial-of-service attacks, cryptojacking, supply chain attacks, advanced persistent threats, zero-day attacks, salami attacks, man-in-the-middle attacks, SQL injection, and brute-force attacks as some of the significant cybersecurity issues experienced by the FinTech industry. The results also suggested authentication and access control mechanisms, cryptography, regulatory compliance, intrusion detection and prevention systems, regular data backup, basic security training, big data analysis, use of artificial intelligence and machine learning, FinTech regulatory sandbox, cloud computing technology, blockchain technology, and fraud detection and prevention systems as mitigation measures for cybersecurity issues.

Despotović et al (2023) outlined cybercrime in the field of financial technology. This research emphasizes the importance of preventing cyber-attacks and that employee training is a very important factor in protecting systems so that they know how to prevent potential attacks and accidental security breaches. In addition, banks were the first to introduce technological innovations into their operations, which led to a revolution of technological advancements in Fintech. Not only do banks participate in the modern financial business, but a large part of the business also consists of companies specializing in the development and implementation of financial technology. Considering cyber risks in detail and providing adequate counter-responses for each of its elements is also an important thing that needs to be considered by relevant parties.

Cyriac & Sadath (2019) present a Model for Countering Cyber Attacks (MECA) that can be adopted by financial institutions. MECA proposes smart implementation of IDS, Security Patches, and big data Analytics to mitigate cyber challenges in financial institutions. The focus of MECA is to technologically orient institutions to handle dynamic cyber breaches, to train employees to effectively deploy these smart applications, and to develop them as the first line of defense against cyber attacks. The research also discusses the perpetrators in cyberattacks and the tools mostly used to achieve their goals.

Strang (2024) analyzed employee behavior big data from the global intranet of a multinational Fintech company. A critical issue worldwide is that ransomware cyberattacks can cost organizations dearly. Furthermore, the risk of unintentional employee cybercrime can be challenging to prevent, even by utilizing advanced computer science techniques. As the research explains, higher levels of employee neuroticism are associated with greater organizational cybercrime risk. In addition, conscientiousness, friendliness, and extroversion, had no informative relationship with cybercrime risk. This research introduces an interdisciplinary paradigm shift for big data cognitive computing by illustrating how to integrate proven scientific constructs into machine learning to analyze human behavior using an otherwise more efficient retrospective big data collection approach.

Ekundayo et al (2024) examined cyber threat intelligence in fintech using big data and machine learning. In the rapidly evolving FinTech landscape, cybersecurity has become a critical priority due to the increasing sophistication of cyber threats targeting financial institutions. The research highlights key applications, including threat pattern recognition using historical data, real-time dynamic risk assessment with financial transaction data, and Natural Language Processing (NLP) to extract actionable insights from threat intelligence feeds. Cloud security solutions, strengthened by Big Data analytics, were examined for their role in protecting FinTech platforms from Distributed Denial of Service [DDoS] and ransomware attacks. Additionally, the research emphasizes the importance of automating incident response mechanisms using advanced ML models to reduce response time and operational disruption, and strategic predictive analytics in strengthening the cybersecurity framework in the FinTech sector.

Cluster 3: Information Security in the Fintech Ecosystem

This cluster has 14 keyword items, namely application, aspect, blockchain, blockchain technology, complexity, information, internet, iot, model, privacy, security, society, system, trust. A number of studies relevant to the topic include Kaur et al (2021) introducing information security governance, various policies and standards used to profile information security governance, and security governance models. This research also examines the roles and responsibilities of individuals working in upper, middle, and lower management. The security governance framework has two main activities: directing and controlling. Directing is a top-down approach initiated by the board of directors and executives (upper management) and followed by middle and lower management personnel. In contrast, controlling is a bottom-up approach that covers the daily operations performed by the lower-level management to work based on the directions given by the top management.

Kurmanova et al (2021) describe the digital transformation of banking, emphasizing the need for better management methods in response to global instability. The research highlights the development of Fintech ecosystems that enhance the provision of financial services through better customer data analysis, automation, and information security measures. Pachare & Bangal (2023) investigated cybersecurity, information security, and privacy in the Indian fintech ecosystem, providing a framework and discussing the various cyber threats faced by various organizations in digital payments. The research highlights the importance of maintaining cyber hygiene, innovative security measures, and prevention strategies to combat fraud in digital transactions. Chubaievskyi & Volosovych (2021) examined the role of FinTech tools in corporate information systems, highlighting the associated threats and the importance of ensuring their security. This research emphasizes that the increasing digitization of financial activities, accelerated by the Covid-19 pandemic, has created new challenges for corporate information systems in managing cyber risks. The research concludes that securing these systems is critical to maintaining enterprise stability amid the evolving FinTech ecosystem.

Cluster 4: Fintech cloud innovation for security

This cluster has 6 keyword items, namely cloud computing, compliance, cyber threat, digital economy, machine learning, threat. A number of relevant studies include Boda (2020) adapting cloud fintech security for health services. This research explains, the key to securing fintech cloud changes lies in understanding the relationship between FinTech and healthcare needs, and proactively developing cloud security solutions that are resilient, adaptable, and able to withstand the evolving threat landscape. The rapid convergence of the FinTech and healthcare sectors, driven by the adoption of cloud technologies, presents both tremendous opportunities and significant security challenges. As healthcare systems increasingly rely on FinTech solutions for everything from payment processing to patient data management, the need to adapt and secure these cloud-based platforms becomes critical.

Vivek et al (2020) explain the role of the cloud in FinTech and RegTech. This research explains, cloud services are key to maintaining information in a secure and accessible way at any time, while maintaining a level of security and transparency. Cloud services are currently required by financial institutions in the era of digital banking, which is almost like one-click banking through a smartphone. Fintech technologies cover a wide range of functions such as mobile banking, big data, predictive models, compliance, crowdfunding, risk management, cryptocurrency, and payments and transfers. On the other hand, RegTech is an innovation in FinTech, offering solutions that are faster and more agile in meeting customer needs. With advanced technologies such as AI, IoT, and cloud services, RegTech provides more flexible, fast, and economical solutions to support legal compliance.

Olorunyomi et al (2024) discuss the integration of fintech innovations and multi-cloud environments in predictive financial modeling. Fintech advances, such as artificial intelligence, machine learning, and blockchain, provide significant improvements in financial forecasting, risk assessment, and decision making. Meanwhile, multi-cloud architectures provide the flexibility, scalability and resilience required to support these advanced fintech solutions. By combining fintech and multi-cloud, financial institutions are better equipped to utilize real-time predictive analytics, ultimately changing the future of financial services.

Immaneni (2020) discusses the challenges and opportunities that Fintech companies face during the cloud migration journey. This research emphasizes the importance of a robust cloud strategy that leverages the strengths of various cloud providers, allowing businesses to avoid dependence on vendors while optimizing resource allocation. Patil et al (2023) discussed Zero

Trust Architecture (ZTA) as a contemporary security framework specifically designed to meet the evolving security needs of cloud-based fintech services. The financial technology (fintech) sector has seen a rapid rise in recent years, driven by the growing adoption of cloud computing and the introduction of innovative financial services. The rapid migration to the cloud, while enabling greater accessibility and scalability, has also posed inherent security challenges that traditional perimeter-based security models struggle to effectively address. As cyber threats become more sophisticated and persistent, fintech companies must adopt a more robust and comprehensive approach to protect their cloud-based services and sensitive financial data. Kollu et al (2023) analyzed a cloud-based intrusion detection system based on IoT federated learning architecture as well as smart contract analysis. This research proposes a new method to detect intrusion using a cyber threat federated graphical authentication system and cloud-based smart contracts in FinTech data.

Cluster 5: Technological Innovation in Financial Markets

This cluster has 5 keyword items, namely financial markets, technological innovation. There are still quite a few studies with this topic. Among the relevant research, Hirsch-Kreinsen (2011) discusses the relationship between technological innovation and finance. Financial markets should be considered as one of the fundamental prerequisites of innovation, as this is where decisions are made about the allocation of capital to firms. However, less has been written about the interdependence between financial patterns and corporate governance on the one hand and firms' innovation strategies on the other. Lewis et al (2017) describe blockchain and financial market innovation. Blockchain technology is likely to be a major source of financial market innovation in the future. This technology enables the creation of an immutable record of transactions that is accessible to all participants in the network. A blockchain database consists of a number of blocks that are "chained" together through references in each block to previous blocks. Each block records one or more transactions, which is essentially a change in the owner of a recorded asset. New blocks are added to the existing chain through a consensus mechanism where members of the blockchain network confirm the transaction as valid.

Hacioglu (2020) examines various aspects of blockchain in the economic system and investment strategies in the crypto market. This research discusses the topic from a conceptual and theoretical standpoint, and then analyzes it from a valuation and investment standpoint. It also discusses the opportunities and limitations of cryptocurrency taxation, as well as its political implications, such as the regulation of speculation with cryptocurrencies. Muharam et al (2020) examined the relationship between process innovation, market innovation, and financial performance of pharmaceutical companies. The results of this study highlight that there is a positive relationship between process innovation, market innovation, and firm financial performance. In addition, disruptive technology moderates the relationship between process innovation and financial performance, but has no moderating role on the relationship between market innovation and financial performance.

CONCLUSION

This research aims to find out the extent of the development of research themed "Cybersecurity and Fintech" in the world. The results of the study show that the number of research publications related to "Cybersecurity and Fintech" there are 351 journal articles indexed by Dimension. Furthermore, in the development of research related to "Cybersecurity and Fintech" based on bibliometric keyword mapping, the most used keywords are security, system, company, model, threat, innovation, regulation, financial inclusion, banking, market, and cryptocurrency. Based on the keywords that are often used, then grouped into 5 research map clusters with the topic that discuss Cybersecurity and Fintech, namely Data Security in Fintech Adoption, Big Data for Cybercrime Mitigation in Fintech, Information Security in the Fintech Ecosystem, Fintech cloud innovation for security, and Technological Innovation in Financial Markets.

REFERENCES

Aksoy, C. (2023). Critical Success Factors For Cybersecurity Just Technical? Exploring The Role Of Human Factors In Cybersecurity Management. Research Journal of Business and Management, 10(2), 51-57.

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2024). Fintech cybersecurity challenges and regulations: Bahrain case study. Journal of Computer Information Systems, 64(6), 835-851.

Alexandri, M. B., Usman, I., Narimawati, U., & Taryana, A. (2023). Unraveling the Fintech Landscape: A Systematic Mapping Study on the Impact of

Financial Technology Innovation on Investment Decision-Making in ASEAN Banking. Khazanah Sosial, 5(1), 113-124.

Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. (2024). A Comprehensive review on cybersecurity issues and their mitigation measures in FinTech. Iraqi Journal For Computer Science and Mathematics, 5(3), 45-91. https://doi.org/10.52866/ijcsm.2024.05.03.004

Ali, J., & Qassem, N. (2023). Blockchain Technology Applications and Cybersecurity Techniques: A Literature Review. International Journal of Computers and Informatics, 2(6). https://doi.org/10.59992/ijci.2023.v2n6p2

AlMomani, A. A., & Alomari, K. F. (2021). Financial Technology (FinTech) and its role in supporting the financial and banking services sector. International Journal of Academic Research in Business and Social Sciences, 11(8), 1793-1802.

Alodhiani, A. A. B. (2023). Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review.)20, (المجلة العربية للعلوم الإنسانية والاجتماعية.

Anyfantaki, S. (2016). The evolution of financial technology (Fintech).

Bae, J.K., & Hong, G.H. (2023). A Study on Digital Financial Security Threats and Cybersecurity Policies. The Academic Society of Global Business Administration. https://doi.org/10.38115/asgba.2023.20.6.133

Bajwa, I. A., Ur Rehman, S., Iqbal, A., Anwer, Z., Ashiq, M., & Khan, M. A. (2022). Past, present and future of FinTech research: A bibliometric analysis. Sage Open, 12(4), 21582440221131242.

Bhaskaran, S. (2024, May). Analysis of an Intelligent and Cybersecurity Optimization Model for Financial Applications. In 2024 International Conference on Electronics, Computing, Communication and Control Technology (ICECCC) (pp. 1-6). IEEE.

Boda, V. V. R. (2020). Securing the Shift: Adapting FinTech Cloud Security for Healthcare. MZ Computing Journal, 1(2).

Chubaievskyi, V., & Volosovych, S. (2021). Security of corporate information in fintech ecosystem. Foreign Trade Economics Finance Law, 119(6), 98-108. https://doi.org/10.31617/zt.knute.2021(119)08

Cyriac, N. T., & Sadath, L. (2019, November). Is Cyber security enough-A study on big data security Breaches in financial institutions. In 2019 4th International Conference on Information Systems and Computer Networks (ISCON) (pp. 380-385). IEEE.

Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and cyber security in fintech. In Digital transformation of the financial industry: approaches and applications (pp. 255-272). Cham: Springer International Publishing.

Ekundayo, F., Atoyebi, I., Soyele, A., & Ogunwobi, E. (2024). Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning. Int J Res Publ Rev, 5(11), 1-15.

Hacioglu, U. (2020). Blockchain economics and financial market innovation. Springer, Switzerland.

Hirsch-Kreinsen, H. (2011). Financial markets and technological innovation. Industry and Innovation, 18(4), 351-368.

Idayani, R. W., Nadlifatin, R., Subriadi, A. P., & Gumasing, M. J. J. (2024). A Comprehensive Review on How Cyber Risk Will Affect the Use of Fintech. Procedia Computer Science, 234, 1356-1363.

Iman, N. (2020). The rise and rise of financial technology: The good, the bad, and the verdict. Cogent Business & Management, 7(1), 1725309.

Immaneni, J. (2020). Cloud Migration for Fintech: How Kubernetes Enables Multi-Cloud Success. Innovative Computer Sciences Journal, 6(1).

Jain, S., Sharma, J., Sharma, S., Kaushik, A., & Rajawat, N. (2024). Bibliometric Analysis of Literature on Fintech and Cyber Frauds in Banking. Multidisciplinary Approaches for Sustainable Development, 138-144.

Junaidi, A., Wulandari, R., Susilowati, E., Safitri, N., & Ikhsan, M. (2023). A literature review on fintech innovations: Examining the evolution, impact, and challenges. SEIKO: Journal of Management & Business, 6(2), 438-448.

Kaur, G., Habibi Lashkari, Z., Habibi Lashkari, A., Kaur, G., Habibi Lashkari, Z., & Habibi Lashkari, A. (2021). Information Security Governance in FinTech. Understanding Cybersecurity Management in FinTech: Challenges, Strategies, and Trends, 35-64.

Khalifah, M. H., Kasri, R. A., & Aslan, H. (2024). Mapping the evolution of ZAKAH theme publications years 1964-2021: a bibliometric analysis. *Journal of Islamic Accounting and Business Research*, *15*(2), 265-290.

Kollu, V. N., Janarthanan, V., Karupusamy, M., & Ramachandran, M. (2023). Cloud-based smart contract analysis in fintech using IoT-integrated federated learning in intrusion detection. Data, 8(5), 83.

Kumalasari, D., & Farida, A. (2024). Utilizing Financial Technology (Fintech) to Drive Increased Economic Growth. Scientific Journal of Unity Management, 12(1), 9-16.

Kurmanova, L., Nurdavliatova, E., Kurmanova, D., Galimova, G., & Khabibullin, R. (2021, March). Development of digital services and information security of banks. In IV International Scientific and Practical Conference (pp. 1-6).

Laila, N., Rusdiana, A. S., & Assalafiyah, A. (2021). The impact of Covid-19 on the halal economy: A bibliometric approach. *Library Philosophy and Practice (e-journal)*, 1-18.

Lavanya, B., & Rajkumar, A. D. (2024). Bibliometric insights on mapping the landscape of cybersecurity: Uncovering the research potential in banking industry. Multidisciplinary Reviews, 7(6), 2024113-2024113.

Lewis, R., McPartland, J., & Ranjan, R. (2017). Blockchain and financial market innovation. Economic Perspectives, 41(7), 1-17.

Mi'raj, D. A., & Ulev, S. (2024). A bibliometric review of Islamic economics and finance bibliometric papers: an overview of the future of Islamic economics and finance. *Qualitative Research in Financial Markets*, 16(5), 993-1035.

Muharam, H., Andria, F., & Tosida, E. T. (2020). Effect of Process Innovation and Market Innovation on Financial Performance with Moderating Role of Disruptive Technology. Systematic Reviews in Pharmacy, 11(1).

Munasinghe, A., Grandhi, S., & Imam, T. (2024). An Assessment of Fintech for Open Banking: Data Security and Privacy Strategies from the Perspective of Fintech Users. In Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing: Volume 17 (pp. 55-67). Cham: Springer Nature Switzerland.

Mustapha, I., Vaicondam, Y., Jahanzeb, A., Usmanovich, B. A., & Yusof, S. H. B. (2023). Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem. International Journal of Interactive Mobile Technologies, 17(22).

Napitupulu, R. M., Sukmana, R., & Rusydiana, A. S. (2024). Governance of Islamic social finance: learnings from existing literature. *International Journal of Islamic and Middle Eastern Finance and Management*, *17*(3), 552-571.

Nayak, K., Singh, P., & Dave, P. (2021). Does data security and trust affect the users of FinTech? International Journal of Management (IJM), 12(1), 191-206.

Olaiya, O. P., Adesoga, T. O., Adebayo, A. A., Sotomi, F. M., Adigun, O. A., & Ezeliora, P. M. (2024). Encryption techniques for financial data security in fintech applications. International Journal of Science and Research Archive, 12(1), 2942-9.

Olorunyomi, T. D., Okeke, I. C., Ejike, O. G., & Adeleke, A. G. (2024). Using Fintech innovations for predictive financial modeling in multi-cloud environments. Computer Science & IT Research Journal, 5(10), 2357-2370.

Özdemir, M., & Selçuk, M. (2021). A bibliometric analysis of the International Journal of Islamic and Middle Eastern Finance and Management. *International Journal of Islamic and Middle Eastern Finance and Management*, *14*(4), 767-791.

Pachare, S. M., & Bangal, S. (2023). Cyber Security in the FinTech Industry: Issues, Challenges, and Solutions. In Cybersecurity Issues, Challenges, and Solutions in the Business World (pp. 1-17). IGI Global.

Patil, K., Desai, B., Mehta, I., & Patil, A. (2023). A Contemporary Approach: Zero Trust Architecture for Cloud-Based Fintech Services. Innovative Computer Sciences Journal, 9(1).

Pham, P. T., Tran, B. T., Huynh, T. H., Popesko, B., & Hoang, D. S. (2024). Impact of fintech's development on bank performance: An empirical study from vietnam. Gadjah Mada International Journal of Business, 26(1), 1-22.

Putri, R. T., Isyanto, P., & Sumarni, N. (2023). The Role of Financial Technology (Fintech) in MSMEs. International Journal of Economics Development Research (IJEDR), 4(1), 294-304.

Ramaswamy, S., Shankaranarayana, R., & Akanfe, O. O. (2024). Data Security and Consumer Trust in Fintech Adoption. In Utilizing Technology for Sustainable Resource Management Solutions (pp. 281-294). IGI Global.

Rusydiana, A. S., Irfany, M. I., As-Salafiyah, A., & Tieman, M. (2023). Halal supply chain: A bibliometric analysis. *Journal of Islamic Marketing*, *14*(12), 3009-3032.

Rusydiana, A. S. (2021). Bibliometric analysis of journals, authors, and topics related to COVID-19 and Islamic finance listed in the Dimensions database by Biblioshiny. *Science Editing*, *8*(1), 72-78.

Sahabuddin, M., Sakib, M. N., Rahman, M. M., Jibir, A., Fahlevi, M., Aljuaid, M., & Grabowska, S. (2023). The evolution of FinTech in scientific research: a bibliometric analysis. Sustainability, 15(9), 7176.

Sahid, A., Maleh, Y., Asemanjerdi, S. A., & Martín-Cervantes, P. A. (2023). A Bibliometric Analysis of

the FinTech Agility Literature: Evolution and Review. International Journal of Financial Studies, 11(4), 123.

Singh, G., Gupta, R., & Vatsa, V. (2021, November). A framework for enhancing cyber security in fintech applications in india. In 2021 International Conference on Technological Advancements and Innovations (ICTAI) (pp. 274-279). IEEE.

Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. Information & Computer Security, 26(1), 109-128.

Strang, K. D. (2024). Cybercrime Risk Found in Employee Behavior Big Data Using Semi-Supervised Machine Learning with Personality Theories. Big Data and Cognitive Computing, 8(4), 37.

Suryono, R. R., Budi, I., & Purwandari, B. (2020). Challenges and trends of financial technology (Fintech): a systematic literature review. Information, 11(12), 590.

Thottoli, M. M. (2024). The tactician role of FinTech in the accounting and auditing field: A bibliometric analysis. Qualitative Research in Financial Markets, 16(2), 213-238.

Vivek, D., Rakesh, S., Walimbe, R. S., & Mohanty, A. (2020). The Role of CLOUD in FinTech and RegTech. Annals of the University Dunarea de Jos of Galati: Fascicle: I, Economics & Applied Informatics, 26(3).

Yenice, A. C., Ozdemir, M., & Koc, A. (2022). Looking at the 'Big Picture'in Islamic Economics and Finance Literature A Bibliometric Analysis of WoS Indexed Documents. *Turkish Journal of Islamic Economics*, *9*(1).

Zhang, W., Siyal, S., Riaz, S., Ahmad, R., Hilmi, M. F., & Li, Z. (2023). Data security, customer trust and intention for adoption of Fintech services: an empirical analysis from commercial bank users in Pakistan. Sage Open, 13(3), 21582440231181388.