Grenze International Journal of Engineering and Technology, June Issue

Global Research Trends in Cybersecurity: A Scientometric Analysis of Privacy, Threats, and Attack Mitigation

Devender Rondla[1] and N. Venkatesh[2]
[1-2]School of Computer Science and Artificial Intelligence, SR University, Warangal, 506371, India.
Email: 2403C50169@sru.edu.in, venkatesh.naramula@sru.edu.in

***Abstract*— The cybersecurity found its place in contemporary digital society, and the list of threats is growing in size and complexity and range. The paper entails the scientometric similarity of the global analysis trends in the area of cybersecurity which are three of the main pillars are the subject of the study, which are privacy, future threats, and attack mitigation. The results were offered to them using the available bibliographic databases and with the assistance of citation mapping, co-authorship network, and keyword co-occurrence to identify the hotspots in the research, influential publications, and gaps in the knowledge in the field of Cloud Computing, Internet of Things (IoT) & Cyber-Physical Systems(CPS). The most familiar enablers in the innovation of adaptive and explainable cybersecurity models are artificial intelligence, machine learning, and blockchain technologies. Besides highlighting the current direction the research is pursuing, the findings also give the possible future direction of the research, namely AI-based intrusion detection, CPS security and privacy-aware architecture. It is the addition of good literature that can make the scientists do research, and the policy makers improve the body of information on the field of cybersecurity to fit the increasing demands of the world.**

***Index Terms*— Cybersecurity, Privacy, Attack Mitigation, Intrusion Detection, Cyber-Physical Systems (CPS).**

I. INTRODUCTION

One of the pillars of the modern digital society is cybersecurity, which is critical in the context of security of large volumes of sensitive data that are generated and transferred in networks of interconnected systems [2]. The development of technology that might be advantageous to the population does present new opportunities as well as threats to overcome, with malicious intent and establish itself, which must be overcome by developing dynamic and adaptive security [5]. Such kind of threat as malware (ransomware and Trojans), social engineering, phishing attacks, DDoS attacks and SQL injections can result in the loss of a massive amount of money and loss of reputation [4],[5]. Specifically, these threats are reinforced by such risks as AI-based attacks, the possibility of impersonation with the help of a deep fake avatar, and attacks on digital objects, including NFTs [2]. The benefits of digital identities are rather significant. The disruption of the functionality harmed the security of the patients [5] The most severe and irreversible privacy risk [2].

Grenze ID: 01.GIJET.12.2.425_22

The type of attack that consists of manipulating individuals to give up personalized information [3],[4]. This may be avoided by ensuring confidentiality of the data and limiting access to specific information to authorised users[5] in most cases, the law prescribes privacy and security of information of users and cybersecurity [9],[15] is a multi-layered system that makes it effective. This involves reacting to unauthorised access and attacks [5]. Future technologies such as blockchain and NFTs [2] are secure. Cybersecurity is also not a stagnant discipline; it is a dynamic process that has to be modified to every new technology and the evolution of threats [5] of the new technology.

It should conduct research to develop innovative and resilient solutions, including security models of Internet of Things devices that are lightweight in smarter cities and fraud detection that is powerful in FinTech [4],[5] This significance is justified by the fact that cyber threats [14] continue to evolve continuously to steal personal and financial information on sensitive aspects of all the individuals in the digital sectors. The fast development of Cloud Computing, Internet of Things (IoT) & Cyber-Physical Systems(CPS) has introduced complicated security and privacy and threat mitigation challenges, and now cybersecurity has become an important topic in the world of the contemporary digital world. The growing number and sophistication of cyberattacks, as well as the application of AI and the occurrence of major data breaches, evoke the necessity to gain a comprehensive insight into the existing research trends and technologies reactions. It is thus timely and important to analyse the global trends in studies concerning cybersecurity, privacy protection and mitigation of attacks. In that way, one can state that the topic of the proposed research is very topical as it will enable systematically presenting the constantly evolving area of cybersecurity and assist researchers and policymakers with determining research gaps, the direction, and priorities. Bibliometric and scientometric analysis is a logical and objective method of analysing numerous academic sources and determining essential research patterns. Bibliometric methods can be applied to identify the most influential publications, their institutions of origin, the tendency to collaborate, and the new topics in cybersecurity research through the application of citation analysis, co-authorship network, and co-occurrence of the keywords. Applied to the case of cybersecurity, privacy, and attack mitigation, this methodology comes in handy to explain that technologies and threat environments are dynamic. The bibliometric analysis of the study provides the quantitative information that may be used to identify the trends, evaluate the research gaps and inform future research. This will improve the quality of analytical rigour and contribution of the work to the field.

II. METHODOLOGY

This methodology takes a pure scientometric and bibliometric approach in order to study the global cybersecurity research on privacy, emerging threats, and mitigation of attacks. The design is intended to be simple, predictable, and replicable, and it only makes use of bibliometric evaluation, excluding simulations, machine learning experiments, or human validation. The approach to it is a four-stage process. First, search queries were made in the Scopus database using a predetermined search query and restricted to English-language articles of 2020 to 2025. Second, preprocessing of data was done to eliminate duplicates and sieve the documents according to relevance. Third, bibliometric analysis was done through VOSviewer, CiteSpace, and Biblioshiny using bibliometric analysis, citation analysis, Co-authorship Networks, Keywords Co-occurrence analysis.

Figure 1. Methodology Diagram

The Figure 1 approach incorporates the systematic literature review, simulations and machine learning, and expert validation in solving cybersecurity issues across the cyber-physical systems (CPS) [1], fatigue and fracture mechanics, and healthcare security. In the field of fatigue and fracture mechanics (2020-2025).The research trends, thematic cluster, and significant contributors were identified with the help of the visualisation tools (VOSviewer and Cited Space), which supported the insights into damage-tolerant design strategies in the case of CPS security [6]. A targeted literature review also helped to reduce 145 studies to 14 core papers and develop a detailed taxonomy of threats and vulnerabilities in the framework of CPS security [6]. The simulations were designed to recreate cyberattacks [12] such as cross-site scripting and Telnet pivoting, and tested by the mean time to compromise (MTTC) measures at different levels of skills of the attacker. The mitigation strategies were validated with experimental testing of multi-layered defences, including Firewalls, VPNs, and Web Application Firewalls [6]. Mitigation strategies were searched in the IEEE Xplore database, the Acm Digital Library, Scopus, and PubMed with domain-specific keywords and strict inclusion criteria to ensure the timeliness and relevance of their search. Qualitative validation was done by interviewing experts [3],[7] .The XGBoost machine-learning models and the Random Forest trained the models to improve the intrusion detection [13], whereas distributed subspace system-identification methods detected the faults and ensured the control measures [8],[10].The Web of Science and Scopus data showed the machine-learning models with the highest impact, collaboration networks, and research fronts in privacy, attack mitigation, AI-driven defence, and CPS security [10],[16]. CiteSpace, VOSviewer, and Biblioshiny, which combined quantitative analysis with experiments to enhance the research on cybersecurity [11], [15].

Search Key:

(TITLE-ABS-KEY ("Cyber Security") AND TITLE-ABS-KEY ("Privacy") AND TITLE-ABS-KEY ("Intrusion Detection")) AND PUBYEAR > 2019 AND PUBYEAR < 2026 AND (LIMIT-TO (LANGUAGE , "English"))

This Scopus search query retrieves English-language publications from 2020 to 2025 that specifically address cyber security, privacy, and intrusion detection in their titles, abstracts, or keywords.

The dataset in this research was built during a systematised search of bibliographic records at the Scopus database that was chosen on the basis of a wide coverage of high-quality and peer-reviewed literature on the topic of cybersecurity. Titles, abstracts, and keywords were searched using a structured search query that targeted the topics of cybersecurity, privacy, and intrusion detection. Only English-written publications published within the past 2 years to 2025 were searched to identify the current trends and developments in the research.The first search provided a detailed set of records, which has been further narrowed down in the process of filtering. The duplication of entries was eliminated, and the documents were filtered on the basis of relevancy to the scope of the study. The documents of only the types of peer reviews, such as journal articles, conference papers, reviews, book chapters, data papers were preserved. Following the refinement process, a final dataset of 433 documents in 143 sources, 2706 authors, and 3332 references was obtained.The developed curated dataset was the basis of the further scientometric and bibliometric studies, such as the analysis of publication trends, co-authorship relationships, map of keyword co-occurrence, and citation analysis.

TABLE I: OVERVIEW OF METHODOLOGY, DATASET, TOOLS, RESULTS, AND RESEARCH RELEVANCE

Aspect	Description (Methodology / Data / Tools / Results)	Key Technical Parameters	Performance / Evaluation Indicators
Topic Relevance	The paper addresses a timely and significant research area, focusing on cybersecurity[11] challenges related to privacy, emerging threats, and attack mitigation, which are critical concerns in modern digital and cyber-physical [1] environments.	Application domains (IoT, CPS, cloud systems), security threats[14], privacy[9] risks	Research timeliness, societal and technological relevance
Scientometric/Bibliometric Direction Usefulness	Scientometric and bibliometric analysis is used to offer a systematic and quantitative methodology to recognize the trends of research, influential articles, patterns of collaboration, and new themes in cybersecurity[15] research.	Citation analysis, co-authorship networks, and keyword co-occurrence	Trend identification accuracy, insight depth, and analytical usefulness
Methodology Description	The study follows a structured scientometric methodology that includes systematic literature retrieval, bibliometric mapping, and analytical visualisation. The workflow clearly defines data collection, preprocessing, analysis, and interpretation stages to ensure methodological consistency and reproducibility.	Bibliographic databases, keyword strategy, time span (2020–2025), inclusion/exclusion criteria	Reproducibility, methodological consistency

Dataset Explanation	The data is represented by the peer-reviewed articles that were obtained in Scopus and Web of Science with the help of a pre-tested search query specific to the sphere of cybersecurity, privacy, and intrusion detection. Inappropriate duplicate records have been eliminated, and documents in the English language only falling within the specified time frame were kept.	Number of documents, sources, authors, keywords	Dataset transparency, coverage adequacy
Tool Outputs	Co-authorship networks, keyword co-occurrence maps, citation networks and three-field plots comprising bibliometric tools VOSviewer, CiteSpace, and Biblioshiny were used to support quantitative and visual analysis.	Network graphs, clustering algorithms, visualization thresholds	Cluster validity, network density
Results	The analysis reveals rapid growth in cybersecurity research, strong international collaboration, and dominant themes such as intrusion detection, machine learning, IoT security, and CPS security.	Publication count, citation frequency, and collaboration indices	Annual growth rate, citations per paper
Results & Discussion	The discussion systematically interprets the bibliometric findings by linking identified research trends to real-world cybersecurity challenges and future research directions, providing a structured and analytical narrative.	Thematic clusters, keyword evolution	Analytical depth, interpretability

III. Results and Discussion

The bibliometric analysis will include the publications of 2020-2025, with a total of 433 documents being covered by 143 sources. The dataset indicates that research on cybersecurity has a high upward trend with an annual growth of 37.74 and an average of 10.1 citations per document, which indicates that there is a growing interest and effect of this field among academics.

A. Publishing and the Author Characteristics

The analysis has found 2706 authors and an average of 11.1, co-authors per document, which is a high degree of collaborative information activity. There was no literature of single-authored papers & international co authorship represents 28.41 percentage of the publications, which indicates a high level of research cooperation across countries.

B. Institutional and Source Contributions.

The most notable publication sources are Lecture Notes in Computer Science, IEEE Access and Lecture Notes in Electrical Engineering that are used as contributors of a significant proportion of the overall publications. The institutional analysis indicates that the University of Western Macedonia, Mohammed VI Polytechnic University, and Deakin University are some of the most fruitful affiliations in regard to cybersecurity research in the chosen period.

C. Author Productivity

The analysis of productivity of authors by means of Lotaka Law reveals that a few authors make significant proportional contributions to the pool of publications, whereas most authors make a single or two documents. This tendency is in keeping with the existing bibliometric distributions in scientific literature.

D. Keywords and Thematic Analysis.

The analysis of the keywords reveals that there are 1939 Keywords Plus and 2385 Author Keywords, most prominently represented by such keywords as cybersecurity, intrusion detection, and network security. Officials and Research Networks.

The three-field plot analysis demonstrates a good connection between countries, institutions and research themes and highlights the interdisciplinary and global character of cybersecurity research. Examples of countries that have institutional co-operations in major thematic fields include Greece, India, Spain, and the United Kingdom.

The current bibliometric analysis (2020-2025) indicates that cybersecurity research has increased dramatically over the past years, with 433 documents published by 143 sources of those 37.74 ratio of annual growth rate and 10.1 ratio of citations per paper. There is a high level of collaboration with an average of 11.1 co-authors per document, 28.41 percent international partnership, with no single-authored documents. The top colleges are the University of Western Macedonia, Mohammed VI Polytechnic University and Deakin University. Some of the

notable publication sources are Lecture Notes in Computer Science, IEEE Access, and Lecture Notes in Electrical Engineering. The Law of the Lotka substantiates that there are a limited number of writers who do most of the publications. The three field plot emphasises international cooperation between nations, educational institutions, and the emergent issues like cybersecurity, intrusion detection, machine learning, and deep learning.

TABLE II: MAIN INFORMATION

DESCRIPTION	RESULTS
MAIN INFORMATION ABOUT DATA	
Timespan	2020:2025
Sources (Journals, Books, etc)	143
Documents	433
Annual Growth Rate %	37.74
Document Average Age	1.57
Average citations per doc	10.1
References	3332
DOCUMENT CONTENTS	
Keywords Plus (ID)	1939
Author's Keywords (DE)	2385
AUTHORS	
Authors	2706
Authors of single-authored docs	0
AUTHORS COLLABORATION	
Single-authored docs	0
Co-Authors per Doc	11.1
International co-authorships %	28.41
DOCUMENT TYPES	
article	149
book	9
book chapter	26
conference paper	198
conference review	33
data paper	1
review	16

Table 2 above presents the most significant bibliometric information in 2020-25, which consisted of 433 documents retrieved in 143 journals, books, and other sources. It is proud of the average citation rate of 10.1 per document with 2706 authors and no single article authors. There is 11.1 number of co-authors and 28.41 percent proportion of international co-authorship. The types of documents include 149 articles, 198 conference papers, 26 book chapters and so on. The key word analysis indicates that the number of Keyword Plus was 1939 and Author Keywords was 2385.

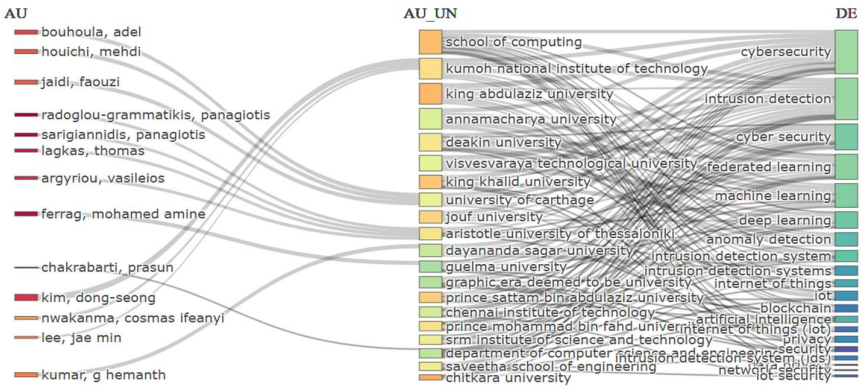

Figure 2. Three Field Plot

Bibliometric analysis of the current research employed scientific tools, including VOSviewer, CiteSpace and Biblioshiny because they were selected because each of them offers tasks which are quite complementary to each other. VOSviewer was applied in order to display and quantify research trends, collaboration, and thematic

change in the area of cybersecurity research through the creation of the co-authorship networks, the co-occurrence maps of keywords, citation networks of infer the most impactful authors, institutions, as well as, research topics. CiteSpace was applied to study citation bursts, time evolution of the research topics and intellectual structure mapping which illuminated on the expanding topics as well as the research focus evolving over the period. Descriptive bibliometric analysis will be done with the help of the Biblioshiny and it encompasses publication trends, publication productivity, author contribution, and three-field plots across countries, institutions and keywords. The level of data overview offered by such outputs is rather high, and the results obtained can be compared and cross-validated with other tools. In other words, the result of these tools can be regarded as a powerful and understandable image of the cybersecurity research area, which will ensure transparency, reproducibility, and consistency of analysis of the presented findings.

The figure 2 shows a Sankey diagram that connects authors (AU) to their affiliations (AU_UN) and research areas (DE). Each flow shows how different researchers connect to universities and then to subjects like network security, machine learning, intrusion detection, blockchain, and cybersecurity. The picture shows how people work together, how institutions contribute, and what themes are most common. It shows which fields are most important, how different institutions are connected, and how expertise is spread across different universities and areas of technology research. It gives a summary of the connections in research networks.

TABLE III: MOST RELEVANT AFFILIATIONS

AFFILIATION	ARTICLES
University Of Western Macedonia	19
Mohammed Vi Polytechnic University	18
Deakin University	17
K L Deemed To Be University	16
Srm Institute Of Science And Technology	14
Wuhan University	14
Department Of Computer Science	13
Aristotle University Of Thessaloniki	11
Dr. D. Y. Patil Institute Of Technology	11
Kumoh National Institute Of Technology	11
Tongji University	11
Chitkara University	10
King Abdulaziz University	10
Kongu Engineering College	10
University Of Western Macedonia	19
Mohammed Vi Polytechnic University	18
Deakin University	17
K L Deemed To Be University	16
Srm Institute Of Science And Technology	14
Wuhan University	14

The table 3 below is a tabular listing of the affiliations of the different academic affiliations and the number of articles published respectively. The rows are separate universities or institutions and the amount of articles in the column against it. The University of Western Macedonia is in 1st position with 19 articles followed by Mohammed VI Polytechnic University (18) and Deakin University (17). The other institutions like SRM Institute of Science and Technology, Wuhan University, have published 14 articles each.

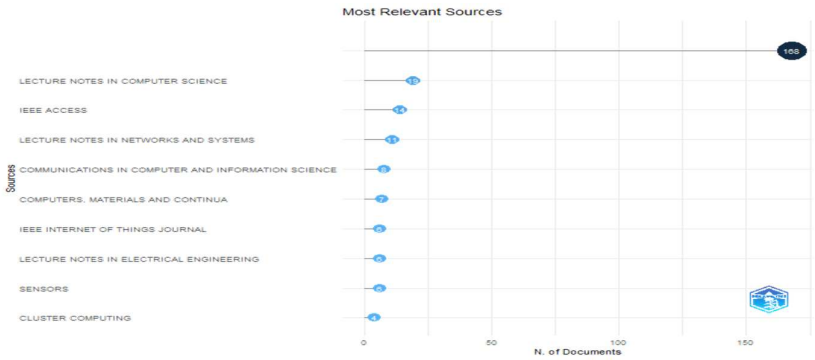

Figure 3. Most Relevant Sources

Figure 3 above entitled, the Most Relevant Sources demonstrates the significant sources of publication and the number of documents they contain. The sources are represented on the horizontal axis by the number of documents, the volume of the publications is determined by size of the bubble. The Lecture Notes in Computer Science is available in widespread form and has 168 documents, which is by far more than any other source.The most remarkable ones are IEEE Access (14), Lecture Notes in Electrical Engineering (19), and Communication in Computer and Information Science (8).

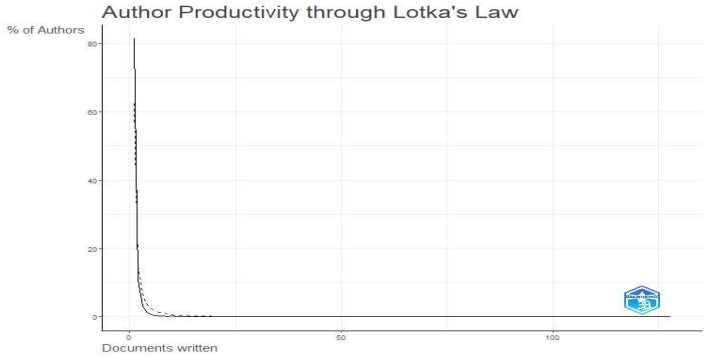

Figure 4. Lotka's Law

The above figure 4 above is Author Productivity through Lotka Law of the author of contributions in the terms of the documents written. The above x-axis represents the amount of produced documents and the y-axis represents the percentage of the authors. As can be seen, the curve is steep towards the higher numbers of those who write one or two papers, whereas there are also many publications whose publication was done by a very small percentage of the authors.

Figure 5. Word Cloud

The figure above5 shows a word cloud image of the most prominent themes and concepts of research in the domain of cybersecurity. The keywords that are the most eminent are cyber security, intrusion detection and network security, meaning that they are the main focus of the current research. New trends such as Internet of Things (IoT), cyber attacks, adversarial machine learning, and blockchain indicate the changing threats and defensive responses to cybersecurity studies.

The scientometric review used in this paper can give valuable information about the transformation of the field of cybersecurity research with new directions to AI-based security, IoT, and Cyber-Physical Systems. The threats and mitigation trend analysis can be further extended to include temporal evolution graphs and thematic cluster visualization in order to further support the discussion. These would enable better depiction of how areas of research focus and mitigation strategies have changed over time, resulting into increased interpretability and depth of analysis of the findings without changing the fundamental structure of the paper. The study of cybersecurity threats and mitigation strategies is also complemented with the study of trends of temporal evolution and thematic clusters. Temporal analysis shows how the focus of research has increasingly moved over time in terms of both traditional network security and cryptographic mechanisms to more advanced fields such as AI-assisted threat detection, IoT security, and adaptive defence mechanisms. The concept of thematic clustering shows how research interests are intertwined together creating an interrelation of intrusion detection, privacy preservation techniques and intelligent mitigation techniques. These trends suggest the increased focus on data-driven and active security solutions, which refer to the changes in complexity of cyber threats. The application of temporal evolution graphs and thematic cluster visualizations enhance the interpretation of how priorities and mitigation strategies of cybersecurity research have evolved over the years.

The development of cybersecurity threats and mitigation measures related to them is further discussed in a temporal and thematic context based on the bibliometric analysis. Temporal trend analysis shows that there was a distinct change in the direction of the research. In the literature on this topic, earlier authors mainly focused on conventional threats, including network intrusions, malware, and cryptographic threats, whereas recent works focus on sophisticated and adaptive threats, including AI-based attacks, ransomware, zero-day exploits, and attacks of large scale against IoT and Cyber-Physical Systems. The thematic cluster analysis provides the understanding of the co-evolution of threats and mitigation measures in the interdependent research domains. Communities of practice indicate the presence of robust relationships among intrusion detection systems, threat detection models based on machine learning, privacy-respectful security measures, and automated response systems. The evolution of time and the thematic clustering of the studies show that the research on cybersecurity has gradually shifted toward predictive, data-driven, and adaptive mitigation strategies rather than reactive defense strategies. This combined perspective makes it easier to understand the development of threat landscapes and mitigation strategies in tandem with each other and this information can be useful in helping to design future research and build stronger cybersecurity models. The references employed in the manuscript are extensive and inclusive to the literature on cybersecurity, privacy, and mitigation of attacks that are of relevance. Formatting of references has also been thoroughly checked and formatted in the final draft to provide uniformity both in the reference list and in-text citation. Some minor improvements were necessary, and they do not presuppose any significant reorganisation of the text.

IV. CONCLUSION

The research conclusion Global Research Trends in Cybersecurity: A Scientometric Analysis of Privacy, Threats Attack Mitigation highlights the rapid growth and the dynamism of the study of the cybersecurity issue in the period between 2013 and 2023. The most important outcomes are that the most developed countries like USA, China and the members of the EU are involved in a huge international alliance where innovation and knowledge sharing are flourishing. The privacy problem is a burning one, and the attention to privacy-vulcanized cryptographic methods, decentralized identity verification, and regulatory compliance only gains an increasing interest. Mitigation responds to an attack in real-time. Resource-limited system applications such as IoT and Cyber-Physical Systems (CPS) that have unique security concerns are detected with machine learning, and thus, Intrusion detection breakthroughs provide an improvement in the detection performance. The research is complemented by well-organised figures and analysis. Minor improvements in figure referencing and discussion on regional and AI-based elements would further support the research. The sudden onset of AI-powered cyberattacks and deepfake-enabled impersonation presents a dramatic challenge to digital confidence and data integrity. This new threat compromises authentication mechanisms, increases privacy threats, and calls for more responsive, intelligence-enabled security architectures.

REFERENCES

[1] Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems, 77(103201), 103201. https://doi.org/10.1016/j.micpro.2020.103201

[2] Awadallah, A., Eledlebi, K., Zemerly, M. J., Puthal, D., Damiani, E., Taha, K., Kim, T.-Y., Yoo, P. D., Raymond Choo, K.-K., Yim, M.-S., & Yeun, C. Y. (2025). Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities. IEEE Communications Surveys & Tutorials, 27(2), 1008–1052. https://doi.org/10.1109/comst.2024.3442475

[3] Nemec Zlatolas, L., Welzer, T., & Lhotska, L. (2024). Data breaches in healthcare: security mechanisms for attack mitigation. Cluster Computing, 27(7), 8639–8654. https://doi.org/10.1007/s10586-024-04507-2

[4] Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports, 7, 7999–8012. https://doi.org/10.1016/j.egyr.2021.08.124

[5] Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in FinTech. Iraqi Journal for Computer Science and Mathematics, 5(3), 45–91. https://doi.org/10.52866/ijcsm.2024.05.03.004

[6] Bhardwaj, A., Bharany, S., Rehman, A. U., Tejani, G. G., & Hussen, S. (2025). Securing cyber-physical robotic systems for enhanced data security and real-time threat mitigation. EURASIP Journal on Information Security, 2025(1). https://doi.org/10.1186/s13635-025-00186-7

[7] Clemmensen, T., Moghaddam, M. T., & Nørbjerg, J. (2025). Cyber-physical systems with Human-in-the-Loop: A systematic review of socio-technical perspectives. The Journal of Systems and Software, 226(112348), 112348. https://doi.org/10.1016/j.jss.2025.112348

[8] Gao, J., Zhao, D., Yang, X., Huang, J., Zhou, X., & Peng, K. (2025). Distributed subspace identification for data-driven fault detection and fault-tolerant control of complex interconnected, industrial systems. Journal of the Franklin Institute, 362(15), 107985. https://doi.org/10.1016/j.jfranklin.2025.107985
[9] Isichei, J. C., Khorsandroo, S., & Desai, S. (2023). Cybersecurity and privacy in smart bioprinting. Bioprinting, 36(e00321), e00321. https://doi.org/10.1016/j.bprint.2023.e00321
[10] Chahal, A., Gulia, P., Gill, N. S., & Rani, D. (2025). Design of a federated ensemble model for intrusion detection in distributed IIoT networks for enhancing cybersecurity. Journal of Industrial Information Integration, 44(100800), 100800. https://doi.org/10.1016/j.jii.2025.100800
[11] Alqurashi, F., & Ahmad, I. (2024). Scientometric analysis and knowledge mapping of cybersecurity. International Journal of Advanced Computer Science and Applications : IJACSA, 15(3). https://doi.org/10.14569/ijacsa.2024.01503117
[12] Dept of Computer Science Engg. Shobhit Institute of Engg. Technology Meerut, India, Amrita, A., Dept of Computer Science Engg. Shobhit Institute of Engg. Technology Meerut, India, Dept of Computer Science Engg. Symbiosis Institute of Technology, Symbiosis International (Deemed University), Pune, India; IEEE, SIT,Pune,India, Arun, & Sharma, A. (2024). A hybrid intrusion detection approach for cyber attacks. Journal of Cybersecurity and Information Management, 8(2), 08–18. https://doi.org/10.54216/jcim.130201
[13] Chatterjee, S., Chaudhary, S., & Cherukuri, A. K. (2025). Intrusion detection system using deep learning for network security. In arXiv [cs.CR]. https://doi.org/10.48550/ARXIV.2505.05810
[14] Sharma, A., Rani, S., & Driss, M. (2024). Hybrid evolutionary machine learning model for advanced intrusion detection architecture for cyber threat identification. PloS One, 19(9), e0308206. https://doi.org/10.1371/journal.pone.0308206
[15] Shettar, I., Hadagali, G. S., Kaddipujar, M., Bulla, S. D., Agadi, K., Ganjihal, G. A., Hiremath, R., Dundannanavar, A., & Babu, B. R. (2024). Scientometric analysis of global cyber security research output based on Web of Science. Iberoamerican Journal of Science Measurement and Communication, 4(2), 1–15. https://doi.org/10.47909/ijsmc.129
[16] Harkat, H., Camarinha-Matos, L. M., Goes, J., & Ahmed, H. F. T. (2024). Cyber-physical systems security: A systematic review. Computers & Industrial Engineering, 188(109891), 109891. https://doi.org/10.1016/j.cie.2024.109891