**PRACTITIONER RESEARCH**
*https://e-journal.uum.edu.my/index.php/pr*

How to cite this article:
Zaini, M. K., M. Razali, F., Ismail, S., & Fauziah, K. (2025). Trends and insights on the intersection of financial technology and cybersecurity research: A bibliometric review (2014-2024). *Practitioner Research, 7,* July, 138-155. https://doi.org/10.32890/pr2025.7.11

# TRENDS AND INSIGHTS ON THE INTERSECTION OF FINANCIAL TECHNOLOGY AND CYBERSECURITY RESEARCH: A BIBLIOMETRIC REVIEW (2014–2024)

**[1]Muhamad Khairulnizam Zaini, [2]Fazlida Mohd Razali,**
**[3]Subha Ismail & [4]Kiki Fauziah**
[1]Faculty of Information Science,
Universiti Teknologi MARA (UiTM) Shah Alam, Malaysia
[2]Accounting Research Institute (HICoE),
Universiti Teknologi MARA (UiTM) Shah Alam, Malaysia
[3]Tun Abdul Razak Library,
Universiti Teknologi MARA (UiTM) Shah Alam, Malaysia
[4]Faculty of Humanities, Department of Library and Information Science,
Universitas Indonesia, Indonesia

*[1]Corresponding author: nizam0374@uitm.edu.my*

Received: 13/11/2024 Revised: 2/2/2025 Accepted: 25/4/2025 Published: 31/7/2025

## ABSTRACT

The main goal of this study is to reveal the most distinctive trends in the intersection between financial technology (FinTech) and cybersecurity using bibliometric study of the Scopus database sources. The analysis revealed that the research of FinTech and information and cyber security has been growing consistently over the years, since 2014. Implications wise, this study provides researchers and practitioners with a more in depth understanding of how the components of information security and cybersecurity intersect in FinTech based on the trend of the current publications in both areas. Specifically, this study could support researchers in a better insight into and summarization of the most foundational knowledge of information and cyber security factors to FinTech developments. This bibliometric analysis is expected to offer an insight into the structural knowledge of cyber and information security integration with FinTech in the last decade, which is a crucial step in determining the future of research in this area.

**Keywords**: FinTech, bibliometric analysis, cybersecurity, information security, bibliometrix.

## INTRODUCTION

The world's financial ecosystem is changing for the better due to the increasing adoption and integration of technologies such as blockchain, artificial intelligence (AI), decentralized finance (DeFi), and digital banking. The emergence of Cybersecurity and Financial Technologies (FinTech) has simplified and secured transactions. However, it also raises concerns regarding privacy risks, data security, and compliance with legal frameworks (Stewart & Jürjens, 2018; Jović & Nikolić, 2022). Besides the convenience provided by online services, the risk of unauthorized access, data breaches, exposure of sensitive private information, and cyber fraud becomes more plausible. The digitization of the financial services industry has become indispensable, accompanied by the equally urgent need to safeguard sensitive financial information from cyber-attacks, fraud, and breaches, requiring more advanced cybersecurity systems. Cybersecurity has assumed pivotal for safeguarding trust and stability in digital finance infrastructure, which makes it imperative to study its intersection with FinTech. For this study, analyzing the existing literature is deemed as a vital approach to provide insights on the developing technologies and to the digital finance security.

The literature on the development of these domains, while still ongoing, does not quite tell us how effective these approaches are, how cybersecurity is intersected with Financial Technology (FinTech), how they have been adopted, and how security approaches are in alignment with the recent global objectives of digital finance and technology. Hence, there is a need for consolidating the current body of the literature to find out the common themes, patterns and the potential of existing imbalance in the growth of the intersection between cybersecurity and FinTech.

The goal of this study is to conduct a bibliometric analysis for discovering patterns found in the existing body of knowledge in cybersecurity and FinTech. In this, the identified publication trends, and influential works can be used to identify the major patterns and trends during the development of this field. In addition, the bibliometric analysis offers a valuable opportunity to uncover unexplored regions of research, neglected topics (Abdullah et al., 2023). In addition to that, this approach does not only identify new patterns and future approaches but also gives the clue on the intersection of cybersecurity and FinTech using evidence-based insights.

This study intends to conduct a bibliometric analysis to gain the relevant information related to the research trends, seminal works, and future directions of FinTech and cybersecurity in the digital financial services. With the rapid development of these fields due to innovations in Blockchain, AI, and DeFi, a structured review assists in understanding how research has evolved with time by tracking development of new concepts against available literature. Through citation analysis, this method of analysis depicts key sources and publications, primary contributors, and relevant authors and citations shaping these disciplines. In addition, it highlights knowledge gaps that might be related to regulatory limitations and security risks posed by the expansions of emerging technologies in Fintech, thereby guiding the needs for future studies. As a result, the analysis demonstrates critical insights with great value for researchers, financial authorities, and business executives making decisions regarding using digital finance infrastructure and needing effective security infrastructures.

The focus of this study is to investigate and examine this field's most important research subjects and themes and how this can aid in moving forward the research fields. This study seeks to analyze performance outcomes of the publications, recognize main thematic areas, look into emerging trends and research gaps which can help insights into the design of innovative teaching methodology. We address the following questions to achieve this objective.

RQ1. Publication Performance: What have been the performance results of the publications in the field of cybersecurity in FinTech? How has the achievement of these results affected the growth of the field?
RQ2. Key Themes and Trends: What patterns and topics emerge from the intersection of cybersecurity and FinTech literature?
RQ3. Future Research Directions: What are the trends, gaps, or opportunities that can guide further research and priorities in the area of cybersecurity and Fintech?

## LITERATURE REVIEW

### Overview of FinTech and Information Security and Cybersecurity

FinTech refers to the technology based financial service that aims to enhance the accessibility, efficiency and security of financial service. Generally, FinTech describes new, technology driven financial services prompted by entrepreneurial entities, including the rise of crowdfunding, peer to peer (P2P) lending, and the basic digital technologies such as blockchain, DeFi and AI (Busayatananphon & Boonchieng, 2022; Palmié et. al, 2020; Bollinger & Yao, 2018).

In the last ten years, the emergence of FinTech has greatly increased the efficiency of formerly used financial systems (Varga, 2017). Accordingly, it has assisted in enhancing customer experience, broadening the scope of financial inclusion, and minimizing transaction costs (Takeda, & Ito, 2021; Lee et al., 2021; Vives, 2017). FinTech's influence on the global economy is exemplified by the mobile banking and e-wallet applications, online payment systems, and even cryptocurrency trading. The changes have largely led to the inclusion of unbanked and underbanked individuals in developed and emerging economies (Adelaja et al., 2024; Salampasis & Mention, 2018). Traditionally, borderless remittances and contactless payments have been a burden on traditional banking systems, but now the digital payment methods have made this possible, thus allowing FinTech to increase exponentially in speed and convenience of transaction.

In addition, the integration of AI and the use of machine learning (ML) algorithms have enabled the financial sector to perform more sophisticated risk analysis, automated trading, and personalized financial services. Other than that, AI chatbots and robo-advisors have transformed the customer engagement with virtual support and means of investment at the customer's disposal round the clock (Belanche et al., 2019). The increasing use of decentralized blockchain ledgers has also added increased security, transparency and reduced fraud and no more need for intermediary institutions (Renduchintala et al, 2022; Cai, 2018). Consequently, FinTech, which aims to create innovation, efficiency and security as opposed to the conventional banking models, has continued with unprecedented changes to the financial landscape (Alt et al. 2018; Gomber et al. 2018; Varga 2017).

With FinTech growing, cybersecurity is becoming a key component. As digital transactions are becoming more common, the magnitude of cyber threat escalates in digital transactions and requires a highly secure framework to protect sensitive information (Umoga et al., 2024; Corbet & Gurdgiev, 2017). Phishing, ransomware, identity fraud and identity theft highlights the need for the automation of more sophisticated security measures such as encryption; biometric; multi factor authentication; AI based fraud detection and more. At the global stage, governments and relevant authorities are trying to formulate rules and policies that guide FinTech innovations to ensure they adhere to set security frameworks, appropriately guarding consumers and financial institutions against cyber threats (Ng &

Kwok, 2017). In other words, protecting the security of FinTech is crucial in upholding trust, compliance with regulations, and enduring sophisticated cyber threats.

Nonetheless, the ongoing advancement of FinTech is transforming the financial systems of different countries, unlocking opportunities for economic development, while broadening access to finance. Fairly, it seeks to promote inclusivity and develop protective mechanisms like regulations and ethical frameworks for its continuous growth. With an upsurge in research being conducted around FinTech, studies exploring new emerging phenomena, regulatory issues, and the impact of these advancements over time are still needed, thus justifying the importance of this study.

### The Roles of Cybersecurity in the Modern Digital Economy

In today's interconnected digital economy, the synergy between FinTech and cybersecurity is crucial. Apparently, the previous research has shown the rise in cyber-attacks towards the financial institutions, businesses, and consumers are mainly caused by increasing reliance on digital payments, e-commerce, and online banking. As digital information increases in the financial services domain, cyber security incidents including fraudulent transactions, extortion, denial of service attacks, and credit card fraud is also growing in these digital landscapes (Kaur et al., 2021; Hossain et al., 2022; Despotović et al., 2023). In this regard, fostering proper cyber security strategies, policies and regulations in both technological and human places has been shown to support the adoption of technological advancement in the field of financial services (Scheau et. al, 2022).

Emerging technologies like blockchain and AI are changing how cybersecurity is managed in the FinTech sector. For example, Blockchain assists in securing and making financial transactions more visible through decentralized ledgers, while AI in cybersecurity solutions enhances threat detection and response systems (Kumari & Devi, 2022; George, 2023). Within this context, the adoption of new advanced protective measures in the field of cybersecurity is necessary to nurture trust, inspire innovation, and promote sustainable growth in the world of digital finance amidst the advancement of FinTech, thus indicating its crucial role in this field.

## METHODOLOGY

A systematic literature search through Scopus database is optimized to enable the performance of a bibliometric analysis related to cybersecurity and FinTech. The specified research query aimed to collect studies which explored cybersecurity approaches and issues alongside the Fintech domain. The research approach and search query were designed as follows:

### PRISMA Approach for Bibliometric Analysis

This study uses the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to implement a systematic, transparent bibliometric analysis of FinTech and cybersecurity research. The process comprised four phases, identification, screening, eligibility, and inclusion. A structured search query for Fintech and cybersecurity and teaching approaches in Scopus online database was deployed and 1146 publications retrieved initially. Duplicate records were removed and non-relevant document types in the screening phase, after which title and abstract review was performed to confirm the records were aligned with study's objectives. The study then proceeded with the eligibility phase, where initial articles were full text analyzed for inclusion into the dataset. Then, the

library of 1102 publications were analyzed with Bibliometrix for publication trend, citation networks and a thematic evolution. This study employed PRISMA to ensure that such a rigorous, reproducible, and transparent process was applied for the selection of the studies, resulting in more reliable findings in cybersecurity education research.

**Search Query on Scopus database**

Advanced query for Scopus search was used as follows:

> TITLE-ABS-KEY ( ( "Financial Technology" OR "fintech" OR "financial innovation" OR "digital banking" OR "banking technology" OR "electronic finance" OR "decentralized finance" OR "DeFi" OR "Digital Wallet" OR "open banking" ) AND ( "information security" OR "cybersecurity" OR "cyber security" OR "data protection" OR "secure transaction" OR "information security risk" OR "security threat" OR "fraud*" OR "hack*" ) ) AND PUBYEAR > 2013 AND PUBYEAR < 2025 AND NOT AUTHLASTNAME ( "" ) AND ( LIMIT-TO ( SUBJAREA , "COMP" ) OR LIMIT-TO ( SUBJAREA , "BUSI" ) OR LIMIT-TO ( SUBJAREA , "SOCI" ) OR LIMIT-TO ( SUBJAREA , "ENGI" ) OR LIMIT-TO ( SUBJAREA , "MATH" ) OR LIMIT-TO ( SUBJAREA , "DECI" ) OR LIMIT-TO ( SUBJAREA , "ECON" ) ) AND ( EXCLUDE ( PREFNAMEAUID , "Undefined" ) ) AND ( LIMIT-TO ( LANGUAGE , "English" ) ) AND ( EXCLUDE ( DOCTYPE , "tb" ) OR EXCLUDE ( DOCTYPE , "no" ) )

**Data Source & Search Strategy**

To conduct a comprehensive bibliometric analysis on the intersection of FinTech and cybersecurity, data was extracted from Scopus, a widely recognized database for high-quality scholarly publications. Scopus was chosen due to its extensive coverage of peer-reviewed articles, conference proceedings, and book chapters across multiple disciplines. This database provides structured metadata, including citation counts, author affiliations, and keyword indexing, which are crucial for mapping research trends and identifying influential studies in FinTech security. By leveraging these authoritative sources, the study ensures the reliability and relevance of the collected literature.

The strategy of searching for data required creating a complex search string to combine a series of keywords alongside Boolean logic operators to narrow down the search. The formulation of the search string included a wider array of terms associated with FinTech such as “financial technology,” “digital banking,” or even “decentralized finance (DeFi)” along with other cybersecurity terms like “cybersecurity”, “data protection”, “secure transaction”, etc. These keywords were interconnected through the usage of AND/OR operators to ensure a range of different views pertaining to research were cited while also capturing studies that talk about both, FinTech and cybersecurity. Other edits to the search query included filtering the results by particular subject areas, including computer science (COMP), business (BUSI), social sciences (SOCI), engineering (ENGI), mathematics (MATH), decision sciences (DECI), and economics (ECON). In turn, this ensures only literature relevant to the study is included while mitigating publications that do not add value towards the study’s objectives.

The search was restricted to studies published in the period of 2014 and 2024 to identify recent developments in FinTech and cybersecurity for inclusion and exclusion criteria. To keep consistency in data analysis and interpretation only English language publications were considered. On top of that, any publication without an identifiable name of the author was removed to retain proper citation and credibility. In addition, publications outside the target subject areas were filtered to ensure the dataset focused on few meaningful subject areas. Through applying these criteria, the bibliometric analysis ensures that the dataset consists of high quality, relevant studies that produce informative insights on research trends, influential contributions and gaps that are emerging in FinTech and cybersecurity.

## RESULTS AND DISCUSSION

Based on Table 1 below, this bibliometric analysis starts from 2014 to 2024, covering ten years of data for FinTech and Cybersecurity. Within this timeframe, 725 different sources, including journals, books, and conference proceedings have published 1102 documents. Clearly from the analysis, the field is expanding, according to the annual increase of 56.59 % of the publications which indicates exponential increase in academia. This means that the volume of the work completed in this area is relatively recent, as the average document age is only 2.48 years. Furthermore, the average documents per publication is 7.736, which shows the considerable value and significance these documents hold in the academic field.

In total, 3918 Keywords Plus (ID) and 2812 Author's Keywords (DE) document contents emphasize various topics studied in intersection between FinTech and cybersecurity. The analysis of authors has identified 3291 authors and 160 single-authored papers, showing the extent of collaboration in the research output for this field. In this interdisciplinary field, the average number of co-authors per document is 3.37, while international collaboration accounts for 26.65% of publication, which indicates the international scope of research in FinTech and cybersecurity is fairly expanding.

In relation to document types, most of the publications are conference papers (504) and journal articles (388), which showcases the significance of conferences in circulating cutting-edge research. There are also 171 book chapters, which are useful in the context of academic discourse. Other publication types consist of reviews (34), editorials (3), and a couple of notes (1) and conference papers (1). The small number of review papers published indicates that more comprehensive literature reviews would be beneficial in integrating existing knowledge and setting the pace for future research endeavours.

**Table 1**

*Bibliometric Main Information*

| Descriptions | Results |
|---|---|
| ***MAIN INFORMATION*** | |
| Timespan | 2014:2024 |
| Sources (Journals, Books, etc) | 725 |
| Documents | 1102 |
| Annual Growth Rate % | 56.59 |
| Document Average Age | 2.48 |
| Average citations per doc | 7.736 |
| **Descriptions** | **Results** |
| ***DOCUMENT CONTENTS*** | |

(continued)

| | |
|---|---|
| Keywords Plus (ID) | 3918 |
| Author's Keywords (DE) | 2812 |
| ***AUTHORS*** | |
| Authors | 3291 |
| Authors of single-authored docs | 160 |
| ***AUTHORS COLLABORATION*** | |
| Single-authored docs | 164 |
| Co-Authors per Doc | 3.37 |
| International co-authorships % | 26.65 |
| ***DOCUMENT TYPES*** | |
| Article | 388 |
| Book chapter | 171 |
| Conference paper | 505 |
| Editorial | 4 |
| Review | 34 |

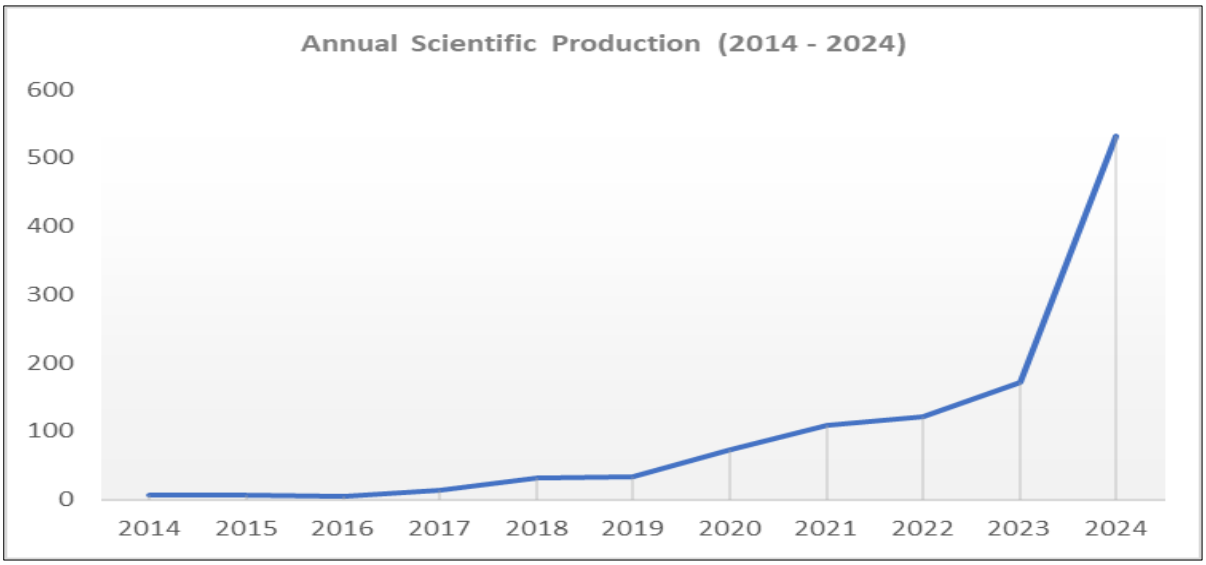
**Publication Trends (2014–2024)**

Cybersecurity and FinTech have been receiving considerable attention in the past decade, and in the past five years this attention has significantly increased. The period 2014 to 2016 was slow in terms of publishing with only 6 articles published in 2014 and 2015 and a decline to 4 in 2016. This reflects the initial phase of academic focus on the relation between technology in finance and cybersecurity because concerns regarding digital finances were emerging but no significant attention was directed towards it in academic literature. However, there was a striking increase to 14 articles in 2017 which marks the focus shift towards newer areas of research like digital payment systems, blockchain technology, and the cyber risks associated with them.

As of 2018, there was a noticeable increase in publications with research output reaching 31 articles in 2018 and 34 in 2019. This period indicates the growing academic and industrial attention towards FinTech solutions like mobile banking, cryptocurrency, and DeFi which also at the same time amplifies cybersecurity threats. Publications showed significant growth in 2020, when the number of studies doubled to 73, then to 109 in 2021, and subsequently 122 in 2022. This pattern coincides with global phenomena such as the COVID-19 pandemic which intensified the adoption of digital financial transactions and heightened cybersecurity risks, thus increasing the need for secure digital payment systems, fraud detection, and data protection measures. Figure 1 below illustrates the trend.

**Figure 1**

*Annual Scientific Production and Growth of Publications for 10 Years*




The period of 2023 to 2024 marked the increase in the research activities as publications surged from 172 in 2023 to an unprecedented 532 in 2024. This increment further stresses the importance of cybersecurity elements in FinTech considering the adoption of emerging technologies such as AI-empowered fraud detection systems, blockchain security, and also effective governance for digital finance. The staggering increase in research productivity during this time reflects the changing dynamics of academia and industry towards strengthening the defences of digital financial systems against advanced cyber threats. From these patterns, it can be inferred that the domains of FinTech and cybersecurity are likely to remain on the focus of research attention, which will determine the next frontier in digital financial security and innovation.

**Citation Impact Analysis**

As summarized by Table 2, from the years 2014 to 2024, the citation analysis of FinTech and cybersecurity reveals notable trends in the influence of publications. The average total citations attributed to each article (MeanTCperArt) shows pronounced variation from year to year suggesting differences in impact. The greatest impact from citations was in 2018 when each article received an average of 34.55 citations and in 2020, which had 27.00 citations per article. This demonstrates essential periods where research substantially impacted the industry.

Sustained impact of publications over time is indicated by the Mean Citations per Year metric (MeanTCperYear). The greatest mean citation frequency was noted in 2020 with 4.50 citations per year, demonstrating that works from this period continue receiving considerable attention. In parallel, 2018 (4.32 citations per year) and 2021 (3.70 citations per year) also show significant academic impact. However, the most recent publications from 2023 (2.15 citations per year) and 2024 (0.36 citations per year) indicate lower citation rates, which is reasonable considering the shorter window for citation accumulation.

**Table 2**

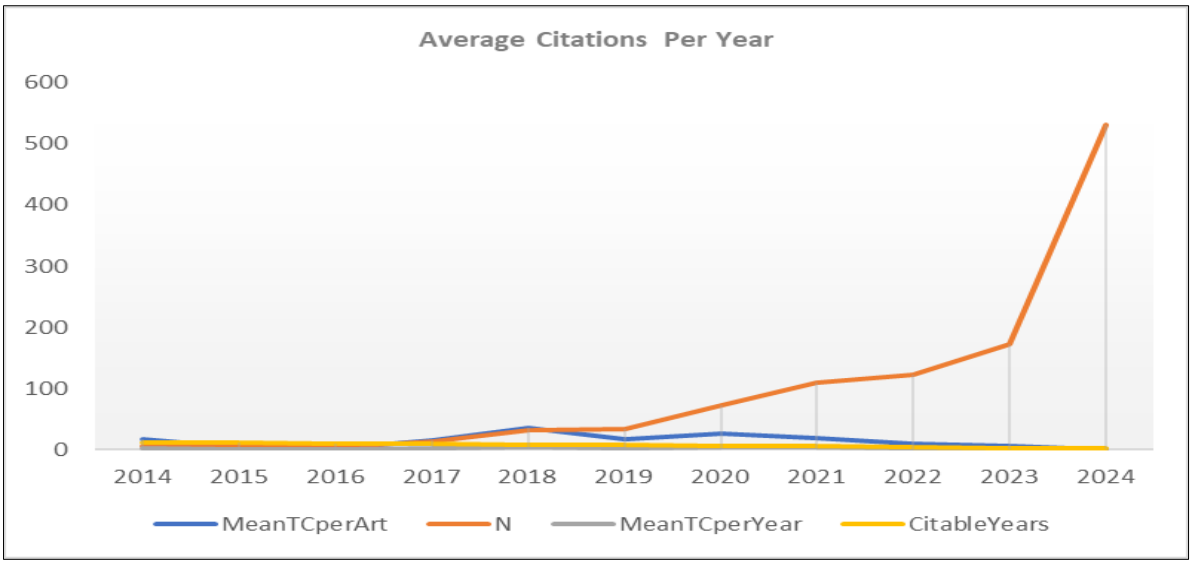
*Citations Data of FinTech and Cybersecurity*

| Year | MeanTCperArt | N | MeanTCperYear | Citable Years |
|---|---|---|---|---|
| 2014 | 16.83 | *6* | *1.40* | *12* |
| 2015 | 3.33 | *6* | *0.30* | *11* |
| 2016 | 1.50 | *4* | *0.15* | *10* |
| 2017 | 15.14 | *14* | *1.68* | *9* |
| 2018 | 34.55 | *31* | *4.32* | *8* |
| 2019 | 17.41 | *34* | *2.49* | *7* |
| 2020 | 27.00 | *73* | *4.50* | *6* |
| 2021 | 18.51 | *109* | *3.70* | *5* |
| 2022 | 8.66 | *122* | *2.16* | *4* |
| 2023 | 6.45 | *172* | *2.15* | *3* |
| 2014 | 0.71 | 532 | 0.36 | 2 |

Overall, the total number of publications has increased dramatically and hit a peak in 2024, with 532 articles published. Nevertheless, even though the volume of publications has increased, the average citation rate per article in 2024 is also very low, with only 0.71 citations per article indicating that many of these articles are likely awaiting citations. This assertion is supported by the citable years metric, which suggests older publications have had more time to accumulate citations. In essence, these observations can be interpreted as a sustained interest in FinTech and cybersecurity research, with peaks in scholarly focus during 2018 and 2020, while more recent publications are not yet being recognized widely in academia. Figure 2 below illustrates the trends.

**Figure 2**

*Citations vs Publications (2014 – 2024)*




Several factors can be attributed to the falling trend in citations especially in the more recent years from 2022 to 2024. Firstly, there has been a remarkable increase in publication volume which rose

dramatically in 2024 with a total of 532 articles published which means citations are more diluted across a larger number of studies. The more papers that are published in a particular time frame, the less individual citations a paper will receive because researcher focus gets spread over a wider selection of literature.

In addition, gathering citations for specific research areas such as this takes time. Publications from older years like 2018 and 2020 have had more time to be recognized and cited in other research works, for which they have been indeed prepared for a longer time. Articles from 2023 and 2024 on the other hand, are fairly new and their impact is yet to be fully understood. Many academic citations tend to happen after a few years due to the staggering pace at which studies get absorbed into the research ecosystem.

Besides, changing research concentration and saturation might be the influence as well. As FinTech and Cybersecurity research are dynamic fields, the earlier works may have been foundational and are considered as remarkably novel. In addition to that, intensifying competition among researchers means that more recent studies need to be more highly differentiated to make an impact, which is increasingly difficult given the rising volume of publications in this field.

**Most Influential Publications with High Citations**

From the analysis, it is found that there have been rapid developments within fraud identification technology, blockchain protection, and AI powered financial systems associated with Fintech and Cybersecurity. In the bibliometric analysis, the top ten published articles, inclusive of the most cited ones, offer a great deal of information on the crucial aspects of modern digital finance, fraud identification, digital security, and blockchain technology. Table 3 below summarizes the data.

**Table 3**

*The 10 Most Influential Publications & Citations*

| Authors | Year | Title | Source | Citations |
|---|---|---|---|---|
| Mosteanu, N. R., & Faccia, A | 2020 | Digital Systems and New Challenges of Financial Management – Fintech, XBRL, Blockchain and Cryptocurrencies | Quality – Access to Success | 154 |
| Ileberi, E., Sun, Y., & Wang, Z | 2021 | Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and Adaboost | IEEE Access | 111 |
| Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Luo, X., & Xu, G | 2021 | Trade Or Trick? Detecting And Characterizing Scam Tokens on Uniswap Decentralized Exchange | Proceedings of the ACM on Measurement and Analysis of Computing Systems | 74 |

(continued)

| Authors | Year | Title | Source | Citations |
|---|---|---|---|---|
| Mosteanu, N. R., & Faccia, A. | 2021 | Fintech Frontiers in Quantum Computing, Fractals, and Blockchain Distributed Ledger: Paradigm Shifts and Open Innovation | Journal of Open Innovation: Technology, Market, and Complexity | 69 |
| Emara, N., & Zhang, Y. | 2021 | The Non-Linear Impact of Digitization on Remittances Inflow: Evidence from The BRICS A Framework for Enhancing Cyber Security in Fintech Applications in India | Telecommunications Policy Proceedings of International Conference on Technological Advancements and Innovations, ICTAI 2021 | 39 |
| Tian, M. W., Wang, L., Yan, S. R., Tian, X. X., Liu, Z. Q., & Rodrigues, J. J. P. | 2019 | Research On Financial Technology Innovation and Application Based On 5G Network | IEEE Access | 33 |
| Faccia, A., Moşteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. | 2020 | Electronic Money Laundering, The Dark Side of Fintech: An Overview of The Most Recent Cases | ACM International Conference Proceeding Series | 27 |
| Eltweri, A., Faccia, A., & Khassawneh, O. | 2021 | Applications Of Big Data Within Finance: Fraud Detection and Risk Management Within the Real Estate Industry | ACM International Conference Proceeding Series | 15 |
| Ma, S., Guo, C., Wang, H., Xiao, H., Xu, B., Dai, H. N., ... & Wang, T. | 2018 | Nudging Data Privacy Management of Open Banking Based on Blockchain | Proceedings - 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018 | 11 |
| Dai, W., Wang, Q., Wang, Z., Lin, X., Zou, D., & Jin, H. | 2021 | Trustzone-Based Secure Lightweight Wallet for Hyperledger Fabric | Journal Of Parallel and Distributed Computing | 10 |
| Mosteanu, N. R., & Faccia, A | 2020 | Digital Systems and New Challenges of Financial Management – Fintech, XBRL, Blockchain and Cryptocurrencies | Quality – Access to Success | 154 |

Based on Table 3, the analysis has revealed key area contributions of these influential publications. The discussion are as follows:

***Digital Financial Systems and Emerging Technology***

The most cited work on the list is Mosteanu & Faccia (2020) with "Digital Systems and New Challenges of Financial Management – FinTech, XBRL, Blockchain and Cryptocurrencies", which has 154 citations. This paper discusses the merging of digital finance systems with blockchain, cryptocurrencies, and XBRL, incorporating other issues pertaining to modern regulatory and security management in finance. Another of their works, "FinTech Frontiers in Quantum Computing, Fractals, and Blockchain Distributed Ledger" published in 2021, had 69 citations, discusses the utilization of quantum computing in financial technology, focusing on how distributed ledger technology (DLT) and fractal mathematics will define the future of FinTech.

***AI and Machine Learning for Fraud Detection***

Ileberi, Sun, & Wang Z (2021) significantly advanced AI-driven fraud detection with their work, "Performance Evaluation of Machine Learning Methods for Credit Card Fraud Detection Using SMOTE and AdaBoost," which received 111 citations. This study examines the use of machine learning for fraud detection and proves that the application of the Synthetic Minority Over-sampling Technique (SMOTE) and AdaBoost algorithms enhances fraud detection accuracy. It remains one of the most impactful contributions in AI-based financial security.

Also, in Eltweri, Faccia, & Khassawneh (2021) focus on the real estate sector in their paper "Applications of Big Data Within Finance: Fraud Detection and Risk Management Within the Real Estate Industry" (15 citations), highlighting the importance of big data in detecting financial fraud in real estate and financial systems.

***Blockchain and Cryptocurrency Fraud Prevention***

Cryptocurrency scams and other security risks are a rising issue in decentralized finance (DeFi). The research by Xia et al. (2021), with more than 74 citations titled "Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange" offers a deep dive into the analysis of various tokens designed to defraud users within the Uniswap ecosystem. Utilizing blockchain surveillance and security audit of smart contracts blockchain enhances the level of fraud and scam prevention in DeFi trading.

Another piece of research concerning blockchain security is by Ma et al. (2018), ''Nudging Data Privacy Management of Open Banking Based on Blockchain'', which has garnered 11 citations, concentrates on the management of privacy in open banking architecture based on blockchains and takes a step further by proposing a model of virtually unidentifiable transactions.

***Cybersecurity and Trust in Financial Systems***

Multiple works in this list emphasize the security concerns in digital finance systems. Emara & Zhang (2021) contribute to this discourse in their paper "The Non-Linear Impact of Digitization on Remittances Inflow: A Framework for Enhancing Cybersecurity in Fintech Applications in India" (39 citations) and offer a unique cybersecurity framework for the protection of digital remittance platforms.

At the same time, Dai et al. (2021) focus on blockchain technology in their paper "TrustZone-Based Secure Lightweight Wallet for Hyperledger Fabric" (10 citations), where they concentrate on the improvement of blockchain wallet security by implementing ARM TrustZone technology which provides secure execution of cryptographic operations.

***Money Laundering and Financial Crimes Prevention***

The prevention and detection of financial crime stands out among the challenges in FinTech. In "Electronic Money Laundering: The Dark Side of FinTech – An Overview of the Most Recent Cases," Faccia et al. (2020) focuses on actual instances of digital money laundering and offers insights on risk management through regulatory compliance with AI detection systems (27 citations).

**Keyword Analysis & Emerging Themes**

The Figure 3 below is a word cloud diagram that illustrates themes and areas of focus concerning the intersection of financial technology and cybersecurity. Terms like "decentralized finance," "blockchain," "fraud detection," "network security," and "machine learning" underscore both the expanding scope of digital financial systems and the security issues associated with them. Focus on "cybersecurity," "crime," "risk evaluation," and "data privacy" indicates attention on protecting financial activities from cyber-related dangers. Also, "fintech," "cryptography," "deep learning," and "artificial intelligence" suggest the use of other specific technologies to strengthen financial security and fraud deterrence. The diagram captures the balance between current research focus areas, technological shifts, and regulation activities defining the evolution of safely managed digital financial resources.

**Figure 3**

*The Word Cloud*


The word cloud captures the most important issues in relation to FinTech and security issues. The term "decentralized finance", the most dominating word in the cloud, depicts another aspect of the concern where the DeFi systems are increasingly adopted in the development and transformation of financial service systems using blockchain technology, smart contracts, and distributed ledgers. Words like "fraud detection", "crime", and "cybersecurity" indicate growing concerns towards managing risk in

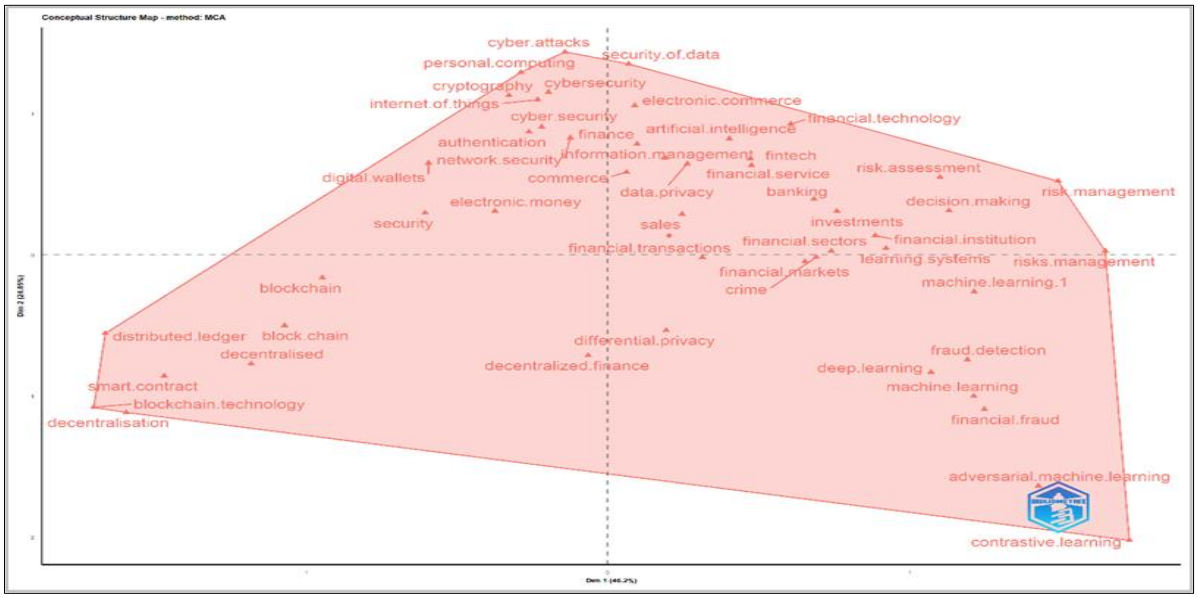
digital financial transactions. The addition of "machine learning", "deep learning" and "adversarial machine learning" suggests the application of AI to the detection of fraud and risk management is also growing. The word cloud also presents "network security", "cryptography" and "authentication", showing the role of safeguarding data within the FinTech areas. All in all, this visualization demonstrates the merging of the development of blockchain technology, AI, and cybersecurity and their impact on the efficiency and security of digital financial ecosystems.

**Network Visualization of Co-occurrence of Key Emerging Topics**

The Conceptual Structure Map (Figure 6) below summarizes and visualizes the major themes of research and their links within financial technology, cybersecurity, blockchain, and fraud detection. The visualization indicates two main conceptual clusters. The left cluster focuses on blockchain and decentralization featuring "blockchain", "smart contract", "distributed ledger", and "decentralized finance". This cluster underlines that blockchain technology enables and supports secure, transparent, and decentralized financial transactions. The high level of interest in smart contracts and distributed ledger systems points out that there are ongoing attempts to build more secure financial systems without the need for centralized control.

**Figure 4**

*The Conceptual Structure Map*




The AI-driven fraud detection and risk management cluster on the right encapsulates "machine learning", "deep learning", "fraud detection", "financial fraud", and "adversarial machine learning". To begin with, this area defines the use of artificial intelligence with regard to driving fraud detection, within the financial risks, and mechanized decisions by financial institutions. Signals of "AI being used for fraud prevention and evolved risk evaluation" probability is in proximity (within the finance domain) of terms "risk management", "decision making", and "financial institutions". In addition to that, the concepts of cybersecurity such as "authentication," "network security," "privacy of data," and "secured data" sit in the middle to emphasize how crucial it is for protection of financial transactions and to avoid cyberattacks.

The map also includes new innovations and innovative uses of “artificial intelligence”, “Internet of Things (IoT)”, and “electronic commerce”. In these, too, AI and blockchain technologies are being used to improve the security of digital transactions more and more extensively, not limited to financial services. Furthermore, including ‘financial crime’, ‘risk assessment’, and ‘financial institutions’ in the map imply the importance of fraud mitigation strategies on a preventive aspect in this matter. To sum up, the map shows that there is a clear delineation between the decentralization systems of blockchain, the AI-powered fraud detection, and cybersecurity, which serves as a critical integrative component. These technologies will transform the future of finances making them secure, efficient, and intelligent.

Overall, this Conceptual Structure Map illustrates the interplay of FinTech, cybersecurity, DeFi, and blockchain. The role of security and privacy in digital finance is fundamental, and as an AI technology, solutions are becoming more prominent. In addition, considerations of financial regulations and ethics continue to be of importance, which shows that the development of FinTech must balance technological progress with governance policies.

## CHALLENGES AND FUTURE RESEARCH DIRECTIONS

The domain of cybersecurity and FinTech integrates a number of complexities that slows down the growth of secure, adaptable financial technologies. The rapid speed of technology development is one of the main challenges that makes existing research irrelevant even after a wide implementation is deployed. The advancements in blockchain, AI, and even digital finance are progressing at such a rapid pace that security frameworks are unable to keep up. At the same time, the growing sophistication of financial systems creates new and extensive security threats, including cyber-attacks, data theft, and various forms of fraud. The indifferent of global financial regulatory and compliance from one jurisdiction to another also creates further complication in establishing the mutually agreed uniform protective criteria for digital financial services.

There are promising research avenues that can broaden the security and resiliency of FinTech. Fraud detection is one major area where AI is being applied. Using predictive analytics with machine learning can detect fraudulent transactions as they happen. AI has the potential to enhance the development in cybersecurity to improve threat detection, assessment, and anomaly detection that can significantly solve the issues of financial crimes in FinTech. Other than that, as DeFi platforms become more popular, people are more vulnerable to hacking, phishing, and smart contract exploits. Understanding of the risk in this domain can help in the adoption of appropriate protection measures to ensure DeFi applications and users are secure in this area.

Privacy in financial technologies also could be of interest for future research in this area. With governments and organizations becoming more stringent when it comes to their data protection and security policies, like the GDPR, it is important for financial systems to strike a balance between innovation with privacy and security. In this case, there is a need for further research, particularly on regulatory of technology solutions like AI and blockchain on financial institutions.

## CONCLUSION

This bibliometric study offers an understanding of the trends in the field of FinTech and cybersecurity research. This study shows the growing concern in the industry and academia by analyzing trends of publications, influential authors, key journals, and co-occurrence networks of key topics related to the subjects. The results show that there has been an increasing trend in publications over the years, which demonstrates that FinTech are increasingly focusing on areas such as cybersecurity, blockchain security, fraud detection, and compliance to regulations. This study has found the greatest contributions were made from the most cited articles focused on new technologies which include artificial intelligence-based protection systems, decentralized finance (DeFi), and other privacy-enhancing techniques which are suggested as the next frontiers that need to be addressed with innovation without compromising security in financial systems. The bibliometric analysis of the literatures covered in this study was extensive; however, the single database utilized and the choice of only English literature posed limitations. Subsequent studies could adopt a multi-database approach and include analysis from other disciplines associated with FinTech and cybersecurity. In general, this analysis helps understand the development of research in this area and how academics, decision makers, and professionals can build stronger and secure financial technologies to enhance their strategies actively.

## ACKNOWLEDGMENT

We would like to thank the Faculty of Information Science, the UiTM's Research Management Center (RMC), the ARI, and the Tun Abdul Razak Library (UiTM) for the support of this research.

## REFERENCES

Adelaja, A. O., Umeorah, S. C., Abikoye, B. E., & Nezianya, M. C. (2024). Advancing financial inclusion through fintech: Solutions for unbanked and underbanked populations. *World Journal of Advanced Research and Reviews, 23*(01), 427-438.

Alt, R., Beck, R. & Smits, M. T. (2018). FinTech and the transformation of the financial industry. *Electron Markets, 28,* 235–243. https://doi.org/10.1007/s12525-018-0310-9

Belanche, D., Casaló, L. V., & Flavián, C. (2019). Artificial Intelligence in FinTech: Understanding robo-advisors adoption among customers. *Industrial Management & Data Systems, 119*(7), 1411-1430.

Bollinger B., & Yao, S. (2018). Risk transfer versus cost reduction on two-sided microfinance platforms. *Quant Mark Econ 16,* 251–287.

Busayatananphon, C., & Boonchieng, E. (2022). *Financial Technology DeFi Protocol: A Review*. 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunications Engineering (ECTI DAMT & NCON), Chiang Rai, Thailand, 2022, pp. 267-272. https://doi.org/10.1109/ECTIDAMTNCON53731.2022.9720373

Cai, C. W. (2018). Disruption of financial intermediation by FinTech: A review on crowdfunding and blockchain. *Accounting & Finance, 58*(4), 965-992.

Corbet, S., & Gurdgiev, C. (2017). Financial digital disruptors and cyber-security risks: Paired and systemic. *Forthcoming in Journal of Terrorism & Cyber Insurance, 1*(2).

Dai, W., Wang, Q., Wang, Z., Lin, X., Zou, D., & Jin, H. (2021). Trustzone-based secure lightweight wallet for hyperledger fabric. *Journal of Parallel and Distributed Computing, 149,* 66-75.

Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and Cyber Security in Fintech. In: Benković, S., Labus, A., Milosavljević, M. (Eds), *Digital Transformation of the Financial Industry*. Contributions to Finance and Accounting. Springer. https://doi.org/ 10.1007/978-3-031-23269-5_15

Eltweri, A., Faccia, A., & Khassawneh, O. (2021, December). *Applications of big data within finance: Fraud detection and risk management within the real estate industry*. In Proceedings of the 2021 3rd International Conference on E-Business and E-commerce Engineering (pp. 67-73).

Emara, N., & Zhang, Y. (2021). The non-linear impact of digitization on remittances inflow: Evidence from the BRICS. *Telecommunications Policy, 45*(4), 102112.

Faccia, A., Moşteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020, September). *Electronic money laundering, the dark side of fintech: An overview of the most recent cases*. In Proceedings of the 2020 12th International Conference on Information Management and Engineering (pp. 29-34).

Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). Security compliance and its implication for cybersecurity. *World Journal of Advanced Research and Reviews, 24*(01), 2105-2121.

George, A. S. (2023). Securing the future of finance: How AI, blockchain, and machine learning safeguard emerging neobank technology against evolving cyber threats. *Partners Universal Innovative Research Publication, 1*(1), 54-66.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems, 35*(1), 220–265. https://doi.org/10.1080/ 07421222.2018.1440766

Hossain, M. J., Rifat, R. H., Mugdho, M. H., Jahan, M., Rasel, A. A., & Rahman, M. A. (2022, November). *Cyber threats and scams in FinTech organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh*. In 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) (pp. 190-195). IEEE.

Ileberi, E., Sun, Y., & Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost. *IEEE Access, 9*, 165286-165294.

Jović, Ž., & Nikolić, I. (2022). The darker side of FinTech: the emergence of new risks. *Zagreb International Review of Economics & Business, 25*(SCI), 46-63.

Kaur, G., Habibi Lashkari, Z., Habibi Lashkari, A. (2021). Cybersecurity threats in FinTech. In *Understanding cybersecurity management in FinTech. Future of business and finance*. Springer. https://doi.org/10.1007/978-3-030-79915-1_4

Kumari, A., & Devi, N. C. (2022). The impact of fintech and blockchain technologies on banking and financial services. *Technology Innovation Management Review, 12*(1/2).

Lee, C. C., Li, X., Yu, C. H., & Zhao, J. (2021). Does fintech innovation improve bank efficiency? Evidence from China's banking industry. *International Review of Economics & Finance, 74*, 468-483.

Ma, S., Guo, C., Wang, H., Xiao, H., Xu, B., Dai, H. N., ... & Wang, T. (2018, October). *Nudging data privacy management of open banking based on blockchain*. In 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks (I-SPAN) (pp. 72-79). IEEE.

Mosteanu, N. R., & Faccia, A. (2020). Digital systems and new challenges of financial management–FinTech, XBRL, blockchain and cryptocurrencies. *Quality–Access to Success, 21*(174), 159-166.

Mosteanu, N. R., & Faccia, A. (2021). Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation. *Journal of Open Innovation: Technology, Market, and Complexity, 7*(1), 19.

Ng, A. W., & Kwok, B. K. B. (2017). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance, 25*(4), pp. 422-434. https://doi.org/10.1108/JFRC-01-2017-0013

Palmié M., Wincent J., Parida V., & Caglar, U. (2020). The evolution of the financial technology ecosystem: An introduction and agenda for future research on disruptive innovations in ecosystems. *Technol Forecast Soc Chang, 151*, 119779.

Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing, 14*(3), 01-16.

Renduchintala, T., Alfauri, H., Yang, Z., Pietro, R. D., & Jain, R. (2022). A survey of blockchain applications in the fintech sector. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(4), 185.

Salampasis, D., & Mention, A. L. (2018). FinTech: Harnessing innovation for financial inclusion. In *Handbook of blockchain, digital finance, and inclusion* (Volume 2, pp. 451-461). Academic Press.

Șcheau, M. C., Rangu, C. M., Popescu, F. V., & Leu, D. M. (2022). Key pillars for FinTech and cybersecurity. Acta Universitatis Danubius. *Œconomica, 18*(1).

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

Takeda, A., & Ito, Y. (2021). A review of FinTech research. *International Journal of Technology Management, 86*(1), 67-88.

Tian, M. W., Wang, L., Yan, S. R., Tian, X. X., Liu, Z. Q., & Rodrigues, J. J. P. (2019). Research on financial technology innovation and application based on the 5G network. *IEEE Access, 7*, 138614-138623.

Umoga, U. J., Sodiya, E. O., Amoo, O. O., & Atadoga, A. (2024). A critical review of emerging cybersecurity threats in financial technologies. *International Journal of Science and Research Archive, 11*(1), 1810-1817.

Varga, D. (2017). Fintech, the new era of financial services. *Vezetéstudomány-Budapest Management Review, 48*(11), 22-32.

Vives, X. (2017). The impact of FinTech on banking. *European Economy, 2*, 97-105.

Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Luo, X., ... & Xu, G. (2021). *Trade or trick? detecting and characterizing scam tokens on Uniswap decentralized exchange*. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 5(3), 1-26.