West Science Information System and Technology
Vol. 2, No. 03, December 2024, pp. 374~382

Mapping the Cybersecurity Research through Bibliometric Analysis

Loso Judijanto[1], Endrixs Endrianto[2], Arnes Yuli Vandika[3]
[1]IPOSS Jakarta
[2]Institut Telnologi Petroleum Balongan
[3]Universitas Bandar Lampung

Article Info

Article history:

Received December, 2024
Revised December, 2024
Accepted December, 2024

Keywords:

Cybersecurity
Advanced Technologies
Innovation
Bibliometric Analysis

ABSTRACT

This bibliometric analysis explores the evolution and global landscape of cybersecurity research from 2010 to 2024. Utilizing data sourced exclusively from Scopus and analyzed through VOSviewer, this study identifies significant trends, key themes, and the dynamics of international collaboration within the field. The findings reveal a notable increase in the volume of publications over the years, highlighting a shift from basic security measures towards the integration of advanced technologies such as artificial intelligence, the Internet of Things (IoT), and blockchain. The study also maps the dense network of international collaborations, with the United States, China, India, Germany, and the United Kingdom emerging as central nodes. This analysis not only reflects the increasing complexity of cyber threats but also the global effort to develop proactive and dynamic defense mechanisms. The results emphasize the need for continuous innovation and expanded international cooperation to address the challenges posed by rapidly evolving cyber threats. Future research should consider more interdisciplinary approaches and a wider range of databases to capture the full spectrum of cybersecurity research.

Corresponding Author:

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

1. INTRODUCTION

In the contemporary digital era, cybersecurity stands as a critical concern for governments, organizations, and individuals worldwide. As technology rapidly evolves, so does the complexity of cyber threats, necessitating advanced defenses in cybersecurity infrastructure. The immense expansion in digital data and reliance on cloud services has broadened attack surfaces, making effective cybersecurity mechanisms indispensable [1]. The ever-increasing sophistication of cyber-attacks requires continual advancements and innovations in cybersecurity strategies and technologies. Notably, the global cybersecurity market reflects this urgency, with projections estimating a growth to approximately $366 billion by 2028, up from $202 billion in 2021, indicating a significant focus on fortifying digital assets [2].

Historically, cybersecurity research has pivoted from focusing merely on technological defenses to integrating psychological and sociological aspects, considering the human factors influencing cybersecurity practices [3]. This shift acknowledges that cybersecurity is not only a technical challenge but also a human one, where user behavior plays a pivotal role in the effectiveness of security measures. The interdisciplinary nature of cybersecurity research, which now encompasses fields such as machine learning, data analytics, and human behavior, necessitates a systematic approach to understanding its evolution and current trends. This approach ensures that stakeholders can develop comprehensive strategies that address both technological and human-centric vulnerabilities.

The academic and practical landscapes of cybersecurity research are continually influenced by emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT). These technologies, while presenting new opportunities for enhancing security measures, also introduce unique vulnerabilities that cybercriminals can exploit [4]. The integration of AI in cybersecurity, for instance, offers the potential for predictive security measures but also raises concerns about the ethical use of AI and the possibility of AI-driven attacks. Similarly, the proliferation of IoT devices expands the vector for cyber-attacks, necessitating research into robust security protocols that can operate effectively at scale and in diverse environments [5].

Moreover, the regulatory and policy frameworks surrounding cybersecurity are continually evolving, as governments and international bodies strive to keep pace with technological advances. The complexities of cybersecurity legislation and the need for international cooperation in cyber defense mechanisms underscore the importance of a global perspective on cybersecurity research. As such, mapping the existing research through bibliometric analysis can provide valuable insights into the most influential studies, prevailing research trends, and potential gaps in the literature that future investigations could address.

Despite the critical importance and dynamic nature of cybersecurity research, there is a notable lack of comprehensive analyses that map out the field's developmental trajectory and current state. Traditional literature reviews, while insightful, often do not capture the extensive scope and interconnectedness of the varied research themes within cybersecurity. Furthermore, the rapid pace at which new cybersecurity technologies and threats emerge can render conventional reviews outdated quickly. Therefore, a more structured and quantifiable approach, such as bibliometric analysis, is essential to objectively measure the impact and evolution of cybersecurity research over time and identify the most impactful themes and contributors in the field.

The objective of this study is to conduct a bibliometric analysis of the cybersecurity research landscape. This analysis aims to uncover the developmental trends, key themes, and influential works within the field over the past decade. By mapping these elements, the study seeks to provide a comprehensive overview that can serve as a foundation for academics, practitioners, and policymakers to understand the evolution of cybersecurity issues and solutions, fostering better-informed strategies for future research and practical cybersecurity applications.

The Evolution of Cybersecurity Threats and Strategies

Cybersecurity has undergone a significant evolution, transitioning from basic protocols to sophisticated systems designed to counteract advanced cyber threats. Initially, the focus was predominantly on creating firewalls and antivirus software as fundamental barriers against intrusion [6]. However, as the landscape of cyber threats has evolved, so has the approach to cybersecurity. Today, the focus has shifted towards more comprehensive strategies that encompass not only technological solutions but also procedural and human factors. [7] highlights the shift towards integrated cybersecurity frameworks that leverage data analytics and machine learning to predict and mitigate potential breaches before they occur. This proactive approach is crucial in a landscape where cyber threats are increasingly sophisticated and pervasive.

Human Factors in Cybersecurity

The role of human behavior in cybersecurity has been a growing area of interest. Studies have shown that despite advanced security systems, human error remains one of the most significant vulnerabilities within cybersecurity frameworks [8]. Social engineering attacks, such as phishing and baiting, exploit human psychology and are continuously adapting to bypass the increasing awareness and training among users. [6] explored the impact of continuous education on reducing human-related security breaches and found that regular, engaging training significantly enhances the security posture by equipping individuals with the knowledge to identify and avoid potential threats.

Cybersecurity in the Era of IoT and AI

The integration of IoT and AI in various sectors has introduced new cybersecurity challenges. IoT devices often lack the robust security features that are standard in more traditional computing environments, making them susceptible to attacks [9]. Furthermore, as AI begins to play a more integral role in cybersecurity, it also becomes a target for attacks. AI systems can be manipulated through data poisoning or model evasion strategies, complicating the cybersecurity landscape [10]. [11] discuss the dual use of AI in cybersecurity, highlighting how AI can enhance security through predictive analytics while also posing risks through its potential exploitation by cybercriminals.

Regulatory and Ethical Issues in Cybersecurity

The regulatory landscape of cybersecurity is as dynamic as the technological aspects. With different countries implementing varied cybersecurity policies, the need for a harmonized regulatory framework is evident. [12] discusses the challenges of aligning international cybersecurity laws, which are essential for managing cross-border cybercrime and ensuring a cohesive response to global cybersecurity threats. Additionally, the ethical use of cybersecurity technologies, particularly concerning AI, poses significant debates. Ethical considerations include the potential for surveillance, privacy breaches, and the development of AI-driven offensive cybersecurity measures [11].

2. METHODS

This study utilizes bibliometric analysis, focusing exclusively on data sourced from the Scopus database, known for its extensive repository of peer-reviewed literature. The analysis is confined to articles and reviews published within the field of cybersecurity. Keywords used for the initial search include "cybersecurity," "information security," "network security," and related terms to capture the breadth of research in this area. The timeframe for the literature search spans from the year 2000 to the present, ensuring a comprehensive view of both historical and contemporary trends in cybersecurity research. To conduct the analysis, the study employs VOSviewer, a tool specifically designed for constructing and visualizing bibliometric networks. These networks will include co-citation, bibliographic coupling, and co-authorship analyses to pinpoint the most influential researchers, seminal publications, and emergent themes within the cybersecurity domain. VOSviewer will also be used to perform keyword co-occurrence analysis, which helps in identifying the evolving focus areas and trends within the collected literature

3. RESULTS AND DISCUSSION

3.1 Yearly Publication

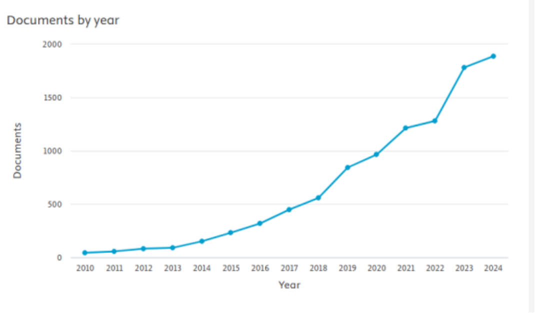

Figure 1. Documents by Year
Source: Scopus, 2024

The figure 1 above depicts a clear and steady increase in the number of documents published annually in the field of cybersecurity from 2010 to 2024. Starting from below 100 documents in 2010, there is a gradual upward trajectory reaching approximately 500 documents by 2015. This growth becomes more pronounced from 2015 onwards, with the curve steepening significantly, indicating an accelerated interest and investment in cybersecurity research. By 2020, the publications exceed 1000 documents per year, and this momentum continues with a slight plateau observed in 2023 before rising again in 2024. The overall trend suggests a robust expansion in cybersecurity research, likely driven by the escalating complexity and frequency of cyber threats, highlighting the growing global recognition of the importance of cybersecurity in safeguarding information and systems in an increasingly digital world.

3.2 Top Affiliations

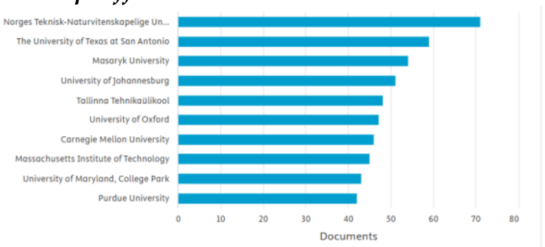

Figure 2. Documents by Affiliation
Source: Scopus, 2024

The bar graph illustrates the number of cybersecurity-related documents published by various universities around the world. Norges Teknisk-Naturvitenskapelige Universitet leads with the highest number, approaching 80 documents. This is followed closely by The University of Texas at San Antonio and Masaryk University, both also active contributors to the field with nearly 70 and over 60 documents, respectively. Other notable institutions include the University of Johannesburg, Tallinna Tehnikaülikool, and the University of Oxford, each contributing significantly with document counts ranging from about 40 to 60. Prestigious institutions like Carnegie Mellon University, Massachusetts Institute of Technology, University of Maryland, College Park, and Purdue University are also key players, each publishing between 30 and 60 documents. This distribution indicates a robust international effort in advancing cybersecurity research, with contributions spanning from the United States to Europe and Africa, reflecting the global priority of addressing cybersecurity challenges.

3.3 Keyword Co-Occurrence Network

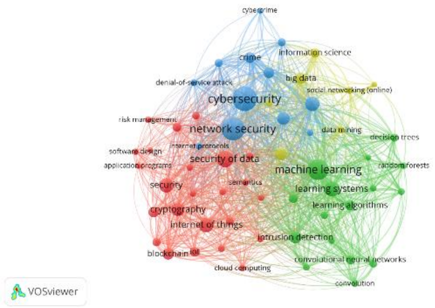

Figure 3. Network Visualization
Source: Data Analysis, 2024

The visual depicted by VOSviewer illustrates the interconnected research landscape in cybersecurity, presenting a robust network of themes that highlight the complexity and breadth of the field. The network is segmented into several clusters, each represented by different colors, indicating the thematic focus and relationships among various cybersecurity topics. Central to the visualization is "cybersecurity," "network security," and "security of data," signifying their roles as foundational aspects in the study of cybersecurity. These nodes act as pivotal points, with numerous connections to other specialized topics, underscoring their broad relevance across the field.

One significant cluster highlighted in blue focuses on the issues of cybercrime, including "denial-of-service attack" and broader crime-related themes. This cluster is closely linked to "cybersecurity," indicating a strong emphasis on protective measures against malicious activities in digital environments. The proximity of these nodes to "internet protocols" and "information science" suggests a scholarly focus on developing more secure systems and enhancing the understanding of how cyber threats operate within the complex webs of internet infrastructure. Another vibrant cluster in red revolves around "cryptography," "internet of things (IoT)," and "blockchain." This cluster indicates a deep dive into technologies that secure communications, data integrity, and transactions in the increasingly connected world. The presence of "IoT" at the core of this cluster alongside "blockchain" points to the growing importance of securing distributed networks and devices, a critical concern as the number of internet-connected devices escalates globally. The linkage between these and "cloud computing" reflects the integrated nature of modern digital infrastructures requiring advanced security protocols.

The green cluster showcases the integration of "machine learning" and "data mining" with cybersecurity efforts, highlighting the advancing role of artificial intelligence in threat detection and response. Keywords such as "learning algorithms," "convolutional neural networks," and "intrusion detection" suggest a trend towards leveraging AI to automate and enhance the accuracy of identifying potential security breaches. This cluster's connection to "decision trees" and "random forests" illustrates the use of sophisticated analytical techniques to interpret complex data patterns, aiding in proactive cybersecurity defenses. These technological advancements represent a significant shift towards predictive cybersecurity measures, aiming to stay ahead of potential threats through innovative research and applications.

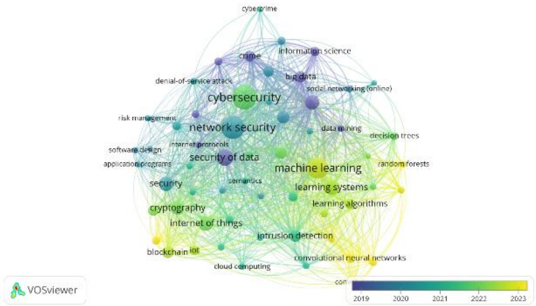

Figure 4. Overlay Visualization
Source: Data Analysis, 2024

The second visualization showcases the temporal evolution and concentration of research topics in cybersecurity from 2019 to 2023, as indicated by the color gradient from yellow to blue across the network. This temporal mapping indicates not only the focal areas of study but also the shifts in research attention over the years. The nodes colored in yellow, which represent earlier years in this timeframe, are predominantly focused on foundational technologies like "blockchain," "cloud computing," and "Internet of Things (IoT)," suggesting a strong initial emphasis on securing emerging digital infrastructures. As we move towards the blue nodes, indicative of more recent research from 2022 to 2023, there is a noticeable shift towards "machine learning," "data mining," and "intrusion detection," reflecting an advanced integration of artificial intelligence in cybersecurity practices.

The network illustrates the dynamic interplay between various cybersecurity domains, where foundational elements like "network security" and "security of data" remain consistently relevant, serving as hubs that connect older and newer technological concerns. The sustained prominence of these core topics over time underscores their enduring importance in the cybersecurity field, while the evolving connections to newer technologies like "convolutional neural networks" and "learning algorithms" highlight the field's adaptation to leverage AI for enhanced security measures. This evolution mirrors the broader technological landscape where AI's role in predictive analytics and threat detection becomes critical amidst increasingly sophisticated cyber threats.

The visualization also highlights the interdisciplinary nature of cybersecurity research, with nodes connecting across different technological and application domains. The convergence of "big data" and "social networking (online)" with cybersecurity themes points to the growing concern over data privacy and security in the era of massive information sharing and social media. The spread and intensity of the connections across the network emphasize the complex and interconnected challenges that cybersecurity research aims to address, reflecting a comprehensive approach that spans technical, social, and ethical dimensions to safeguard information and infrastructures in an increasingly digitalized world.

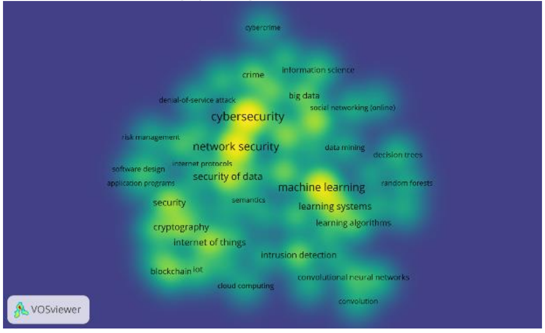

Figure 5. Density Visualization
Source: Data Analysis, 2024

The visualization presents a thematic heatmap of the most prevalent topics within cybersecurity research, arranged to show the central and surrounding themes based on their interrelatedness and prevalence in the literature. At the core, the terms "cybersecurity," "network security," and "security of data" form a foundational trio reflecting the primary focus areas within the field. These central topics are tightly linked to both traditional aspects such as "risk management," "software design," and "cryptography," and more modern technological elements like "internet of things (IoT)" and "blockchain IoT." This arrangement underscores the dual focus on improving traditional security measures and adapting to newer technological challenges.

Surrounding these core topics are advanced computational techniques and emerging trends, including "machine learning," "data mining," and "convolutional neural networks." The proximity of "machine learning" and related terms to core cybersecurity topics illustrates the growing integration of AI and machine learning algorithms in developing advanced cybersecurity solutions, particularly in intrusion detection and handling the vast amounts of data generated by modern networked environments. The layout of these nodes, with a gradient from traditional to more advanced topics, highlights the evolutionary path of cybersecurity research from foundational security measures to incorporating sophisticated, data-driven technologies to protect against increasingly complex threats.

3.4 Citation Analysis

Table 1. Top Cited Literature

Citation	*Author*	*Title*
834	[13]	Machine Learning and Deep Learning Methods for Cybersecurity
578	[6]	A survey of emerging threats in cybersecurity
481	[10]	Blockchain's roles in strengthening cybersecurity and protecting privacy
392	[7]	Internet of things (IoT) cybersecurity research: A review of current research topics
388	[14]	Cybersecurity data science: an overview from machine learning perspective
383	[15]	Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks
365	[8]	Cybersecurity for critical infrastructures: Attack and defense modeling
291	[16]	The Cybersecurity Landscape in Industrial Control Systems
282	[4]	Cybersecurity in healthcare: A narrative review of trends, threats and ways forward
270	[3]	Cybersecurity for Industry 4.0 in the current literature: A reference framework

3.5 Co-Authorship Network

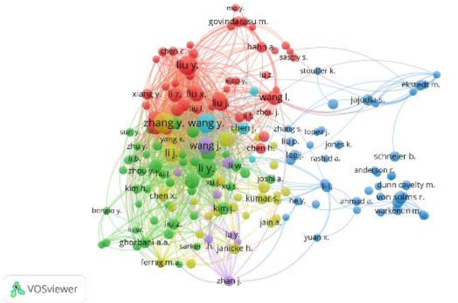

Figure 6. Author Visualization

Source: Data Analysis, 2024

This VOSviewer visualization depicts a co-authorship network among researchers in the field of cybersecurity, showcasing the collaborative interactions and prominent scholars in this domain. The network is color-coded into three distinct clusters—red, green, and blue—each representing a different community or research group likely focusing on various aspects of cybersecurity. The red cluster, which includes prolific authors such as "Liu Y.," "Chen X.," and "Wang Y.," suggests a dense, highly interconnected group, possibly indicating a focus on foundational cybersecurity technologies or methodologies. The green cluster includes researchers like "Kim J." and "Jain A.," pointing towards a collaborative group possibly engaged in applied cybersecurity research or innovative security solutions. Meanwhile, the blue cluster, with nodes like "Jajodia S." and "Stouffer K.," might represent a network focusing on strategic and policy aspects of cybersecurity.

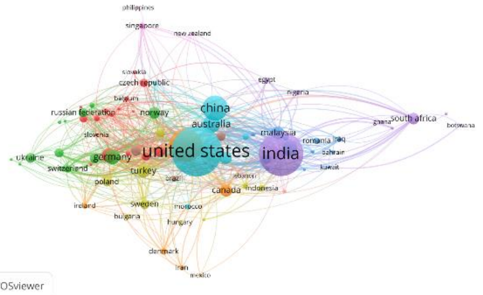

Figure 7. Country Visualization

Source: Data Analysis, 2024

This VOSviewer map illustrates the global collaboration network among countries engaged in cybersecurity research, highlighting the most active nations and the extent of their interactions. Central to this network, the United States appears as a significant hub, depicted in a larger node size, indicating its dominant role in global cybersecurity research and collaborations. Other prominent countries like China, India, Germany, and the United Kingdom are also key players, with substantial contributions to the field, suggesting robust research outputs and international partnerships. The diverse array of connections between these countries across different continents underscores the global nature of cybersecurity challenges and the collaborative efforts required to address them. Smaller nodes such as those representing countries in Eastern Europe, Southeast Asia, and Africa, while less prominent, indicate emerging participants in this crucial field, highlighting the expanding recognition of cybersecurity as a global priority.

DISCUSSION

The bibliometric analysis presented in this study offers a comprehensive overview of the global landscape of cybersecurity research from 2010 to 2024, revealing significant insights into the evolution of research themes and the dynamics of international collaboration. The findings indicate a robust growth in the volume of publications over the years, which underscores the escalating importance of cybersecurity as a critical area of concern for governments, organizations, and individuals worldwide.

Evolution of Research Themes

Initially, the focus of cybersecurity research was predominantly on basic protective measures such as firewalls and antivirus software. However, the data extracted from recent publications indicates a paradigm shift towards more sophisticated technologies and methodologies. The rise of machine learning and artificial intelligence in cybersecurity is particularly noteworthy. These technologies are increasingly employed to enhance predictive capabilities and automate the detection of threats and anomalies. This shift not only reflects the advancement in technology but also the growing complexity of cyber threats that require more proactive and dynamic defense mechanisms. Moreover, the integration of cybersecurity with the Internet of Things (IoT) and blockchain technology highlights the field's response to the expanding scope of digital connectivity and the need for secure transactions and data integrity in decentralized networks. The prominence of these themes in recent literature points to a critical evolution from a reactive to a predictive and preventive cybersecurity posture, leveraging cutting-edge technologies to anticipate, identify, and neutralize threats before they manifest.

International Collaboration in Cybersecurity Research

The analysis of collaboration networks provides an interesting perspective on how geopolitical and economic factors influence research partnerships. The United States, China, India, Germany, and the United Kingdom emerge as central nodes in the global network, which is indicative of their substantial investments in cybersecurity research and development. The dense network of collaborations among these countries highlights a shared recognition of the strategic importance of cybersecurity and a concerted effort to advance the field through international cooperation. However, the presence of smaller nodes and the participation of countries from regions such as Eastern Europe, Southeast Asia, and Africa suggest that cybersecurity is increasingly being recognized as a global issue that transcends national borders. The involvement of these countries, although currently limited, is crucial for developing a holistic global cybersecurity strategy. This trend towards wider international collaboration is likely driven by the universal vulnerability to cyber threats and the understanding that effective cybersecurity solutions require diverse perspectives and expertise.

Strategic Implications and Future Research Directions

The growing complexity of cybersecurity threats, coupled with the rapid pace of technological change, calls for continuous innovation in research and development. The strategic implications of the findings from this study are manifold. For policymakers and practitioners, understanding the key trends and shifts in research focus can help in allocating resources effectively and formulating policies that foster innovation and collaboration in cybersecurity. Furthermore, the interdisciplinary nature of modern cybersecurity solutions, as evidenced by the integration of AI, IoT, and blockchain technologies, suggests that future research should focus on cross-sectoral studies that explore the synergies between cybersecurity and other fields such as data science, engineering, and behavioral science. Such interdisciplinary approaches are crucial for developing comprehensive security solutions that address both the technological and human elements of cybersecurity.

Challenges and Limitations

Despite the valuable insights derived from this study, there are inherent challenges and limitations that need consideration. The dynamic nature of cybersecurity threats means that the landscape of research is continually evolving. Bibliometric analyses, while useful, may not capture the most current trends or the full spectrum of global research activities due to delays in publication and indexing in databases. Additionally, the study's reliance on Scopus and VOSviewer for data extraction and visualization may overlook relevant research contributions that are not indexed in these platforms. Future studies could expand the range of databases and tools used for analysis to provide a more comprehensive overview of the field.

4. CONCLUSION

This bibliometric analysis of cybersecurity research has illuminated the evolving landscape of the field, showcasing significant growth in publication volume and a shift towards integrating advanced technologies such as AI, IoT, and blockchain. The study highlights the central role of countries like the United States, China, India, Germany, and the United Kingdom in driving global research efforts, while also pointing to an increase in international collaborations that bridge diverse geographic and economic contexts. These findings underscore the critical nature of cybersecurity as a global priority, necessitating continuous innovation and broad-based cooperation to effectively counteract the growing sophistication of cyber threats. Future research should prioritize interdisciplinary approaches and expand analytical frameworks to include more diverse databases and real-time data, ensuring that the insights remain relevant and actionable in a rapidly advancing technological landscape. This study not only maps the current state of cybersecurity research but also sets the stage for future strategic developments in this vital area of global security.

REFERENCES

[1] S. Sood and A. Kim, "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," *Int. J. Innov. Econ. Dev.*, vol. 9, no. 2, pp. 7–23, 2023, doi: 10.18775/ijied.1849-7551-7020.2015.92.2001.

[2] A. Nelson and S. Wang, "The importance of cybersecurity disclosures in customer relationships," *J. Corp. Account. Financ.*.

[3] M. Lezzi, M. Lazoi, and A. Corallo, "Cybersecurity for Industry 4.0 in the current literature: A reference framework," *Comput. Ind.*, vol. 103, pp. 97–110, 2018.

[4] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, 2018.

[5] C. Caddy, "Cybersecurity and Digital Components: Supply Chain Deep Dive Assessment," USDOE Office of Policy (PO), Washington DC (United States), 2022.

[6] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2014.

[7] Y. Lu and L. Da Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, 2018.

[8] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst. Man, Cybern. A Syst. Humans*, vol. 40, no. 4, pp. 853–865, 2010.

[9] A. H. Brown and T. D. Green, *The essentials of instructional design: Connecting fundamental principles with process and practice*. Routledge, 2019.

[10] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecomm. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[11] C. Mavani, H. K. Mistry, R. Patel, and A. Goswami, "The Role of Cybersecurity in Protecting Intellectual Property," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 12, no. 2, pp. 529–538, 2024.

[12] L. Pina Taylor, "Raising Cybersecurity Awareness and improving Organizational Resilience in the Critical Infrastructure Sector," 2023.

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

[14] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *J. Big data*, vol. 7, pp. 1–29, 2020.

[15] A. Taeihagh and H. S. M. Lim, "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks," *Transp. Rev.*, vol. 39, no. 1, pp. 103–128, 2019.

[16] S. McLaughlin *et al.*, "The cybersecurity landscape in industrial control systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016.