ICMEB

Proceeding of the International Conference on Management, Entrepreneurship, and Business

E-ISSN: 3090-9155

Research Article

Bibliometric Analysis of The Global Research Landscape in Financial Cybersecurity

Akastya Choirun Nisa [1,*], Istia Dwi Pitaloka[2], Novita Sari[3]

[1,2,3] Universitas Negeri Semarang; e-mail : akastya@students.unnes.ac.id
* Corresponding Author : Akastya Choirun Nisa

Abstract: The digital era has driven change in the financial sector through FinTech, but it has also made it vulnerable to increasingly sophisticated cyber threats. These escalating risks have triggered a surge in academic research, demanding a comprehensive understanding of how it works. This study aims to examine the development of cybersecurity research in the financial sector globally. Using bibliometrics, this study analyzes literature data sourced from the Scopus database over the past five years. The VOSviewer and RStudio analysis tools were used to identify dominant clusters, where cybersecurity and network security are the core connecting various sub-fields such as artificial intelligence, cyber attacks, and phishing. This research serves as a guide for researchers and workers in this field. The results show which areas have been extensively researched and which areas are still 'blank' or require further research.

Keywords: Cybersecurity; Fintech; Bibliometric; Vosviewer

1. Introduction

The development of financial technology (FinTech) and the expansion of digital banking have driven significant innovations in the digital transformation of the financial sector. These advancements, while offering greater efficiency and accessibility, simultaneously expose the industry to an increasingly sophisticated and dangerous spectrum of cyber threats. Consequently, the financial sector has become a prime target for cybercriminals, who utilize various attack methods, such as phishing, malware, and ransomware, to cause large-scale financial losses and erode public trust (Akhta et al., 2021). This paradox of digital transformation—where technological progress inherently creates new vulnerabilities—has fundamentally altered the perception of risk. Cyber threats are no longer viewed as isolated technical incidents but rather as a source of systemic risk with the potential to disrupt market stability and damage the foundation of trust upon which the entire financial system is built.

As the volume and sophistication of cyber threats increase, cybersecurity has transformed from a mere technical issue into a vital component of boardroom strategy. This perspective is widely recognized by regulators, practitioners, and academics as the foundation for maintaining the stability of the global financial ecosystem (Calderaro & Craig, 2020). Faced with these challenges, researchers are intensively investigating various technological solutions to strengthen cyber defenses in the financial sector. Among the various areas of research, the application of artificial intelligence (AI) and machine learning (ML) for real-time fraud detection and predictive analysis of transaction anomalies is one of the most dominant (Nweze et al., 2024). In addition, blockchain technology, which was initially considered a decentralized security fortress, is now being studied more deeply to identify its potential vulnerabilities. Research also focuses not only on technology but also on the urgency of developing adaptive risk management frameworks and solid security governance to respond to ever-changing threats. Collectively, these studies confirm that financial cybersecurity is a complex multidisciplinary domain that requires the integration of advanced technological solutions with robust management strategies and policies.

Received: date
Revised: date
Accepted: date
Published: date
Curr. Ver.: date

Although research on these specific topics has developed significantly, there is still an urgent need to understand the structure, trends, and dynamics of the financial cybersecurity research landscape holistically. Bibliometric analysis is an effective quantitative method for mapping the intellectual evolution of a field, identifying influential researchers and institutions, and highlighting emerging or under-explored areas of research. By analyzing large-scale publication data, bibliometric studies are able to provide a macro perspective that is difficult to achieve through conventional narrative literature reviews. Therefore, this study is designed to fill this gap by presenting the first comprehensive bibliometric analysis in the field of financial cybersecurity. This study provides a comprehensive mapping of global research trends by applying bibliometric analysis methods to publication data from the Scopus database for the period 2016-2023. The aim is to present a visualization that maps key trends, key concepts, and interrelationships between studies, thereby providing a strategic foundation for researchers and practitioners to identify critical research gaps and formulate future research agendas.

Overall, rapid technological innovation in the financial sector has brought about efficiency gains while creating cyber risks that are now systemic and threaten financial stability. Although much research has focused on specific technological solutions such as artificial intelligence and risk management frameworks, a comprehensive understanding of the structure and evolution of the overall financial cybersecurity research landscape is still lacking. To address this gap, this study will apply bibliometric analysis methods to quantitatively map global research trends.

2. Preliminaries or Related Work or Literature Review

Bibliometric analysis provides an objective quantitative framework. This method is essentially a study of academic publications that utilizes statistical tools (Ninkov et al., 2022) and quantitative analysis to visualize the characteristics and trends of publishing (Maggio et al., 2021). Its purpose goes beyond simply counting the number of publications; it aims to capture the dynamics of a discipline's evolution, discover emerging research areas, evaluate the current status, and map the structure of knowledge holistically. By analyzing citation patterns, collaboration networks between researchers, and thematic relationships, this approach provides an in-depth picture of the research landscape, which is very useful for highlighting established areas as well as finding research gaps that require further attention, making it a popular and systematic approach to investigating large volumes of scientific data (Donthu et al., 2021). This method offers a strong empirical foundation that can be used to position their scientific contributions more strategically within the existing research landscape. With this deep understanding, they can not only highlight the novelty of their research but also effectively map out prospective collaboration networks. Ultimately, this facilitates the development of a future research roadmap that is not only relevant to current trends but also has a greater chance of generating a broad and meaningful impact on the development of science.

Conceptually, financial cybersecurity can be understood as efforts to protect financial systems from various cyber threats that have the potential to create systemic vulnerabilities. Cybersecurity in this context is seen as part of cybersecurity hazards that directly threaten the stability, data integrity, and operational continuity of financial institutions (Uddin et al., 2018). Along with FinTech innovation, cybersecurity has also become a crucial response needed to protect institutions from digital crime through solid policies and effective mitigation technologies (Al Duhaidahawi et al., 2021). From a macro risk perspective, this concept is defined as the potential for attackers to disrupt information technology systems, which in turn can damage public trust and financial stability in general, thus requiring a more robust regulatory framework (Adelmann et al., 2020). Collectively, these various definitions highlight four key elements: the existence of cyber threats, the existence of vulnerabilities in the system, the potential impact on operations and stability, and the importance of mitigation components through policy, technology, and oversight. Similarly, another view emphasizes that cybersecurity in the financial sector is a technical, organizational, and regulatory protection effort against threats that could undermine stability, where attacks on vital financial infrastructure risk disrupting market operations and public confidence, thus requiring international cooperation for mitigation (Maurer & Nelson, 2021).

Overall, this literature review confirms that bibliometric analysis serves as a tool to visualize the intellectual structure and evolving trends within a scientific discipline. Its application in the context of financial cybersecurity—a crucial domain for safeguarding the

financial system's stability from cyber attacks—enables the identification of scholarly dynamics, researcher connections, and unexplored research areas. This insight provides a strong, evidence-based foundation for formulating effective mitigation strategies by integrating policy, technology, and regulation, thereby ensuring operational integrity and maintaining public trust.

3. Proposed Method

This study began with a systematic literature search on the Scopus database, which was then followed by a document evaluation process through three structured phases as illustrated in (Figure 1): (Phase 1) focused on data collection by establishing specific search criteria to identify and filter relevant records; Next, in (phase 2), the collected documents were visualized using VOSviewer software for in-depth bibliometric analysis, which included publication trends, collaboration networks, and field mapping; and (Phase 3) was a qualitative analysis to explore and identify the main research themes and trends discussed by academics in the field of cybersecurity in the financial sector.

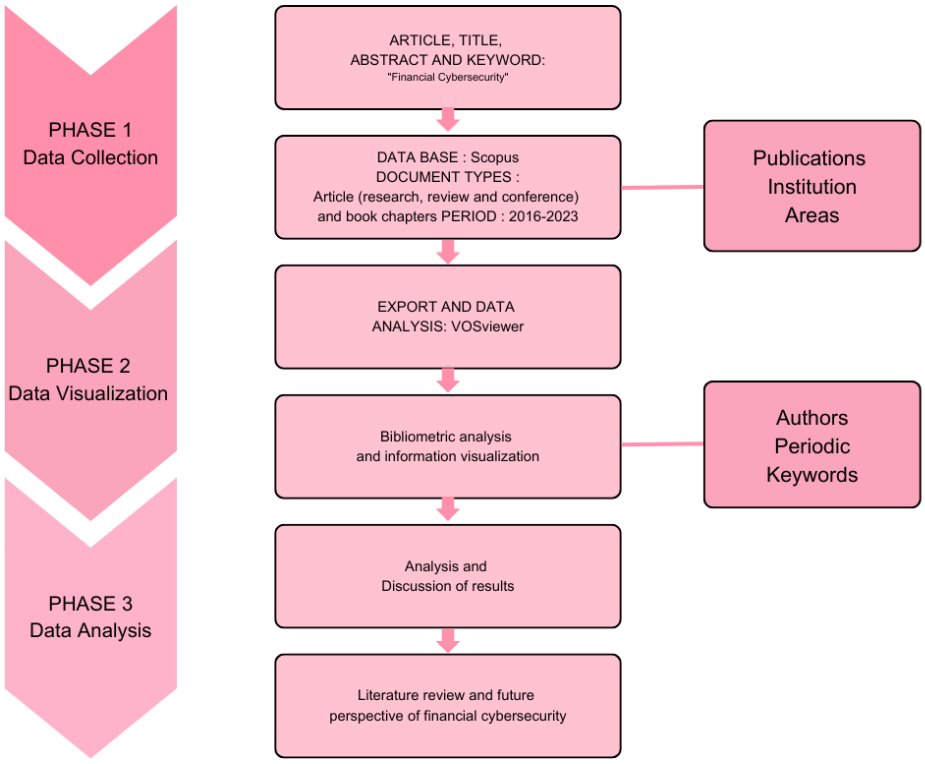

Figure 1. Methodology phases applied to the present work.

The first step in this study was to systematically identify relevant literature. This process was carried out by focusing on the titles, abstracts, and keywords of various publications, using the search term "financial cybersecurity" to ensure accurate results. Data collection was carried out exclusively through the Scopus database, which was used as the sole source. The criteria set included various types of documents, such as research articles, review articles, and conference proceedings published between 2016 and 2023, taking into account the publishing institutions. To ensure that no relevant literature was overlooked, a total sampling method was applied, in which all documents that met the criteria were included in the study.

After all raw data had been successfully collected, the process continued with importing the complete data set into VOSviewer software (version 1.6.19) for further analysis. This tool was used to conduct in-depth bibliometric analysis and create data visualizations to map the intellectual landscape of this field. The analysis included mapping the collaboration network between authors, the distribution of scientific contributions from various countries, and the identification of the most influential journals. The results of these visualizations, both qualitative and quantitative, were then thoroughly examined to interpret the patterns found and conclude the main findings. As a final step, all analysis results were synthesized to compile a comprehensive literature review and formulate a future research agenda for the field of financial cybersecurity.

4. Results and Discussion

Bibliometric research for the period 2016-2023 indicates an extraordinary level of research productivity. During this period, 1,450 scientific articles were published in 473 different sources, with contributions from 7,452 authors. One of the most notable data points is the annual growth rate, which reached 49.02%. This rapid growth shows that this field of study is undergoing major expansion, attracting the attention of academics and practitioners around the world, while also signaling the relevance and urgency of its research topics.

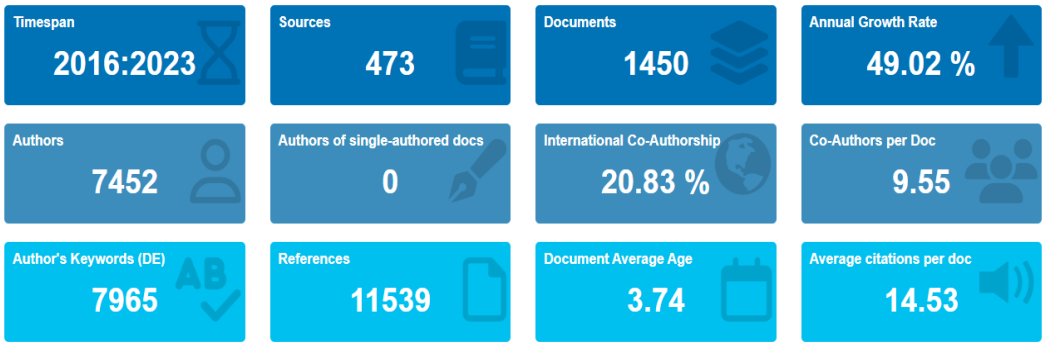

Figure 2. Main information overview (using R Studio).

The most interesting thing is that there were no publications with a single author, emphasizing the multidisciplinary nature and complexity of the research topics, which require team collaboration. On average, each publication was authored by 9.55 authors, a figure that significantly exceeds the average in other disciplines and indicates a high intensity of collaboration. Furthermore, this collaboration is global in nature, with 20.83% of all publications being the result of collaboration between researchers from different countries, proving that the scientific network in this field is extensive and diverse. In terms of scientific influence and impact, research in this area has remarkable visibility. Each article is cited an average of 14.53 times, reflecting that the work produced is recognized, utilized, and further developed by the research community. The theoretical foundation of this research is also strong, as evidenced by the use of a total of 11,539 references in all documents analyzed. Furthermore, the average age of publications, which is only 3.74 years, implies that the literature in this field is very new and filled with the latest discoveries, confirming its status as a relevant and dynamic area of research.

The detailed line graph provides a quantitative overview of Annual Scientific Output in a specific academic field. In this visualization, the vertical axis (Y) measures the number of articles published, which serves as a direct measure of research output, while the horizontal axis (X) systematically maps this production over a specific period of time starting in 2016 and ending at the end of the observation period, around 2023. The main trend shown is a clear and robust positive growth in the volume of scientific literature throughout the entire period analyzed. This consistent upward trend indicates a sustained and rapid increase in research activity, suggesting that the field of study has gained significant momentum and academic attention.

A more detailed chronological analysis of the data reveals a non-linear pattern of development, marked by a clear acceleration in the rate of scientific production over time. This period began in 2016 with relatively low output, recording fewer than 50 articles. Following this initial stage, the years leading up to 2019 were marked by a phase of moderate and gradual growth. However, 2020 appears to have been a crucial turning point, initiating a period of much sharper growth in publication rates. This acceleration became most pronounced after 2022, when the number of publications skyrocketed exponentially, increasing dramatically to reach a peak of 500 articles. The exponential pattern in recent years strongly supports the conclusion that this field has transitioned from a niche area of interest to a large and rapidly growing academic domain, attracting significant investment and academic effort.

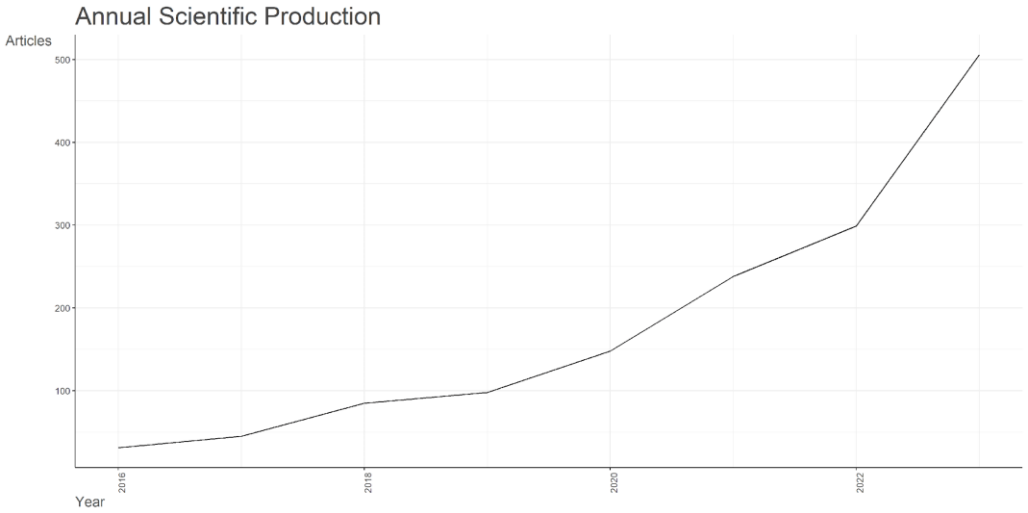

Figure 3. Annual Scientific Production (using R Studio).

Figure 4 shows a line graph titled Average Citations per Year, which illustrates in depth the volatility in the average annual citation figures throughout the period from 2016 to 2023. A thorough review of the data reveals a highly dynamic and unpredictable narrative, marked by sharp fluctuations between annual data points. This characteristic strongly indicates the absence of any identifiable linear trend; the data shows neither a sustained growth nor a consistent decline, making long-term forecasting challenging.

This period began with promising initial growth, rising from around 2.85 citations in 2016 to 3.15 in 2017. However, this optimism quickly faded due to an unexpected sharp contraction that brought the citation rate to its lowest point of around 2.55 in 2018. From this low point, there was a remarkable rebound and significant surge to around 3.55 citations in 2019. After experiencing a minor setback to 3.50 in 2020, the positive trend resumed and pushed the average citation rate to its peak of around 3.65 in 2021. However, this peak was immediately followed by a significant decline to around 2.77 citations in 2022. This series of events clearly underscores the highly volatile nature of the data, where periods of rapid expansion can quickly give way to periods of equally deep contraction.

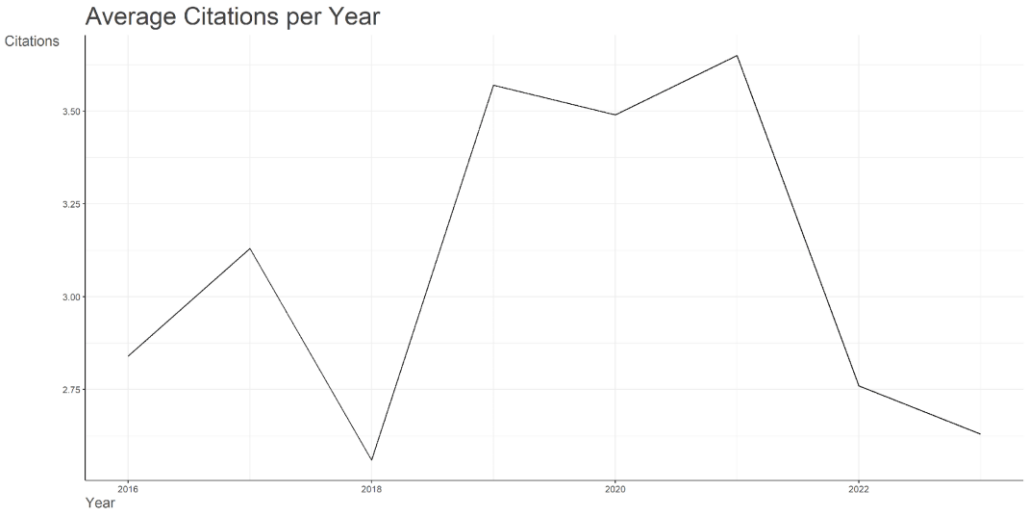

Figure 4. Average Citations per Year (using R Studio)

Figure 5 shows that the provided image displays a chart titled Most Relevant Sources, which ranks academic publication sources based on the number of documents published. This horizontal bar graph lists the names of sources, such as journals, conference proceedings, or book series, on the vertical (Y) axis, while the horizontal (X) axis indicates the total number of documents. The most significant finding from this visualization is the existence of one exceptionally dominant, though unnamed, publication source. This top-ranked source is

credited with publishing 556 documents, a figure that drastically surpasses all other listed sources, identifying it as the primary outlet for research in the analyzed field.

Below this dominant source, a number of other relevant publications are listed, each with a substantially smaller yet important contribution. Lecture Notes in Networks and Systems ranks next with 28 documents, followed by Lecture Notes in Computer Science with 25 documents, IEEE Access with 23, and the ACM International Conference Proceeding Series with 20. Other sources on the list have contributions of fewer than 20 documents. This distribution pattern indicates that while knowledge on this topic is heavily concentrated in a single primary source, it is also widely disseminated across various secondary publication types, including lecture note series, reputable journals, and international conference proceedings.

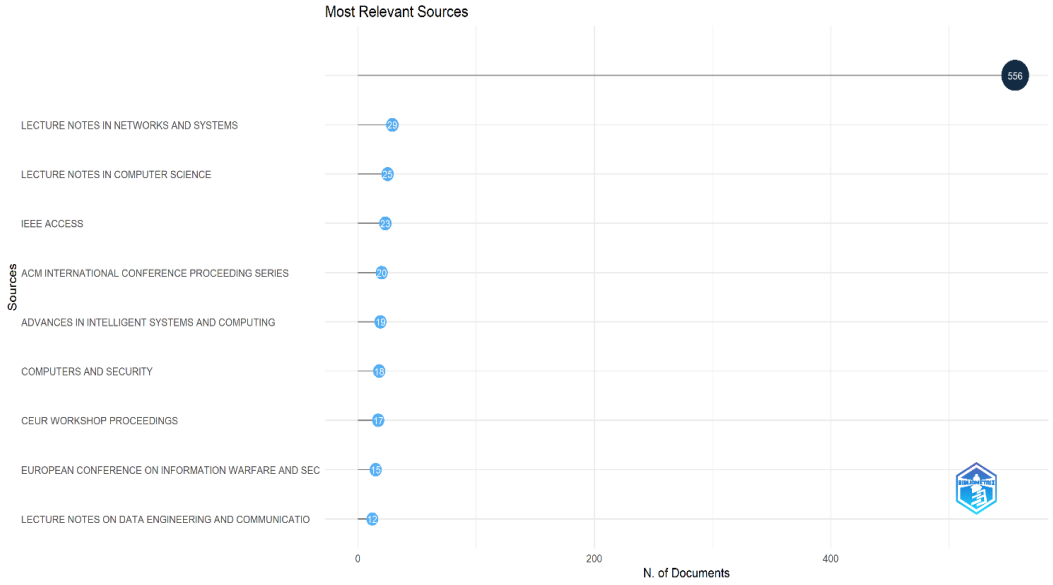

Figure 5. Most Relevant Sources (using R Studio).

Figure 6 shows a visual mapping of research keywords that clearly places "cybersecurity" as the most prominent core concept in scientific discourse, as evidenced by its superior node size. Surrounding this core concept is a constellation of other closely related keywords, such as "network security," "computer crime," and "internet of things." This dense interconnectedness illustrates that research in this field is not fragmented, but rather forms a holistic cybersecurity ecosystem, in which each component has a strong relationship with the others.

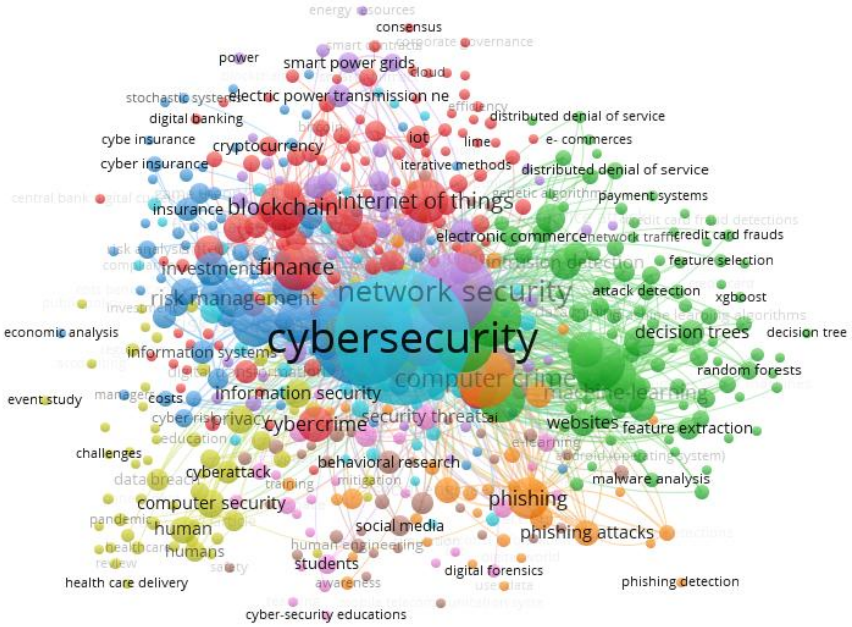

Figure 6. Network Visualization (using VOSviewer).

Upon closer examination, the map also reveals more specific and diverse thematic groupings. A significant cluster centers on technical defense methodologies, covering terms such as "machine learning," "decision trees," and "intrusion detection," which underscore the crucial role of artificial intelligence in building adaptive threat detection systems. On the other hand, there is a group that focuses on threat vectors and their applicable contexts, such as "phishing attacks," "malware analysis," "blockchain," and "digital banking." The diversity of these clusters effectively maps a comprehensive spectrum of research, ranging from the development of advanced technical solutions and in-depth analysis of cyberattack methods to their relevance in crucial sectors such as finance and technological innovation.

Figure 7 is a visualization that maps the network of various research topics within the broad scope of cybersecurity. Each circle on this map represents a subject or key term. The main principle is that the larger the circle, the more central and frequently discussed the subject is in academia and industry. It is clear that the term cybersecurity is the largest circle at the center, signifying its role as the main theme connecting all other areas. Surrounding it are other important topics such as network security, machine learning, and blockchain. Meanwhile, the intertwined lines connecting the circles indicate a strong correlation or relationship between these topics, which are often studied together.

The different colors on this map serve an important function in sorting various topics into more specific thematic groups. For example, there is a light blue group in the center that forms the main foundation with topics related to cybersecurity and network security. On the right side, the dominant green group covers the application of artificial intelligence or machine learning, as well as detection methods such as intrusion detection to combat credit card fraud. There is also a red group at the top that combines discussions on security in new technologies, such as the Internet of Things (IoT) and blockchain. Furthermore, the orange group at the bottom right specifically discusses various types of digital attacks, including phishing and malware analysis. This color-based division makes it easier for us to see that the scope of modern cybersecurity is multidisciplinary, not only limited to technical aspects, but also extending to data analysis, financial technology, and even human behavior studies.

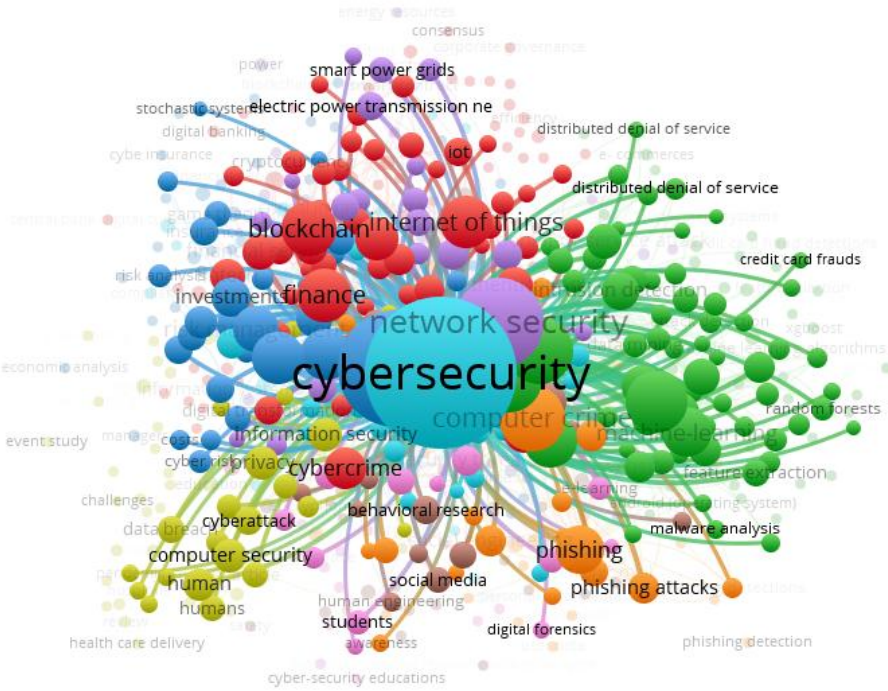

Figure 7. Network Visualization of the Term Cybersecurity (using VOSviewer).

Figure 8 shows a bibliometric network map that illustrates the research landscape with a primary focus on cybersecurity. This map depicts conceptual relationships and the frequency of key terms in scientific literature. The size of each node correlates directly with the frequency of the term, with "cybersecurity" emerging as the most dominant and central node, confirming its position as a core theme. This central symbol is surrounded by various important thematic clusters, including "network security," "computer crime," "blockchain," "internet of things," and "machine learning." The spatial proximity between symbols on this map reflects high cohesion and co-occurrence frequency between topics in scientific publications.

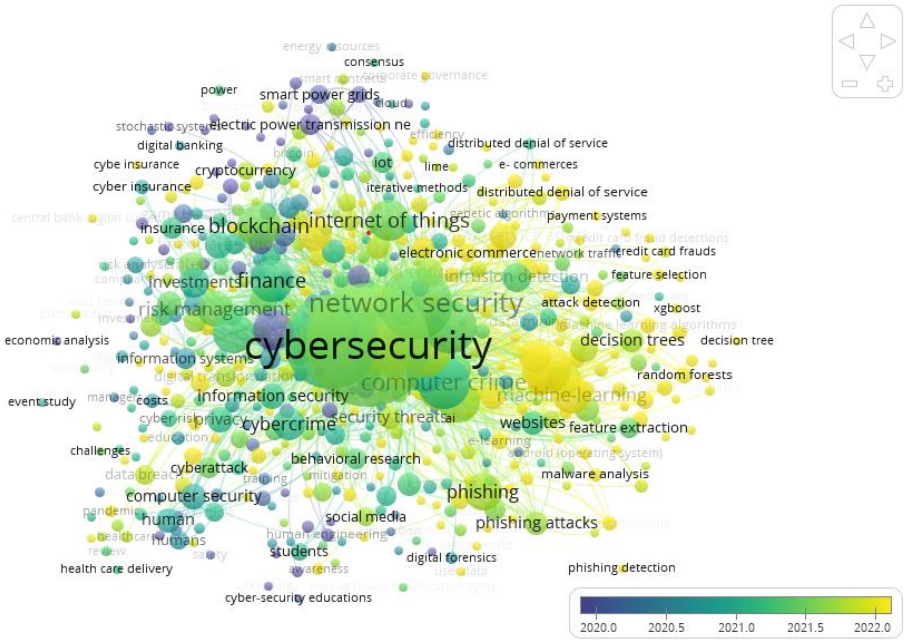

Figure 8. Overlay Visualization of Term Cybersecurity (using VOSviewer).

Additionally, temporal analysis can be performed based on the color gradation displayed on the scale in the lower right corner, which represents the time range from 2020 to 2022. It can be identified that basic concepts such as cybersecurity and network security are marked in green, indicating that both are established and consistent research subjects during that period. On the other hand, terminology marked in yellow, such as machine learning, decision trees, phishing attacks, and phishing detection, indicates more recent or emerging research trends in the latter part of the observation period. This phenomenon signifies the evolution and shift in the focus of research in the field of cybersecurity towards the application of artificial intelligence methods for more specific threat detection and cyber attack analysis.

Figure 9 shows a visualization of keyword density that clearly identifies cybersecurity as the main focus of research, marked by the most intense yellow hotspot in the center, indicating that this is the main and most dominant theme of the data set represented. Surrounding it, in a green zone that is also very prominent, are closely related core concepts such as network security, information security, risk management, and computer crime. This shows that cybersecurity is a multidisciplinary field that focuses not only on network technology, but also on risk management, information security in general, and combating computer crime. In addition, highly relevant modern technological terms such as machine learning, blockchain, and the internet of things are also prominently featured, indicating that advances in these areas are strongly interrelated and are an important focus in current cybersecurity discussions.

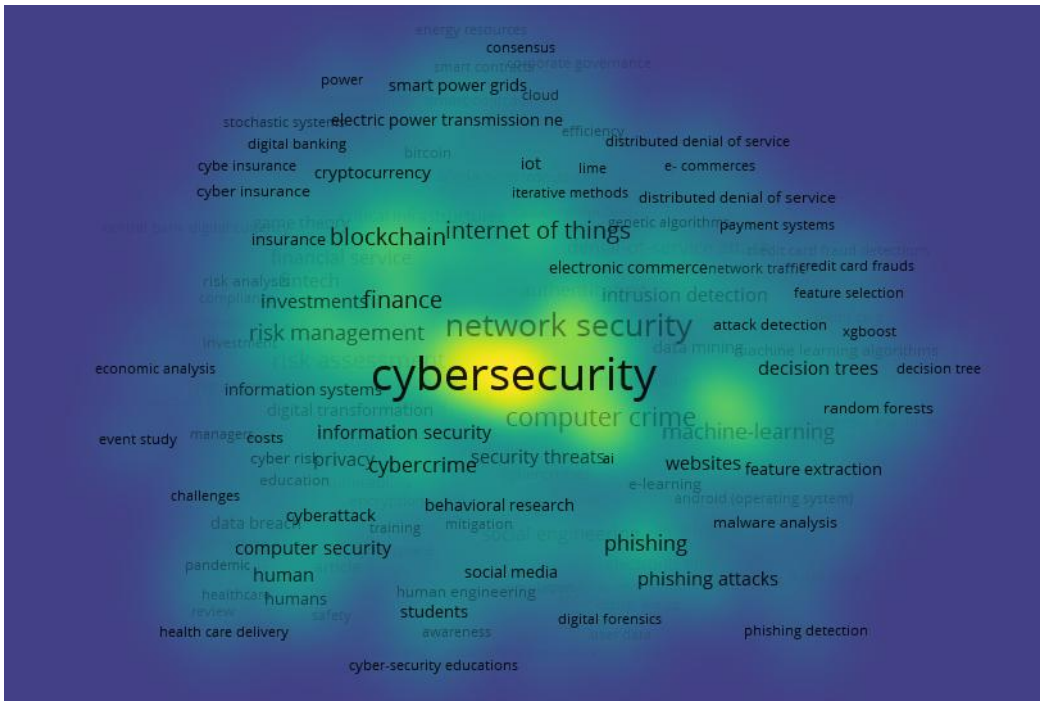

Figure 9. Density Visualization (using VOSviewer).

Spreading out from the center, this word map breaks down the cybersecurity landscape into more detailed elements in the blue and purple areas, unraveling more specific subtopics and showing the breadth of the cybersecurity field. On one side, this image details types of cyber threats and attacks such as phishing, phishing attacks, malware analysis, and distributed denial of service. On the other hand, it also presents various defense methods and techniques, including intrusion detection, digital forensics, and specific machine learning algorithms such as random forests and decision trees. The image also highlights sectors that are heavily affected by cybersecurity, such as finance, cryptocurrency, digital banking, e-commerce, and healthcare. Finally, the human aspect as a key element in cybersecurity is also emphasized through words such as human engineering, social media, students, education, and awareness, implying that human factors, training, and awareness are crucial components in a comprehensive cyber defense strategy.

5. Conclusions

A comprehensive bibliometric analysis of the cybersecurity research landscape in the financial industry over an eight-year period, from 2016 to 2023, indicates a very significant increase in academic interest. This dynamic is clearly reflected in the impressive 49.02% annual growth rate of publications, with an exponential growth trend that accelerated sharply, especially in the post-2022 period. One of the most notable findings of this study is the extensive level of collaboration among researchers. Remarkably, there were no publications written by a single author, with the average number of contributors per article approaching ten. Furthermore, more than 20% of the total publications were the result of international collaboration, which convincingly confirms the status of financial cybersecurity as a complex, multi-layered research domain that requires the synergy of expertise from various disciplines.

Using data from the Scopus database, thematic mapping identified 'cybersecurity' and 'network security' as the main conceptual pillars that unite various derivative research areas. Cluster analysis successfully revealed several dominant research clusters. On one hand, there is a cluster that focuses on technical defense mechanisms, driven by sub-topics such as machine learning and intrusion detection systems. On the other hand, there is a cluster that explores attack vector analysis, with phishing and malware as the main focus, as well as how these threats evolve with the adoption of emergent technologies such as blockchain and the Internet of Things (IoT). Analysis of trends over time also captures the shift in the focus of current research, which now leans more towards exploring the implementation of artificial intelligence and designing cutting-edge methods for more effective phishing detection.

Future research should focus on three crucial priority areas. First, in the technical realm, the development of machine learning architecture should be directed toward goals that go beyond mere accuracy. The priority is to design intelligent systems that are highly precise in identifying cyber anomalies, capable of adapting to large volumes of financial transactions, and providing results that can be interpreted for forensic analysis. Second, as blockchain becomes increasingly relevant, an in-depth study of its threat landscape is absolutely necessary. This includes proactive analysis of various attack scenarios, ranging from smart contract vulnerabilities and social engineering to systemic threats such as 51% attacks.

Third, given that this study highlights human factors as a major vulnerability, measuring the real impact of socio-technical interventions is a must. Initiatives such as security awareness training programs are no longer sufficient; their effectiveness must be quantitatively proven through measurable metrics, such as a decrease in phishing success rates or an increase in the speed of incident reporting by staff. At the industry and policy level, this research calls for a fundamental paradigm shift. The financial sector is encouraged to abandon a reactive security approach that only acts after an incident occurs, and shift to an integrated, holistic defense strategy. This new model requires a synergistic combination of advanced defense technologies, such as AI-based threat intelligence, with a foundation of proactive risk management and governance. Its implementation means fostering a risk-aware culture, conducting ongoing threat assessments, and embedding cybersecurity principles as an integral part of every line of business, beyond the boundaries of the IT department.

References

Adelmann, F., Ergen, I., Gaidosch, T., Jenkinson, N., Morozova, A., Schwarz, N., & Wilson, C. (2020). Cyber Risk and Financial Stability: It's a Small World After All. *Staff Discussion Notes*, *2020*(007). https://www.elibrary.imf.org/view/journals/006/2020/007/article-A001-en.xml

Akhta, S., Sheorey, P. A., Bhattacharya, S., & Ajith, K. V. V. (2021). Cyber security solutions for businesses in financial services: Challenges, opportunities, and the way Forward. *International Journal of Business Intelligence Research*, *12*(1), 82–97. https://doi.org/10.4018/IJBIR.20210101.oa5

Al Duhaidahawi, H. M. K., Zhang, J., Abdulreda, M. S., Sebai, M., & Harjan, S. (2021). Analysing the effects of FinTech variables on cybersecurity: Evidence form Iraqi Banks. *International Journal of Research in Business and Social Science (2147- 4478)*, *9*(6), 123–133.

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World Quarterly*, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*(April), 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Maggio, L. A., Costello, J. A., Norton, C., Driessen, E. W., & Artino, A. R. (2021). Knowledge syntheses in medical education: A bibliometric analysis. *Perspectives on Medical Education*, *10*(2), 79–87. https://doi.org/10.1007/s40037-020-00626-9

Maurer, T., & Nelson, A. (2021). *Global I. February 2020*.

Ninkov, A., Frank, J. R., & Maggio, L. A. (2022). Bibliometrics: Methods for studying academic publishing. *Perspectives on Medical Education*, *11*(3), 173–176. https://doi.org/10.1007/s40037-021-00695-4

Nweze, M., Avickson, E. K., & Ekechukwu, G. (2024). The Role of AI and Machine Learning in Fraud Detection: Enhancing Risk Management in Corporate Finance. *International Journal of Research Publication and Reviews*, *5*(10), 2812–2830. https://doi.org/10.55248/gengpi.5.1024.2902

Uddin, H., Canselor, P., Educity, K. I., Taylor, J., Jaya, S., Ali, H., Taylor, J., & Hall, K. (2018). *Cybersecurity Hazards and Financial System Vulnerability : A synthesis of literature Cybersecurity Hazard and Financial System Vulnerability : A synthesis of literature*. 1–58.