West Science Information System and Technology
Vol. 04, No. 01, April 2026, pp. 34~45

A Scopus-Based Bibliometric Landscape of Cybersecurity Research (2000–2026): Trends, Collaboration, and Research Directions

Loso Judijanto
IPOSS Jakarta, Indonesia

Article Info

Article history:

Received Apr, 2026
Revised Apr, 2026
Accepted Apr, 2026

Keywords:

Cybersecurity
Bibliometric Analysis
Scopus
VOSviewer
Collaboration Patterns

ABSTRACT

The rapid advancement in digital technologies has resulted in a significant increase in the importance of cybersecurity, resulting in an upsurge in the number of studies conducted in this domain during the last two decades. Therefore, the present work is intended to investigate the intellectual structure, collaboration patterns, and evolution of themes in cybersecurity research through a bibliometric analysis. Data have been extracted from Scopus from the time period 2000-2026, and VOSViewer has been used to conduct the visualization process through the identification of the co-authorship network, citation network, and keywords co-occurrence network. As observed from the results obtained, there are a few dominant countries contributing to cybersecurity research, including the US, India, and China that play the roles of central hubs in the network of collaborations. It can be found from the citation network analysis that highly cited papers deal extensively with artificial intelligence, machine learning, and deep learning as they play a crucial role in cybersecurity research. Finally, through keyword analysis, it has been revealed that there is a transition in theme from intrusion detection and network security to newer themes such as artificial intelligence-based security, blockchain, Internet of Things (IoT), and behavioral cybersecurity. This study contributes to the literature by providing a comprehensive overview of the evolution and current state of cybersecurity research, while also identifying emerging trends and potential directions for future studies.

Corresponding Author:

Name: Loso Judijanto
Institution: IPOSS Jakarta, Indonesia
Email: losojudijantobumn@gmail.com

1. INTRODUCTION

There has been an explosion of technology usage, which has significantly impacted how society operates, interacts, and does business [1]. With an increase in internet accessibility, cloud computing solutions, smartphones, and the IoT, there has developed an extremely connected world [2]. Even as all these advances offer enormous opportunities, they also create intricate security risks that leave the networks exposed to cyber-attacks. This has given birth to cybersecurity, a field focused on ensuring that information resources are protected and kept confidential [2], [3]. Cybersecurity is now a key area of study and practice that not only deals with technical issues but also strategic priorities for everyone across the world [4].

In the last two decades, the cyber threat environment has undergone

remarkable transformation not only in terms of its magnitude but also its intricacies. Early cyber events involved fairly simple acts driven by curiosity and financial considerations of low scale [5]. In contrast, cyber threats today involve a variety of complex operations, from ransomware attacks, phishing, and cyber espionage to advanced persistent threats (APTs) [6]. Today's cyber threats are organized attacks carried out by highly structured teams, which use cutting-edge technology such as artificial intelligence and machine learning. As cyber threats become increasingly intricate, the demand for cyber threat studies has also escalated exponentially, necessitated by the increasing urgency surrounding cyber risk management [7].

In light of this problem, it is worth noting that the academic world has become more inclined to apply the principles of bibliometrics in order to track the development of the science of cybersecurity. With the help of bibliometric methods, researchers can effectively study a large amount of scientific literature and detect various regularities associated with publication statistics, citation, authors' networks, and topic evolution. The use of specialized databases, such as Scopus, will allow scholars to draw meaningful conclusions about the structure of the research domain and its dynamics. The existing literature suggests that bibliometrics is a helpful tool for exploring different issues in cybersecurity, including finding research priorities, identifying key contributors, and determining emerging topics [8].

Moreover, previous studies using bibliometric analysis have indicated important trends in research related to cybersecurity. There has been an observed rise in research papers covering areas like malware detection, network security, cyber risk management, and applications of artificial intelligence in threat detection. This increase in research output, especially after 2016, is mainly linked to advances in technology, major security incidents, and changes in the legislative framework.

Although there have been many studies conducted in this field, a systematic analysis over the years that incorporates various aspects of cybersecurity research – trends, networks, and themes – has yet to be performed. In addition, some studies concentrate only on certain subfields like cybercrime and data security or within a short period. Furthermore, the analysis should be extended up to the year 2026, considering the advent of new technologies and shifting dynamics in the threat landscape. These shortcomings should be addressed in order to provide a thorough insight into the cybersecurity research domain and serve as a guide for future endeavors.

Despite extensive research activities within cybersecurity over the last two decades, there is still an absence of an extensive and integrated analysis that would incorporate long-term trends, global cooperation tendencies, and shifts in research interests based on a single and reliable data base, for example, Scopus. Earlier studies typically consider a narrower time interval or a particular research topic, leaving gaps in their coverage and producing an incomplete picture of what actually takes place in the field under investigation. The fast pace of cybercrime and technology developments has led to some shifts in cybersecurity research trends that were not considered in the previous literature.

The purpose of this study is to conduct an in-depth bibliometric investigation of cybersecurity studies in the period between 2000 and 2026, focusing particularly on the emergence of trends, important researchers in the field, global cooperation within research groups, and new areas of research. This paper will attempt to analyze a vast number of scientific articles with the aim of understanding the nature of research, major events, and important findings within the discipline.

2. METHODS

The current study follows the methodology of bibliometrics to quantify the evolution of cybersecurity research from the

year 2000 until 2026. The process of bibliometric analysis has been extensively used across the scientific world as an effective tool for studying scientific publications systematically and objectively, thereby helping identify trends associated with production, citations, and knowledge structures within a discipline [8], [9]. The present study makes use of Scopus as the database to collect data for analyzing cybersecurity research from the selected time period since Scopus is the largest abstract and citation database with vast collections of peer-reviewed journals and conference proceedings. A search query was created by using relevant keywords like "cybersecurity," "information security," "network security," and other related words.

After collecting data from various sources, there is always an important step involved that deals with cleaning and pre-processing the data to enhance its accuracy and relevance. Any duplicate data records and any irrelevant information that do not meet the pre-defined criteria are excluded. The information that is gathered includes author names, title of documents, abstracts, keywords, affiliation details, years of publication, and number of citations among others. After pre-processing the data, it is subjected to bibliometric software like VOSviewer. These packages allow visualization of the scientific network and the relationships between different entities. They helped create networks such as co-authorship, citation, and keywords.

The following methods of analysis were applied in order to realize the objectives of the study. First, descriptive analysis was applied to analyze publication trends yearly, the growth of citations, and the sources that lead publication. Network analysis was also employed to investigate cooperation among the authors, institutions, and nations. Such an approach will enable us to know how many international collaborations exist within cybersecurity research. Lastly, thematic analysis through keywords was carried out to find out the research themes over the years. Thematic analysis entails looking at the themes that have been covered within cybersecurity research for the period starting from the very first studies and going all the way to those of 2026.

3. RESULTS AND DISCUSSION

3.1 Co-Authorship Analysis

The co-authorship analysis sheds light on the collaboration in cybersecurity research by analyzing the links between authors, organizations, and nations in the Scopus database during the period from 2000 to 2026. Collaboration is a key factor that reflects the exchange of knowledge and scientific productivity. In particular, the importance of collaboration is especially relevant for multidisciplinary research fields like cybersecurity, where challenging issues usually require different competencies to be resolved. With the help of visualization, the co-authorship analysis reveals the degree of interconnections among scientists and shows how the formation of clusters stimulates cybersecurity research.

The visualization of the co-authorship network created by VOSviewer shows the collaboration network of authors within the field of cybersecurity studies using data from Scopus database. As can be seen in the map, researchers are connected by their collaborative work on the basis of which they form separate clusters that correspond to collaboration clusters or research communities. In this network, each node corresponds to a particular author while edges show the relations between the co-authors; their thickness shows the level of the intensity of cooperation.

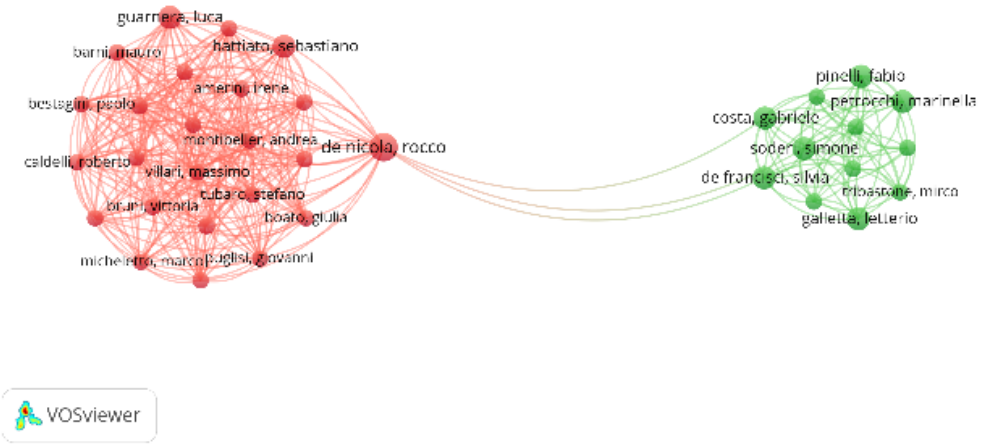

Figure 1. Author-Level Visualization
Source: Data Analysis

Based on the visualization, it can be seen that there are two major clusters present in the visualization, which means that cybersecurity studies have an organized structure where there are different collaborative networks for research. In particular, the red cluster seems to be more compact, meaning that it is characterized by intensive interaction and cooperation between members of the group. Therefore, members of this cluster regularly publish articles together, thus forming a tightly-knit network, which could be either a well-established field of study or a community of scientists studying similar subjects. On the other hand, the green cluster, despite being smaller in size, exhibits a relatively lower degree of collaboration among its nodes. In this case, the density of links is lower, meaning the degree of collaboration is somewhat loose in nature. The occurrence of bridging links among the red and green clusters is especially noteworthy as it indicates collaboration across the clusters.

The co-authorship network of institutions depicted by the aid of VOSviewer software provides a map of collaborations among institutions that engage in cybersecurity-related research as depicted in the Scopus database. The network demonstrates how institutions are connected based on their joint works, and the resultant clusters can be interpreted as collaborations or research alliances among these institutions. The nodes represent institutions whereas the connecting lines denote collaboration between nodes.

Figure 2. Institution-Level Visualization
Source: Data Analysis

The chart demonstrates a linear and sparse pattern of collaboration within institutions, showing that there is still no complex connectivity of partnerships in the field of cybersecurity studies. The location of the School of Computing, Kalesal… in the center of the chart demonstrates that it is a central player in the network and serves as a bridge between all other institutions. The fact that it is connected with institutions from both parts of the network proves that it can be considered an intermediary organization, helping institutions collaborate despite their lack of connections. On the right side of the network, a small cluster of institutions demonstrates localized collaboration, where entities such as Thapar Institute and neighboring nodes form a tightly grouped partnership. However, the limited number of links connecting this cluster to others suggests that collaboration remains somewhat fragmented. Similarly, the left-side cluster appears isolated, with minimal cross-linkages to other institutions.

The co-authorship network map constructed at the country level by using VOS viewer shows the global collaboration trends in the field of cybersecurity using Scopus database. In the constructed network, the nodes are countries, and the links between the nodes show the collaborations that occurred via the collaboration papers. The sizes of the nodes in the map show the research productivities, whereas the clusters created by the connections among nodes show the collaboration groups of certain regions or themes.

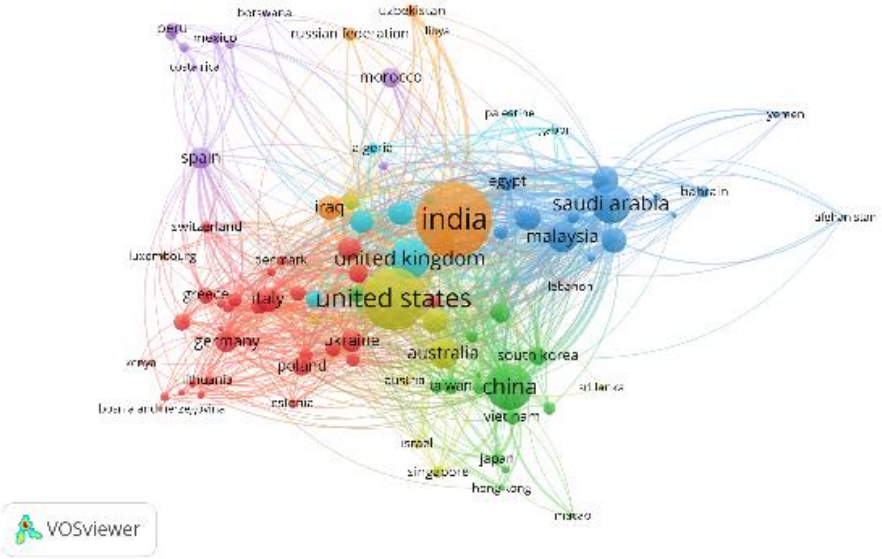

Figure 3. Country-Level Visualization
Source: Data Analysis

From the visualization above, we can deduce that the US, India, and China are among the prominent hubs within the cyber security research network. This has been depicted by their large node size and connection with other countries through the links. The US plays an important role within the clusters. In this case, the US appears to be a strong driving force behind collaborations. Similarly, India is another well-connected country within the network. It is a driving force behind the collaborations that are made by both the developed and developing countries. Conversely, China is placed at the core of its own cluster.

Apart from these dominating players, there are also regional clusters that may be recognized, including countries in Europe being grouped together with close interconnectivities, or countries in the Middle East and Asia with new networks being formed for collaborative purposes. Such examples include countries like Saudi Arabia and Malaysia, which play a vital role as connective links between their respective clusters, thus proving increasing involvement in global research collaborations. The existence of cross-cluster linkages is indicative of the interdisciplinary and international scope of cyber security research. Nevertheless, the unequal distribution of links also implies that there are still underrepresented regions in the global network.

3.2 Citation Analysis

The analysis of citations is one of the primary methods that help assess the intellectual framework and impact of cybersecurity studies. Based on an examination of citation trends among publications, the current study reveals the top contributors in terms of authors, journals, and articles that have made substantial contributions towards the growth of the discipline. Citations can be viewed not just as an expression of academic merit but also as a process of transferring information and creating the theoretical and methodological foundations of a scientific field. This study allows identifying the basic literature sources that form the basis for cybersecurity studies and provides insight into the distribution of scholarly impact within the domain.

Table 1. The Most Impactful Literatures

Citations	Authors and year	Title
6656	[10]	Review of deep learning: concepts, CNN architectures, challenges, applications, future directions
4487	[11]	Machine Learning: Algorithms, Real-World Applications and Research Directions
2323	[12]	Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions
2047	[13]	ChatGPT Utility in Healthcare Education, Research, and Practice: Systematic Review on the Promising Perspectives and Valid Concerns
1072	[14]	Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda
1063	[15]	Wild patterns: Ten years after the rise of adversarial machine learning
1059	[16]	Cyber-physical system security for the electric power grid
1037	[17]	Machine Learning and Deep Learning Methods for Cybersecurity
936	[18]	A survey of intrusion detection in Internet of Things
880	[19]	AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems

Source: Scopus, 2026

Table 1 shows that the most impactful literature within the dataset is strongly dominated by studies related to artificial intelligence, machine learning, deep learning, and their practical applications, including cybersecurity, healthcare, sustainability, and intelligent systems. The highest-cited works, such as [10] and [19], indicate that broad methodological review articles have become foundational references because they offer conceptual frameworks, technical classifications, and future research directions that are widely applicable across disciplines. At the same time, the presence of cybersecurity-specific studies, such as [15], [16]–[18], suggests that the cybersecurity field is increasingly shaped by cross-fertilization with AI-based approaches, particularly in areas such as adversarial machine learning, cyber-physical system protection, intrusion detection, and intelligent threat analysis.

3.3 Keyword Co-Occurrence Analysis

Co-occurrence analysis of keywords is used to create a network map for the conceptual and thematic development of cybersecurity research. Through analyzing the frequencies and co-occurrences of keywords in the corpus, the study will reveal important research themes and clusters, which would be the key issues being studied in the cybersecurity body of knowledge. In addition, this method can help understand how those research issues are related to each other and how they have developed over time. The creation of the keyword network graph will assist in recognizing not only established research issues but also emerging issues in the domain.

Keyword co-occurrence network analysis performed by VOSviewer reveals the underlying concept and theme structure of cybersecurity research based on data from Scopus database. In such a network visualization, individual nodes represent the keywords, whereas the edges reveal the co-occurrence frequency of those keywords within the same articles. The more prominent the size of particular nodes is, the more important those topics are in cybersecurity research. Therefore, through keyword co-occurrence mapping, one can reveal the prevailing fields of studies, their connections, and developments over time.

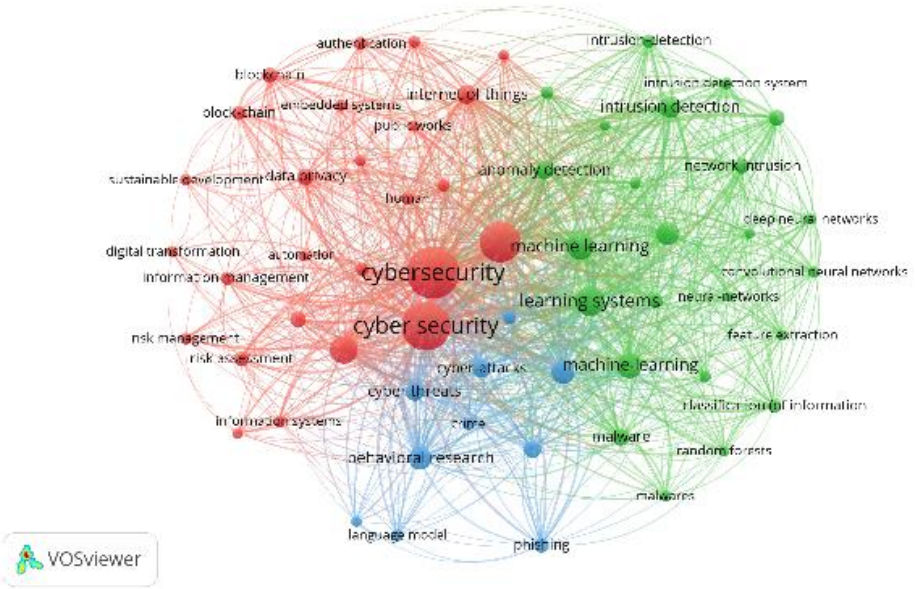

Figure 4. Network Visualization
Source: Data Analysis

From the visualized network graph, we can observe that the terms “cybersecurity” and “cyber security” are positioned centrally within the graph. This is because these two terms can be seen to be the overarching terms that link all other research topics together. The size of their nodes, as well as the number of links attached to them, denotes that these are umbrella terms that cover a broad spectrum of research articles. These are further surrounded by other keywords, namely “machine learning,” “deep learning,” and “learning systems.”

Another one of the prominent clusters is illustrated in green, and it mainly highlights the technical methodologies in the context of intrusion detection systems, network security, and anomaly detection. The key terms such as "intrusion detection," "network intrusion," "feature extraction," and "classification" highlight the high level of focus on developing automated and algorithmic solutions to detect cyber threats.

Another important group of keywords in red deals with general cybersecurity issues, which go beyond technical factors. Key terms such as "blockchain," "internet of things," "digital transformation," "risk management," and "information systems" show that cybersecurity research encompasses more than technical aspects. The use of blockchain and IoT implies that the emergence of new technologies poses fresh security challenges and requires researchers to develop novel approaches to protect interconnected networks.

Blue cluster represents the contribution of the concept of deep learning in application areas of cybersecurity. Keywords such as “deep learning,” “malware,” “phishing,” and “behavioral research” suggest that the study is more concerned about specific forms of cyber threats and ways of detecting and preventing these threats through advanced data analytics techniques. The blue cluster demonstrates how researchers now use big data for threat detection and behavioral analysis as an important method for analyzing potential cyber risks.

The visualized co-occurrence of keyword overlay through the use of VOSviewer illustrates the development of the subject area of cybersecurity throughout time according to the average publication date. From this figure, node coloring depicts the recentness of topic research, with darker node colors indicating older topics and lighter colors indicating newer topics. Thus, this enables one to identify how the research scope

has changed over time and new areas of interest that have emerged.

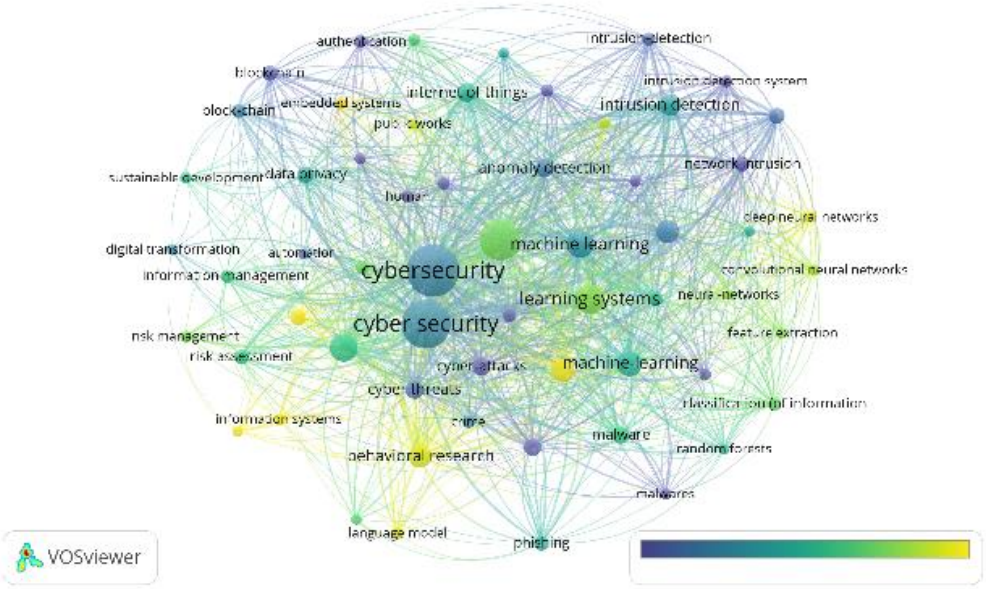

Figure 5. Overlay Visualization

Source: Data Analysis

The chart above reveals that fundamental concepts like "intrusion detection," "network security," and "information systems" are colored darker, which means they have already been widely researched previously in this area. Such concepts serve as the primary technical background of this field, since they concern classical ways of protecting information systems and detecting potential attacks. Despite all the innovations in cybersecurity, these notions are still important.

Recent advances are captured by the terms "machine learning," "deep learning," and "learning systems," which are presented in lighter color gradients. This shows that there is an obvious move towards the application of intelligent technologies in cybersecurity. It becomes evident that the increasing importance of these areas implies that scientists employ the potential of artificial intelligence in order to improve their efficiency in dealing with potential threats, as well as to perform automatic procedures and forecasting.

Moreover, the emergence of terms such as "blockchain," "internet of things," and "behavioral research" is a sign of new trends that have emerged in the field of cybersecurity research to tackle modern issues. Such topics point to a trend where the discipline of cybersecurity is expanding to cover aspects such as decentralized networks, internet of things, and behavioral issues related to cyber security.

The density visualization of keyword co-occurrence analysis created through the use of VOSviewer is used to provide an overview of the density and intensity of the research subjects in the cybersecurity discipline. As seen in Figure 6, the high density (yellow to light green) represents the frequently occurring research subjects in cybersecurity that also exhibit high interconnectivity, whereas the low density refers to subjects that are not widely discussed yet.

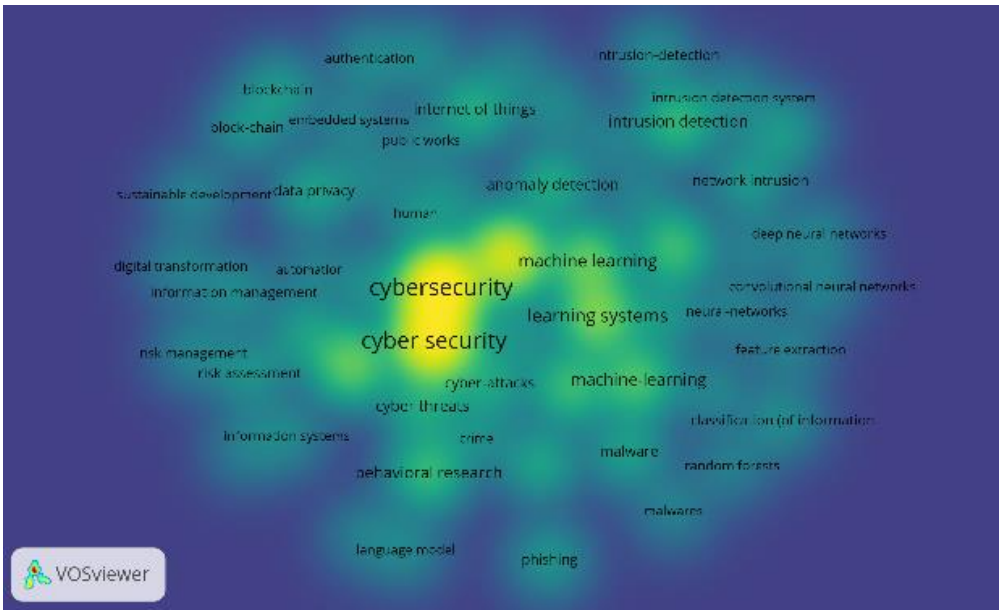

Figure 6. Density Visualization

Source: Data Analysis

As can be seen from the visualization, the two keywords "cybersecurity" and "cyber security" are at the highest density zones in the map, which indicates that they are the two key concepts that are frequently discussed in this domain. In the vicinity of these core keywords, there are several high density zones, where such keywords as "machine learning", "deep learning", and "learning systems" can be found, indicating that the use of AI has become one of the hottest topics in recent years. On the other hand, regions with fewer densities, including those associated with "blockchain," "internet of things," "behavioral research," and "risk management," seem to be scattered and less focused. This suggests that although these topics are part of the research area, they are still either emerging or developing as opposed to those well-established topics. This pattern suggests possible directions for future studies to examine these sparse regions, especially when dealing with multi-disciplinary problems and extending cybersecurity research beyond technical aspects.

Discussion

The results of this study show that cybersecurity studies have gone through considerable changes during the time span 2000-2026, shifting from being a discipline characterized by a focus on technical and systems perspectives to one that is multidisciplinary in nature. The co-authorship network shows that although cohesive clusters are present, the whole framework is somewhat fragmented, with few leading clusters and bridging nodes that enable the flow of information. This indicates that although collaboration is growing, there is much scope left for achieving greater globalization, especially in areas where connectivity is low.

Based on the citation analysis, one can conclude that the intellectual roots of research in the domain of cybersecurity have been significantly affected by scholarly papers discussing artificial intelligence, machine learning, and deep learning. Popular academic papers are no longer concerned only with cybersecurity; instead, they cover methodologies that are not necessarily relevant only to cybersecurity but rather can be applied in other fields. In other words, this demonstrates that there has been a fundamental shift towards a new approach to cybersecurity, which sees cybersecurity not as a standalone domain but as an integral part of a broader technological landscape.

Keyword co-occurrence and keyword density further reinforce the trend through

their findings that machine learning and deep learning have become important topics in cybersecurity literature. These topics have become important because they are increasingly utilized for different purposes such as intrusion detection, malware analysis, and phishing detection. In addition, clusters related to blockchain, IoT, and behavioral science further emphasize how the domain has evolved over time to include new challenges. This implies that modern cybersecurity challenges cannot be resolved using simple security measures but require comprehensive security strategies based on complex solutions that integrate technology, organization, and human behavior.

Moreover, the temporal overlay chart reveals further information about the temporal development of the topic area in question. There is a noticeable shift in research topics from basic issues, such as network security and intrusion detection, to more sophisticated techniques. Novel areas, including artificial intelligence-based security, decentralized technologies, and human-centered cybersecurity, are receiving increasing attention, implying that the future of research will concentrate more on preventive and intelligent solutions to cybersecurity threats. This indicates a tendency that corresponds with the general digital transformation taking place in all sectors of society.

It is hoped that the study will add value to knowledge concerning developments in the field of cybersecurity studies by providing insights on structural, intellectual, and thematic evolutions in this area. The results show that it would be necessary to pay special attention to collaboration, especially between regions, and to continue developing interdisciplinary perspectives, which would include the integration of advanced technological solutions and conventional security strategies. Further research efforts could focus on less-researched areas like behavioral and policy studies in cybersecurity to address social and technical issues related to cyber risks.

4. CONCLUSION

This paper proves that cybersecurity studies have become an ever-changing area of science due to the significant influence of AI, ML, and other data-related developments on cybersecurity. The analysis shows that there is a trend towards growing international cooperation in cybersecurity studies, although the pattern remains quite unbalanced, as certain countries and organizations dominate in the field. The results of conceptualization demonstrate that cybersecurity is moving from classic security systems to the use of artificial intelligence in securing data. Other notable themes include blockchain technology, IoT security, and behavioral cybersecurity. Although this area has come a long way, many issues have yet to be addressed regarding international cooperation and social considerations.

REFERENCES

[1] H. M. Alzoubi *et al.*, "Cyber Security Threats on Digital Banking," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, IEEE, 2022, pp. 1–4.

[2] M. A. Rahman, "Subduing Cyber Threats to Secure the Financial Sector of Bangladesh," *Cybersecurity, Privacy, & Networks eJournal*, vol. 2, no. 78, 2019.

[3] I. Mustapha, Y. Vaicondam, A. Jahanzeb, B. A. Usmanovich, and S. H. B. Yusof, "Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem.," *Int. J. Interact. Mob. Technol.*, vol. 17, no. 22, 2023.

[4] R. Ganesen, A. A. Bakar, R. Ramli, F. A. Rahim, and M. N. A. Zawawi, "Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 8, 2022.

[5] D. Widiyati, "Pengaruh Literasi Keuangan, Perlindungan Data, dan Cybersecurity Terhadap Penggunaan Financial Technology," *Jae (Jurnal Akunt. dan Ekon.*, vol. 9, no. 1, pp. 130–141, 2024.

[6] O. P. Olaiya, T. O. Adesoga, A. Ojo, O. D. Olagunju, O. O. Ajayi, and Y. O. Adebayo, "Cybersecurity strategies in fintech: safeguarding financial data and assets," *GSC Adv. Res. Rev.*, vol. 20, no. 1, pp. 50–

56, 2024.

[7] O. O. Amoo, A. Atadoga, F. Osasona, T. O. Abrahams, B. S. Ayinla, and O. A. Farayola, "GDPR's impact on cybersecurity: A review focusing on USA and European practices," *Int. J. Sci. Res. Arch.*, vol. 11, no. 1, pp. 1338–1347, 2024.

[8] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *J. Bus. Res.*, vol. 133, pp. 285–296, 2021.

[9] N. Van Eck and L. Waltman, "Software survey: VOSviewer, a computer program for bibliometric mapping," *Scientometrics*, vol. 84, no. 2, pp. 523–538, 2010.

[10] L. Alzubaidi *et al.*, "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," *J. big Data*, vol. 8, no. 1, p. 53, 2021.

[11] I. H. Sarker, "Machine learning: Algorithms, real-world applications and research directions," *SN Comput. Sci.*, vol. 2, no. 3, pp. 1–21, 2021.

[12] I. H. Sarker, "Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions," *SN Comput. Sci.*, vol. 2, no. 6, pp. 1–20, 2021.

[13] M. Sallam, "ChatGPT utility in healthcare education, research, and practice: systematic review on the promising perspectives and valid concerns," in *Healthcare*, MDPI, 2023, p. 887.

[14] R. Nishant, M. Kennedy, and J. Corbett, "Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda," *Int. J. Inf. Manage.*, vol. 53, p. 102104, 2020.

[15] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," in *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, 2018, pp. 2154–2156.

[16] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, 2011.

[17] Y. Xin *et al.*, "Machine learning and deep learning methods for cybersecurity," *Ieee access*, vol. 6, pp. 35365–35381, 2018.

[18] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. De Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, 2017.

[19] I. H. Sarker, "AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems," *SN Comput. Sci.*, vol. 3, no. 2, p. 158, 2022.