**Jurnal Multidisiplin West Science**
Vol. 5, No. 04, April 2026, pp. 606-617

# Research Landscape of Cybersecurity: A Bibliometric and Network Visualization Analysis

**Loso Judijanto**
IPOSS Jakarta, Indonesia dan losojudijantobumn@gmail.com

**ABSTRAK**

Tujuan makalah penelitian ini adalah untuk mengeksplorasi dan menganalisis lanskap penelitian mengenai isu-isu keamanan siber melalui penerapan alat bibliometrik dan visualisasi analisis jaringan. Data untuk analisis diperoleh dari basis data Scopus dan dianalisis menggunakan VOSviewer untuk mengevaluasi pola kolaborasi penelitian, makalah-makalah paling menonjol di bidang ini, dan perkembangan tematik isu-isu penelitian dalam sibernetika. Karya ini akan mempertimbangkan pola kolaborasi di antara para penulis yang melakukan penelitian di bidang keamanan siber serta sitasi dan kemunculan kata kunci. Berdasarkan hasil yang diperoleh, dapat dikatakan bahwa bidang keamanan siber sangat interdisipliner dan beragam secara geografis. Negara-negara seperti AS dan Tiongkok menyediakan sebagian besar penelitian di bidang ini. Mengenai pola tematik yang diidentifikasi, perlu dicatat bahwa meskipun beberapa tema tradisional seperti keamanan informasi dan penilaian risiko tetap dominan, tren baru integrasi keamanan siber dengan penggunaan kecerdasan buatan dan Internet of Things menjadi cukup populer. Selain itu, perhatian yang semakin besar diberikan pada aspek manusia dan organisasi yang terkait dengan keamanan siber (pengambilan keputusan dan pendidikan keamanan siber).

***Kata Kunci:*** *Keamanan Siber, Analisis Bibliometrik, Visualisasi Jaringan, Penulisan Bersama*

**ABSTRACT**

The objectives of this research paper are to explore and analyze the research landscape concerning the issues of cybersecurity via application of bibliometric tools and network analysis visualization. Data for analysis was obtained from the Scopus database and analyzed using VOSviewer to evaluate research collaboration patterns, the most prominent papers in the field, and thematic development of research issues in cybernetics. This work will consider the patterns of collaboration among the authors who conducted research in cybersecurity and the citation and co-word occurrences as well. Based on the results obtained, it is possible to say that the field of cybersecurity is very interdisciplinary and geographically diverse. Such countries as the USA and China provide the major part of research in the field. Concerning the thematic patterns identified, it should be noted that although some traditional themes like information security and risk assessments prevail, new trends of integration of cybersecurity with the use of artificial intelligence and Internet of Things become rather popular. Moreover, growing attention is paid to human and organizational aspects related to cybersecurity (decision-making and cybersecurity education).

***Keywords:*** *Cybersecurity, Bibliometric Analysis, Network Visualization, Co-Authorship*

## INTRODUCTION

In connection with the dynamic process of the digitalization of all spheres of the economy, it is possible to note that a new way of doing things emerged. Due to the rapid development of the technologies related to the internet, cloud services, AI, and IoT, there was a great variety of possibilities of becoming efficient and achieving success (Sindiramutty et al., 2024; Sood & Kim, 2023). However, considering all these innovations, one can speak about the emergence of one of the most serious problems that humanity is facing now – cybersecurity. The problem is not only concerned with protection from any cybercrime but rather relates to the economic, political, and even strategic problems when different nations are experiencing attacks from malware, resulting in a significant effect on the infrastructure and finance of the countries (Hassan & Shukur, 2019;

Partadiredja et al., 2020). In the past few years, cyber threats have become more sophisticated and severe. Numerous cases of ransomware attacks, data breaches, and cyber espionage prove the fact that there are many issues associated with cybersecurity that require attention. Not only do companies face certain risks in terms of financial gains but also suffer from reputational damages, which is why governments have to deal with national security-related concerns (Corallo et al., 2020; Ten et al., 2010).

Cybersecurity research has made rapid strides over time, covering a wide range of subjects that include but are not limited to cryptography, network security, intruder detection systems, cyber risk management, and security's human aspect (Pina Taylor, 2023). Cybersecurity is an interdisciplinary field that relies on insights from computer science, information systems, engineering, psychology, and even law and public policy. The result of this interdisciplinarity has been a voluminous and fractured body of research that makes it increasingly difficult for scholars to identify important developments, key works, and emerging research areas. In response to this gap in the cybersecurity research agenda, there has been a need for systematic methods of reviewing and mapping the research landscape (Fischer, 2014; Gupta et al., 2023). One of the most effective approaches for doing so has been bibliometrics. Tools such as VOSviewer and CiteSpace facilitate the visualization of complex relationships among authors, institutions, keywords, and countries, thereby providing insights into research trends and knowledge diffusion. In the context of cybersecurity, bibliometric and network visualization analyses can help identify dominant research themes, influential scholars, and global collaboration patterns (Donthu et al., 2021; Van Eck & Waltman, 2014).

In spite of the widespread use of bibliometric techniques across different fields of study, there are few comprehensive bibliometric analyses related to the cyber security research area, which tend to be narrow in focus. Most studies tend to focus on a particular aspect of cyber security such as network security or privacy instead of offering a broad perspective on the research area. Additionally, due to the fast-changing nature of cyber security, which involves new developments in technology and threats, a constant update is required for the research map. Hence, it is important to conduct a comprehensive bibliometric and visualization study to have a comprehensive picture of the cyber security research area. Despite being recognized as an increasingly important and dynamic area of study, the current state of cybersecurity research literature is extremely fragmented and spread over several fields of study, making it challenging to conduct systematic analyses to uncover the main research topics, key authors, and trends in cybersecurity research. Previous researches have mostly been concentrated on particular areas within cybersecurity or restricted data sets, leaving a gap in conducting a more thorough and contemporary analysis of the entire cybersecurity research field. This study aims to analyze and map the global research landscape of cybersecurity using bibliometric and network visualization techniques.

## RESEARCH METHODS

The present research employed a bibliometric research methodology for the systematic investigation of the world research landscape on the issue under consideration. In essence, bibliometric analysis is a quantifiable method of investigation aimed at the identification of the structure of a certain scientific area through publications' statistics, references and connections between scientific works (Donthu et al., 2021). The dataset used in this study was sourced from Scopus, one of the leading databases offering reliable and comprehensive scholarly literature. Scopus

was selected owing to its broad database coverage including relevant journals, proceedings, and articles related to cybersecurity. Specifically, the data gathering process entailed specifying relevant search terms concerning "cybersecurity," setting certain filters (i.e. document type – articles and conference papers; language – English; publication date), and exporting bibliographic data (title, abstract, author name, affiliation, keywords, etc.).

After data gathering, there was a need for the dataset to undergo a process of cleaning and pre-processing to improve its accuracy and consistency. Duplicate records were deleted, while author names and their institutional affiliations were standardized. Other records that had no relevance to the subject of the research were excluded from the list. Keyword normalization was also carried out to combine related keywords such as cyber security and cybersecurity. The resulting dataset was set for bibliometric mapping. Such a measure is necessary in bibliometric analysis since inconsistency in metadata has an effect on network analysis.

Network analysis and visualization in this study have been carried out through VOSviewer, a tool specifically developed for creating and analyzing bibliometric maps. VOSviewer was used to create several kinds of networks, including co-authorship networks (to study cooperation trends among researchers and nations), co-occurrence networks (to discover leading research trends through the analysis of keywords), as well as citation and co-citation networks (to find influential studies and their intellectual connections). This tool provided data in the form of maps that were further interpreted in order to better understand the development process of cybersecurity research.

## RESULTS AND DISCUSSION

### A. Co-Authorship Analysis

In this segment, we will examine the collaborative networks that exist in the field of cybersecurity research based on the co-authorship analysis among the articles selected for this study. The purpose of conducting co-authorship analysis is to gain understanding of the links and the collaborations that exist among different authors as well as clusters of expertise that may exist in the area.

#### 1. Author-level Visualization

As shown in the following visualization of co-authors network in Figure 1, this diagram shows how researchers collaborate in terms of cybersecurity research. With the help of VOSviewer, this co-authorship map reveals the links that exist between different researchers depending on their collaboration, whereby each node is an author and each link denotes co-authorship between these authors. The larger the node, the more influential the author has been.

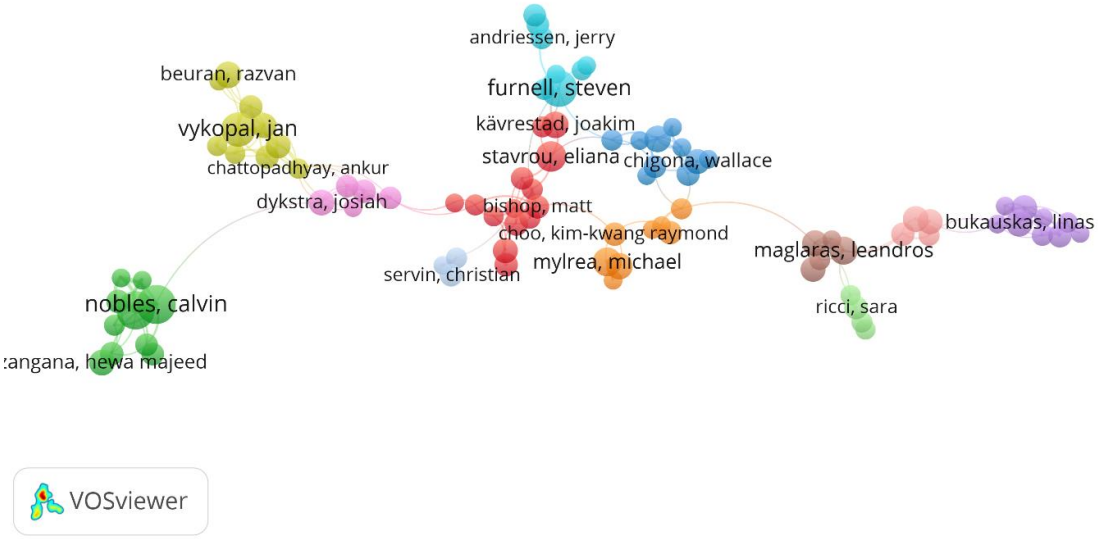


Figure 1. Author-level Visualization

*Source: Data Analyzed*

It becomes clear from the graph that there are several different groups of authors involved in cybersecurity research, showing that it involves collaborative networks that are fragmented but interlinked. The prominent clusters may be seen in relation to notable authors such as Furnell, Steven; Choo, Kim-Kwang Raymond; and Nobles, Calvin, demonstrating the importance of such researchers in their own spheres of research. Typically, the clusters tend to reflect certain aspects of cybersecurity research, such as digital forensics, information security management, and cybercrime. In addition, the network exhibits features where some nodes are densely connected with each other while others form loosely connected communities. The authors who occupy central positions within the network, for instance, Furnell and Choo, play a critical role in connecting various communities, hence serving as effective bridges for knowledge flow among subcommunities. Smaller and less-connected communities, like those comprising Bukauskas, Linas or Ricci, Sara, hint at specialized areas of research.

### 2. Institution-level Visualization

The institutional collaboration network shown in figure 2 above is a representation of the collaborations between organizations involved in cybersecurity research. It was produced using VOSviewer software and shows how universities, research centers, and laboratories collaborate via co-publications. In the diagram, each point represents an organization, while the linking lines depict the linkages between the organizations. The sizes of the points are proportionate to the extent to which each organization contributes, while colors represent different clusters of collaborating organizations.


Figure 2. Institution-level Visualization
*Source: Data Analyzed*

This illustration demonstrates that there exists a diverse group of organizations that provide funding for the study of cybersecurity, which includes university organizations as well as special laboratories. Prominent organizations like Capitol Technology University, Chitkara University Institute, and Sandia National Laboratories emerge as prominent nodes, demonstrating the important part they play in contributing to research studies in cybersecurity. Another interesting thing about the map is that Arizona State University and University of Johannesburg have been identified. These organizations prove the fact that cybersecurity research has an international aspect as well since organizations from different parts of the world participate in research activities. In addition, the structure of the network implies that institutional collaborations are relatively linear and sparse, with little interaction between the clusters. There seems to be a large number of institutions collaborating through a few bridging institutions rather than an extensive collaboration network among the institutions themselves. The following illustration shows how Sandia National Laboratories serves as a bridging institution between various universities. Some institutions also tend to operate from the margins with relatively less collaboration. This shows that even though there is collaboration among institutions, further improvements can be made in creating collaborations between multiple institutions.

### 3. Country-level Visualization

Figure 3 shows the network of cooperation between countries in cybersecurity studies based on co-authorship. This analysis was conducted using VOSviewer software, which reveals the pattern of cooperation between researchers from various countries in the creation of scientific papers. In this diagram, each node is a country, whose size reflects the level of participation in research or the number of published papers. Links are the connections between countries, which means the level of cooperation.

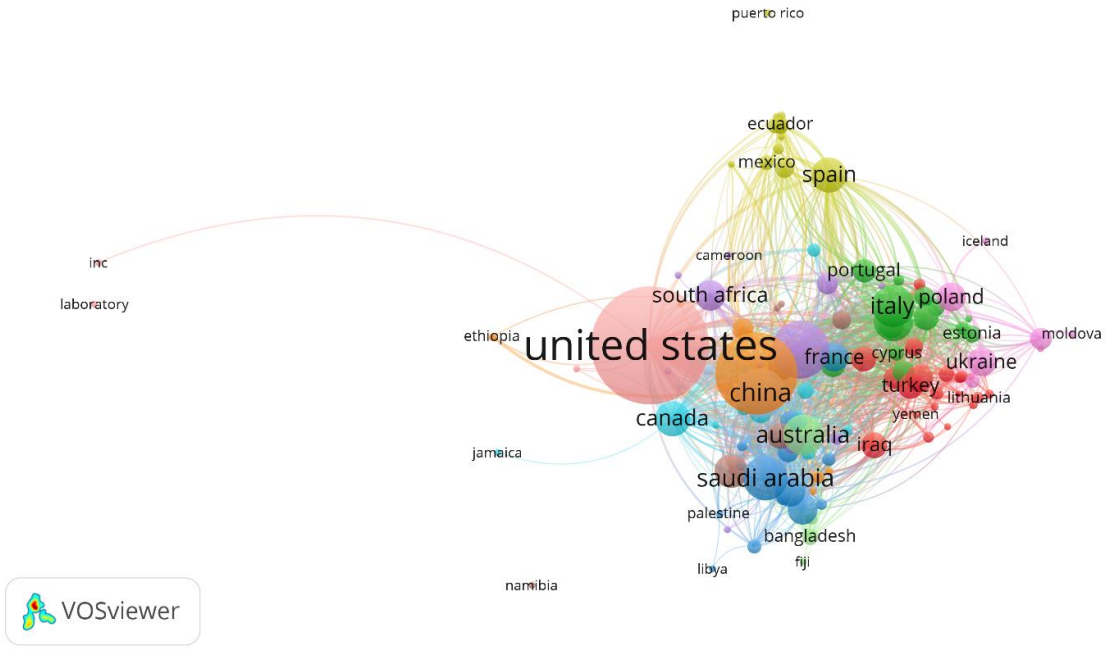


Figure 3. Country-level Visualization

*Source: Data Analyzed*

From the above figure, it is clearly evident that the United States plays a very prominent and central role in the international research network related to cybersecurity. The fact that its node is larger with many connections indicates that it acts as the main hub of such collaborations. Other nations like China, UK, Italy, and Spain have also played important roles in terms of cybersecurity research and collaborations with other nations. This can be attributed to the fact that cybersecurity is a global issue and requires international cooperation among countries rich in technological research. Moreover, the network provides information on the existence of collaboration groups in regions, especially Europe, Asia, and the Middle East. For example, European countries such as Poland, Ukraine, and Estonia create a cohesive European collaboration group, whereas Saudi Arabia, Bangladesh, and other neighboring countries belong to another group. However, despite this, there are several countries that remain peripheral, implying that they have low involvement or fewer collaborations in global research networks. Thus, this indicates that although cybersecurity research has become more globalized, there are still gaps that may present themselves in terms of research capacity and collaboration among countries.

### B. Citation Analysis

It is a very efficient method to measure the influence of scholarly literature on the cybersecurity discipline.

Table 1. Top Cited Literature

| Number of Citations | Author'(s) | Title |
|---|---|---|
| 6841 | (Alzubaidi et al., 2021) | Review of deep learning: concepts, CNN architectures, challenges, applications, future directions |

| | | |
|---|---|---|
| 4591 | (Sarker, 2021b) | Machine Learning: Algorithms, Real-World Applications and Research Directions |
| 2378 | (Sarker, 2021a) | Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions |
| 2092 | (Sallam, 2023) | ChatGPT Utility in Healthcare Education, Research, and Practice: Systematic Review on the Promising Perspectives and Valid Concerns |
| 1665 | (Kolias et al., 2017) | DDoS in the IoT: Mirai and other botnets |
| 1458 | (Alom et al., 2019) | A state-of-the-art survey on deep learning theory and architectures |
| 1096 | (Nishant et al., 2020) | Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda |
| 1086 | (Biggio & Roli, 2018) | Wild patterns: Ten years after the rise of adversarial machine learning |
| 1067 | (Wang et al., 2020) | Resistive switching materials for information processing |
| 1064 | (Sridhar et al., 2011) | Cyber-physical system security for the electric power grid |

*Source: Scopus Database, 2026*

### C. Keyword Co-Occurrence Analysis

Keywords co-occurrence analysis is performed in order to reveal the thematic structure of research on the subject of cybersecurity. As a result of studying the frequency of occurrence and the co-occurrence of keywords in the articles chosen for the analysis, the main themes and trends in this field will be identified, as well as any gaps that may exist in the current research.

#### 1. Network Visualization

The co-occurrence map of keywords depicted in Figure 4 shows the structure and development of the concept of cybersecurity through the use of keywords in the chosen articles. Using VOSviewer software, the co-occurrence map is generated through the number of times certain keywords co-occur. In this case, nodes symbolize individual keywords, while lines between them demonstrate the connections between them. Nodes' sizes represent the importance of particular keywords in the corpus of data analyzed. On the other hand, colors differentiate the clusters created by the keywords and denote various themes.

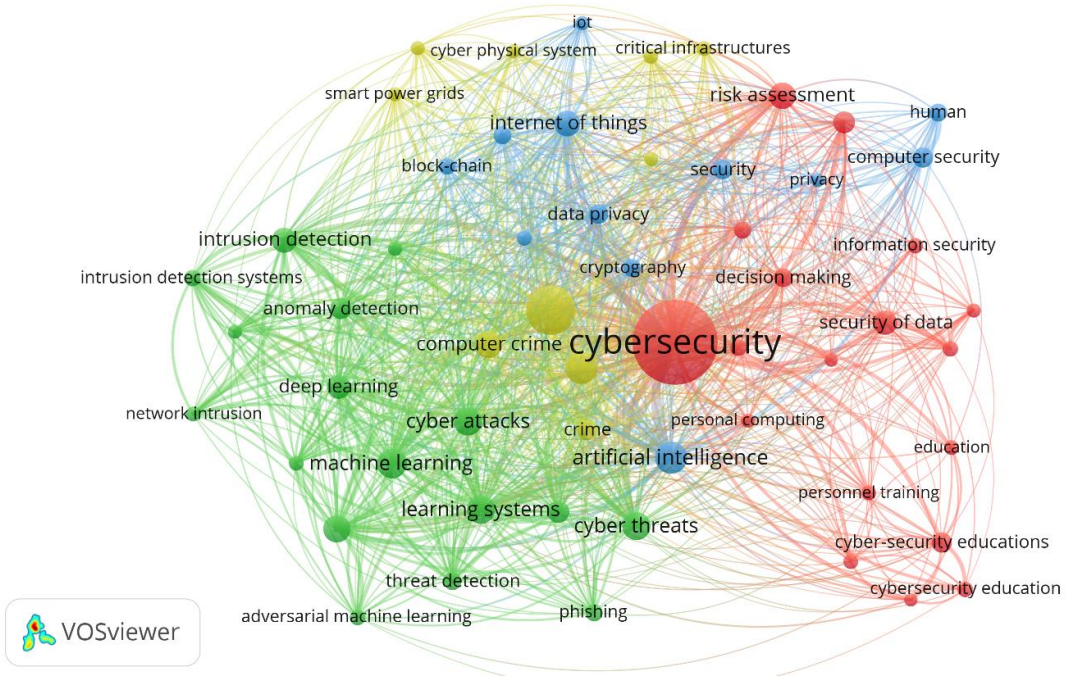


Figure 4. Network Visualization

*Source: Data Analyzed*

It is also evident from the visualization that "cybersecurity" acts as the most important and dominant keyword, meaning that it plays an essential role in almost every research theme. It is worth mentioning that related keywords such as "artificial intelligence," "cyber attacks," "data privacy," and "information security" also form an important cluster, implying that current cybersecurity research trends involve the use of advanced computing technology and the need to mitigate sophisticated cyber-attacks. Furthermore, the density of connections around these keywords implies that the field of cybersecurity is highly interdisciplinary because various aspects of technology and organizations are also involved. An important group of keywords in green reveals that there has been increasing interest in using machine learning and deep learning for cybersecurity applications. Words like "machine learning," "intrusion detection," "anomaly detection," and "threat detection" imply that many researchers aim to develop smart tools for identifying and mitigating threats to cybersecurity. Another interesting phenomenon in cybersecurity research trends is the use of "adversarial machine learning".

Yet another cluster, mostly in red color, focuses on topics related to the governance, risk management, and people-centric dimensions of cybersecurity. Key phrases like "risk assessment," "information security," "privacy," "decision making," and "cybersecurity education" suggest that apart from technical solutions, other factors such as policy and organizational practice have started to get increased importance. These topics relate to the fact that while cyber threats pose technological challenges, they also involve socio-organizational problems and call for adequate training, awareness, and risk-based decision-making. Finally, two more clusters colored in blue and yellow show how the issue of cybersecurity merges with technological innovations and infrastructure systems. Terms like "internet of things," "blockchain," "cyber-physical systems," and "critical infrastructures" imply that cybersecurity has moved into a digital ecosystem consisting of various emerging technologies and infrastructure systems.

**2. Overlay Visualization**

Keyword co-occurrence visualization, as shown in Figure 5, can be used for analyzing the trends of research themes in the field of cybersecurity over time. Keyword co-occurrence map developed using the VOS viewer tool not only shows the co-occurrence network between keywords but also the timeline in which the respective keywords were used. Links between nodes denote co-occurrence relationships and colors ranging from blue to yellow show the timeline, where blue refers to old keywords while yellow denotes recent keywords.

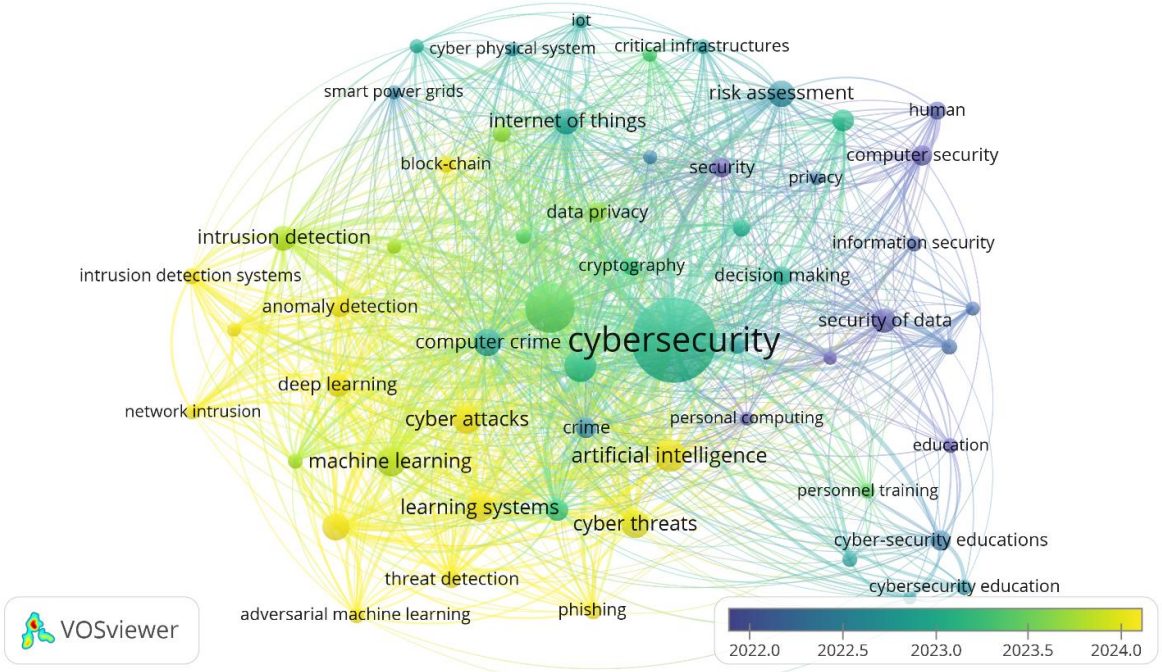


Figure 5. Overlay Visualization

*Source: Data Analyzed*

As illustrated by the diagram above, the key foundational topics like "information security," "computer security," and "risk assessment" are illustrated in dark shades of blue, signifying that these topics have had considerable influence on previous studies of cybersecurity. The importance of these key topics is reflected in the centrality of their positions on the map, meaning that although introduced relatively earlier in the field of cybersecurity research, these issues still affect future studies. On the other hand, more recently developed topics like "machine learning," "deep learning," "artificial intelligence," "phishing," and "adversarial machine learning" are illustrated using colors ranging from green to yellow.

The prevalence of such terms in the research highlights the trend towards an intelligent and automated process for the detection, prevention, and mitigation of cyber threats. Moreover, the term "adversarial machine learning" represents a key development in the field, highlighting the fact that researchers have begun exploring the potential flaws in AI-based cybersecurity systems. Lastly, the occurrence of the terms "internet of things," "cyber-physical systems," and "data privacy" in the intermediate colors shows that the research is in a transition stage, where the focus of the research was shifting from traditional cybersecurity to the challenges of connected systems and data privacy.

### 3. Density Visualization

Figure 6 presents the density visualization of keyword co-occurrence which is a full coverage of research issues in the area of cybersecurity based on their density and concentration in the field. It is prepared by utilizing VOSviewer software and it reveals those topics with high density that show frequent co-occurrence of keywords. The use of colors here shows yellow color for topics that have high density while green and blue colors demonstrate those with low density and less focus.

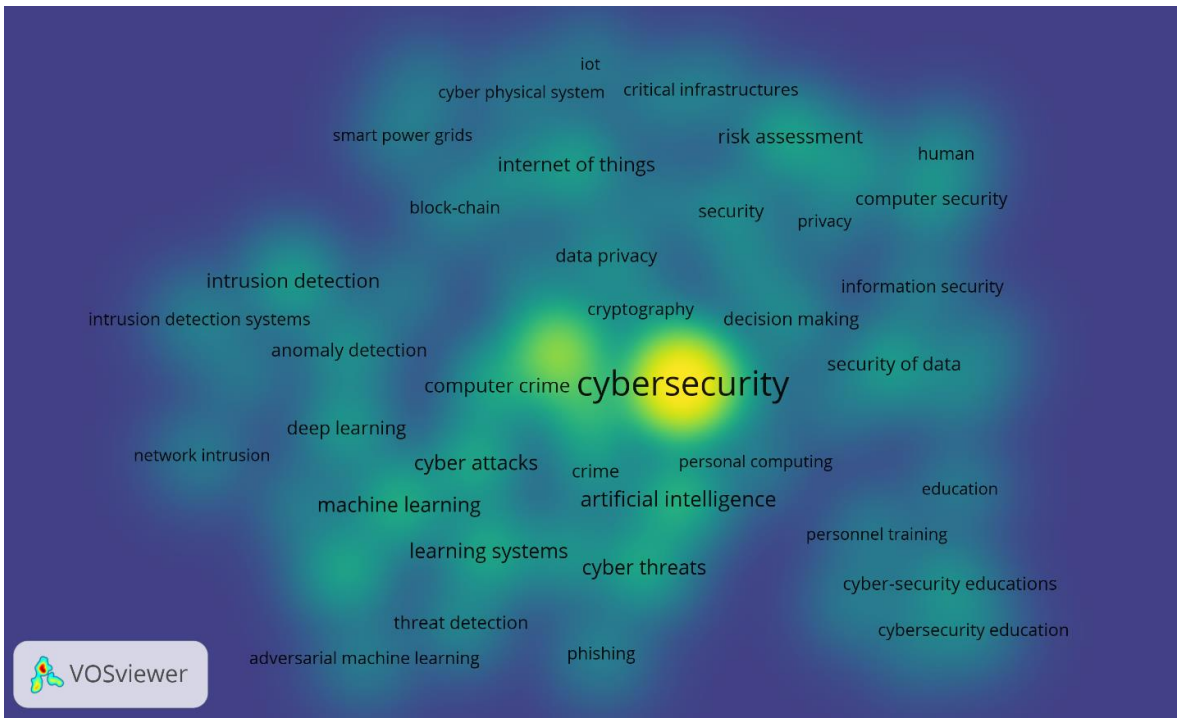


Figure 6. Density Visualization

*Source: Data Analyzed*

As evident from the graph, the concept "cybersecurity" appears to be the most significant and dense keyword in terms of its location within the visualization plot. This is reflected through the bright yellow cluster positioned in the middle of the plot. Hence, it can be said that the topic of cybersecurity is considered one of the most researched and highly interrelated fields among all others, forming the core of the entire literature body. The surrounding clusters include the high-density keywords such as "artificial intelligence," "cyber attacks," "computer crime," and "machine learning." On the other hand, low-density regions, denoted by green and blue colors, encompass subjects like "cybersecurity education," "training personnel," "phishing," and "adversarial machine learning." Although these issues are mentioned in the network, they are discussed less often in the literature, indicating that they could be potential areas for future studies or areas that have not gained much traction yet.

### Discussion

The results obtained from the bibliometric analysis and visualizing of the keyword network suggest that cybersecurity research has become a multi-disciplinary field and an area of study which has achieved global interconnectedness. With the prevalence of keywords like cybersecurity, information security, and computer security, it becomes clear that the field of cybersecurity research

is still true to its aims of securing systems, information, and infrastructures digitally. Nevertheless, the way in which cybersecurity interacts with new technologies shows that there has been a major shift in the realm of cybersecurity research. It becomes evident that cybersecurity research is becoming less disciplinary and more cross-disciplinary, incorporating the use of computer science, data analytics, engineering, and other sciences. Among the key trends found in the research is the role of artificial intelligence and machine learning in advancing the science of cyber security. Through visualization of the density and co-occurrences of keywords, it is evident that the intrusion detection system, anomaly detection, and deep learning have gained popularity in the context of tackling cyber threats. Such an observation arises from the need to address sophisticated attacks that necessitate intelligent and automatic detection and mitigation of such threats. Another emerging trend in cyber security is the idea of adversarial machine learning. This finding shows the level at which scholars are analyzing the weaknesses of these intelligent machines.

The analysis of collaboration highlights the relevance of both international and institutional partnerships in the progress of cybersecurity studies. Both co-authorship and country collaborations confirm the significant role played by influential nations, like the United States and China, in setting the research agenda in the context of cybersecurity, and their active involvement, which is backed up by institutional collaborators, such as important universities and labs. Nevertheless, the network also evidences an uneven distribution of roles within the network, where many countries and institutions remain on the margins of the process. In addition to improvements in technology, the study also points out the emerging importance of the human and organizational factors associated with cybersecurity. Words like 'risk assessment,' 'privacy,' 'decision making,' and 'cybersecurity education' show that there is a growing trend of studying cybersecurity from the perspective of governance and behavior. It should be noted that this is especially relevant because most cybersecurity breaches are caused by human mistakes or poor organizational management. The fact that the study identifies education and training as areas of interest is another sign that people are aware that cybersecurity involves more than technology.

Based on the findings of this analysis, the field of cybersecurity is experiencing an ongoing evolution involving innovation, broadening in the thematic domain, and global collaborations among other aspects. Although the traditional issues associated with cybersecurity research are extremely advanced, there appear to be many other issues related to AI-powered security, Internet of Things (IoT), human-centered security, etc., which may provide many opportunities for future investigation. Thus, the current direction in which cybersecurity is moving can include developing bridges in existing research collaborations, exploring interdisciplinarity in research, and discovering other aspects, such as cybersecurity training and ethics of intelligent systems.

## CONCLUSION

The current analysis shows how the field of cybersecurity research continues to evolve rapidly and become even more interdisciplinary, driven by a high level of global cooperation and technological advances. Bibliometric and network visualization techniques illustrate that even though some classical themes, like information security and risk management, continue to be crucial, there is a notable trend towards using artificial intelligence, machine learning, and new digital systems like the Internet of Things. The focus on human factors, organizations, and education can be considered a sign of a more

complex view on the issue at hand. In spite of significant progress made within the sphere, the existing inequalities in cooperation and insufficiently researched fields show potential for improvement.

**REFERENSI**


Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., Hasan, M., Van Essen, B. C., Awwal, A. A. S., & Asari, V. K. (2019). A state-of-the-art survey on deep learning theory and architectures. *Electronics*, *8*(3), 292.

Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., Santamaría, J., Fadhel, M. A., Al-Amidie, M., & Farhan, L. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data*, *8*(1), 53.

Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2154–2156.

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, *114*, 103165.

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*, 285–296.

Fischer, E. A. (2014). *Cybersecurity issues and challenges: In brief*. Congressional Research Service Washington, DC, USA.

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE Access*, *11*, 80218–80245.

Hassan, M. A., & Shukur, Z. (2019). Review of digital wallet requirements. *2019 International Conference on Cybersecurity (ICoCSec)*, 43–48.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80–84.

Nishant, R., Kennedy, M., & Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. *International Journal of Information Management*, *53*, 102104.

Partadiredja, R. A., Serrano, C. E., & Ljubenkov, D. (2020). AI or human: the socio-ethical implications of AI-generated media content. *2020 13th CMI Conference on Cybersecurity and Privacy (CMI)-Digital Transformation-Potentials and Challenges (51275)*, 1–6.

Pina Taylor, L. (2023). *Raising Cybersecurity Awareness and improving Organizational Resilience in the Critical Infrastructure Sector*.

Sallam, M. (2023). ChatGPT utility in healthcare education, research, and practice: systematic review on the promising perspectives and valid concerns. *Healthcare*, *11*(6), 887.

Sarker, I. H. (2021a). Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions. *SN Computer Science*, *2*(6), 1–20.

Sarker, I. H. (2021b). Machine learning: Algorithms, real-world applications and research directions. *SN Computer Science*, *2*(3), 160.

Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Gharib, A. H., & Yun, K. J. (2024). Applications of blockchain technology in supply chain management. In *Cybersecurity Measures for Logistics Industry Framework* (pp. 248–304). IGI Global.

Sood, S., & Kim, A. (2023). The Golden Age of the Big Data Audit: Agile Practices and Innovations for E-Commerce, Post-Quantum Cryptography, Psychosocial Hazards, Artificial Intelligence Algorithm Audits, and Deepfakes. *International Journal of Innovation and Economic Development*, *9*(2), 7–23. https://doi.org/10.18775/ijied.1849-7551-7020.2015.92.2001

Sridhar, S., Hahn, A., & Govindarasu, M. (2011). Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210–224.

Ten, C.-W., Manimaran, G., & Liu, C.-C. (2010). Cybersecurity for critical infrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, *40*(4), 853–865.

Van Eck, N. J., & Waltman, L. (2014). Visualizing bibliometric networks. In *Measuring scholarly impact: Methods and practice* (pp. 285–320). Springer.

Wang, Z., Wu, H., Burr, G. W., Hwang, C. S., Wang, K. L., Xia, Q., & Yang, J. J. (2020). Resistive switching materials for information processing. *Nature Reviews Materials*, *5*(3), 173–195.