West Science Interdisciplinary Studies
Vol. 4, No. 07, July 2026: pp. 1157-1167

Zero Trust Security in Computer Networks: A Bibliometric Mapping of Research Evolution

Loso Judijanto[1], Arnes Yuli Vandika[2], Nanny Mayasari[3], I Wayan Karang Utama[4]
[1] IPOSS Jakarta, Indonesia and losojudijantobumn@gmail.com
[2] Universitas Bandar Lampung and arnes@ieee.org
[3] Universitas Nusa Cendana and nanny.mayasari@gmail.com
[4] ITB Stikom Bali and karang_utama@stikom-bali.ac.id

ABSTRACT

The rapid transformation of digital infrastructures, cloud computing adoption, Internet of Things (IoT) expansion, and increasing cyber threats have accelerated the need for advanced cybersecurity approaches beyond traditional perimeter-based defense mechanisms. Zero Trust Security has emerged as a strategic security paradigm that emphasizes continuous verification, identity-based access control, and adaptive protection across modern computer networks. This study aims to analyze the evolution, intellectual structure, and emerging research trends of Zero Trust Security through a bibliometric mapping approach. Data were collected from a scientific database and analyzed using bibliometric techniques, including performance analysis, keyword co-occurrence analysis, citation analysis, co-authorship analysis, institutional collaboration analysis, and country collaboration mapping using VOSviewer. The findings reveal that Zero Trust Security research has experienced significant development, with network security, cybersecurity, and Zero Trust Architecture emerging as central research themes. Influential studies highlight the importance of authentication mechanisms, intrusion detection systems, blockchain integration, and secure architectures for cloud, 5G, and IoT environments. The thematic evolution indicates a shift from foundational security mechanisms toward intelligent and adaptive solutions involving machine learning, deep learning, federated learning, and privacy-preserving technologies. Collaboration analysis shows that research contributions are dominated by countries such as the United States, India, and China, while global cooperation continues to expand. This study contributes to the cybersecurity literature by providing a comprehensive overview of Zero Trust Security development and identifying future research directions toward intelligent, scalable, and resilient security frameworks for next-generation computer networks.

Keywords: *Zero Trust Security, Zero Trust Architecture, Network Security, Cybersecurity, Bibliometric Analysis*

1. INTRODUCTION

The exponential growth of digital technologies and the widespread adoption of cloud computing, remote work, and Internet of Things (IoT) devices have fundamentally transformed modern network architectures [1]. Traditional perimeter-based security models, which rely on the assumption that internal networks are inherently trustworthy, are increasingly inadequate in addressing sophisticated cyber threats. Security breaches, data exfiltration, and insider threats have highlighted the vulnerability of conventional network defense mechanisms and underscored the need for a paradigm shift in cybersecurity strategies [2], [3]. In this context, Zero Trust Security (ZTS) has emerged as a critical framework to mitigate risks associated with the evolving threat landscape.

The Zero Trust Security framework operates on the concept of "never trust, always verify" with an intense focus on stringent identity validation, least privilege, and constant monitoring irrespective of whether the user is inside or outside the network perimeter [4]. In contrast to traditional systems, ZTS presumes the presence of threats both inside and outside the network, and therefore does not assume any implicit trustworthiness of any entity trying to access the resources. Utilizing various technologies, including multi-factor authentication (MFA), micro-segmentation,

endpoint protection, and behavior analysis, the ZTS framework provides for granular access control and mitigation of attack surfaces [5], [6].

In the last ten years, the amount of scientific papers and business articles about Zero Trust Security has significantly increased since there is a strong interest in the concept behind the strategy, implementation, and results that can be obtained by using it. Different sides of ZTS have been investigated by researchers, from identity management, to policy enforcement, cloud computing security, and implementation within the enterprise security framework [7]–[9]. The implementation of Zero Trust Security has been especially important for organizations dealing with sensitive data because a breach of their security leads to serious financial and reputational damages. In turn, bibliometrics have become an effective approach to analyzing the development of research trends in this field.

In addition, technology developments like artificial intelligence (AI) and machine learning (ML) have contributed to the transformation of Zero Trust architectures. By using AI-powered analytics of behavior, organizations can evaluate risk levels and access requirements in real-time considering context-aware data including device posture, behavior of users, and geographic location [10]. With the development of the use of artificial intelligence and Zero Trust models, there has been the emergence of predictive security approaches, proactive threat management, and automation of policies. Such developments demonstrate the relationship between technological development and strategic security planning.

Even though there is an extensive amount of research on Zero Trust, the theoretical background and its practical application continue to be heterogeneous due to differing implementations and definitions of ZT in different articles [11], [12]. There are certain difficulties in the use of Zero Trust by organizations, such as complicated technologies, problems of interoperability, and organizational resistance to change. The methodology of bibliometric mapping is used in order to summarize scientific papers and analyze their key features as well as trends in authors' productivity, institutional impact, and collaboration.

Although Zero Trust Security has garnered substantial attention in academic and industrial research, there remains a lack of comprehensive bibliometric analysis that systematically traces its evolution, identifies key contributors, and highlights emerging trends. Existing studies are predominantly descriptive or case-based, often focusing on technical implementation or sector-specific applications without situating findings within a broader research network. This gap limits the ability of scholars and practitioners to understand the cumulative knowledge structure, thematic shifts, and influential studies that have shaped the ZTS domain. Consequently, a detailed bibliometric mapping is necessary to illuminate research trajectories, collaboration patterns, and areas requiring further investigation. This study aims to conduct a bibliometric mapping of Zero Trust Security research to examine its evolution over time, identify leading authors, institutions, and journals, and uncover emerging themes and trends in the literature.

2. METHODS

This research uses bibliometric methods for analyzing the evolution of the field of study called Zero Trust Security (ZTS). This technique helps to investigate the structure of scientific literature, including its citations, authorship, and collaboration network as well as to understand the evolution of research fields [13]. The aim of using such a method is to map the knowledge domain of Zero Trust Security, to determine key publications and to reveal emerging trends and thematic clusters in the area of research.

Data acquisition in the study was conducted using the Scopus database that is characterized by the wide range of coverage of peer-reviewed scientific literature and detailed citation data. A systematic approach to search was used, where the keywords of the Zero Trust Security concept such as "Zero Trust," "Zero Trust Architecture," "network security," and "cybersecurity framework" were applied. Search was restricted within the range from 2010 to 2026 as it covered the recent development of Zero Trust concepts. After that, duplicate entries and publications that were irrelevant to the research question were eliminated to prepare the dataset appropriate for quantitative and network analysis.

Analysis and visualization of the research landscape was done using VOSviewer [14]. It is a special software designed for making and analyzing bibliometric networks. VOSviewer helps to create such kinds of networks as co-authorship, co-citations and co-occurrences, thus helping identify influential researchers, organizations, publications and thematic clusters. In our research we made an analysis of co-authorship networks that help us to explore collaboration patterns in our field, as well as we used co-citations and co-occurrences analysis to identify the intellectual structure of the field and the current trends in ZTS.

3. RESULT AND DISCUSSION

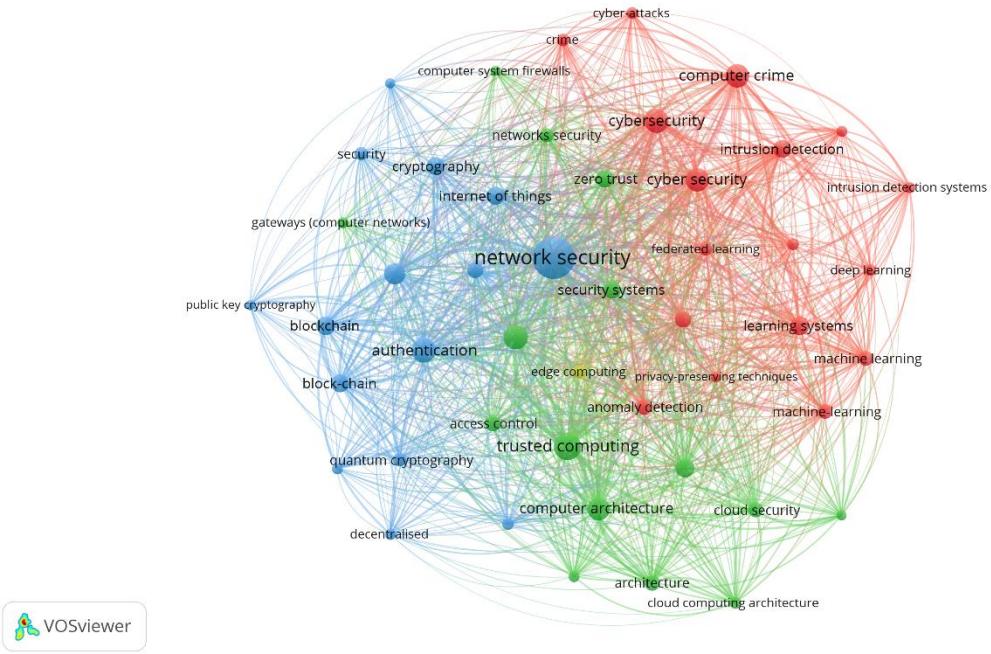

Figure 1. Network Visualization
Source: Data Analysis Result, 2026

Networks are used to show the intellectual structure and relations among frequently used keywords in the literature. The larger the node, the more frequent the keyword, and the line shows the relationship between keywords. There are three main clusters, namely, the red, green, and blue clusters, which correspond to different research directions of the Zero Trust Security field. Red cluster is one of the clusters indicating the cybersecurity intelligence and threat detection aspect of Zero Trust research. Red cluster has keywords like cybersecurity, computer crime, cyber attack, intrusion detection, deep learning, and machine learning among others. The close connection of Zero Trust with these keywords shows that Zero Trust approach is increasingly being linked to proactive methods of defense against cyber threats. Research in this cluster revolves around issues of monitoring, detecting anomalies, security mechanisms based on artificial intelligence, and adaptive protection against cyber threats.

The green cluster is an example of how Zero Trust has been applied to the field of cloud computing, trusted systems, and future networking technologies. Some of the key terms that have been identified in this cluster include cloud security, cloud computing architecture, trusted computing, edge computing, privacy preserving, and access control. This cluster represents how security models are shifting from perimeter based models to distributed security models. Cloud computing and edge computing have led to the increasing requirement for identity verification and least privilege access, which are the key elements of ZTA.

The cluster in blue color refers to the basic security technologies required for the successful deployment of Zero Trust. Words like network security, authentication, cryptography, blockchain, public-key cryptography, and Internet of Things reveal that research on Zero Trust is intimately related to the basic tools used for ensuring security of communication and managing digital identities. It is therefore apparent from this cluster that for the successful adoption of Zero Trust, robust authentication processes, encryption techniques, decentralized security tools, and device protection are essential.

According to the visualization, Zero Trust Security research has transitioned from the conventional approach of network security towards a more comprehensive cybersecurity ecosystem which is associated with the use of artificial intelligence, cloud computing, IoT and authentication technologies. Network security, cybersecurity, and zero trust form the core of the visualization as they connect the different domains of research. The future trends will most likely revolve around intelligent Zero Trust systems that integrate AI-powered threat detection and adaptive access control systems.

3.1 Overlay Visualization

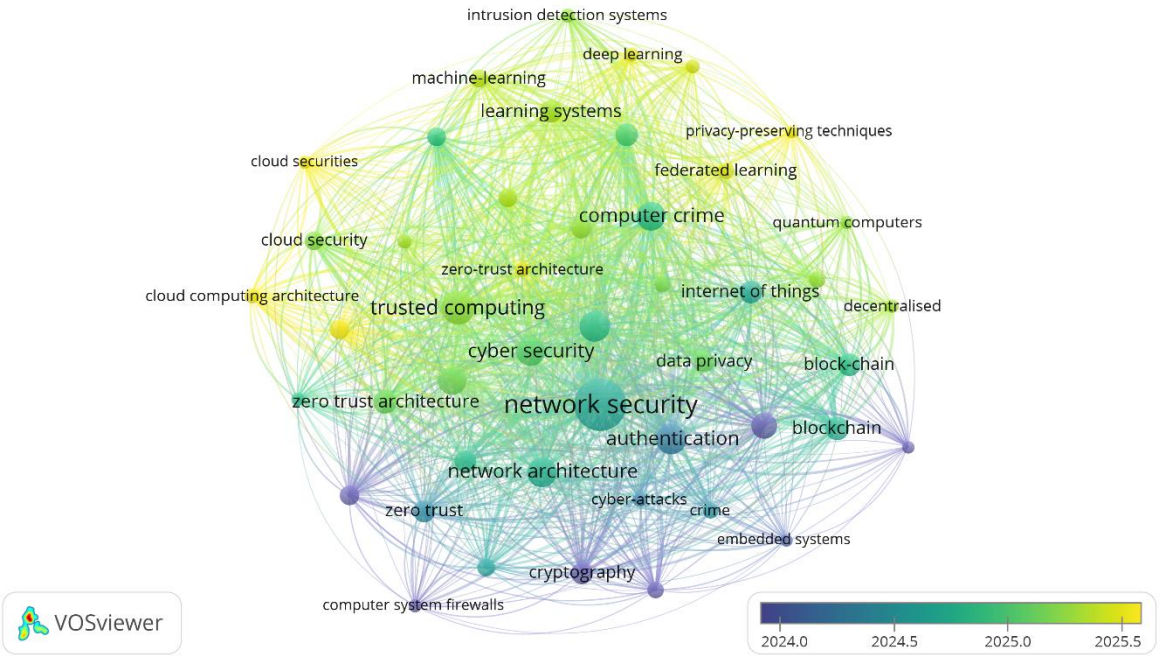

Figure 2. Overlay Visualization

Source: Data Analysis Result, 2026

Figure 2 presents the development of research areas concerning Zero Trust Security in computer networks, where each color represents the average year when keyword articles were published. It is clear that network security, cyber security, and zero trust architecture are used as core terms linking several research areas together. As a result of high density and connections, it can be concluded that Zero Trust Security research has become a multidisciplinary area combining

traditional cybersecurity fundamentals with new technologies like cloud computing, artificial intelligence, blockchain, and privacy techniques.

The previous research topics, indicated through darker shades of blue and purple colors, are related to security technology basics such as cryptography, authentication, computer firewall, network architecture, and zero trust basics. It can be concluded that these topics belong to the first period of development of Zero Trust Security because researchers were concerned about developing secure communication channels, identity verification and access control, as well as the principles of designing an architecture that would replace the perimeter security model. At this stage, the key words of blockchain, embedded systems, and cyber-attacks appeared.

The new research trends, symbolized by shades of green to yellow, point to the trend towards intelligent and adaptive Zero Trust security. The use of emerging words such as machine learning, deep learning, federated learning, privacy-preserving, cloud security, cloud computing architecture, and intrusion detection system points to the current trend towards artificial intelligence-based cybersecurity and secure distributed systems. Based on this development, it can be expected that future Zero Trust Security research will be centered around the use of artificial intelligence, cloud-based security models, and privacy-preserving technologies to provide an adaptive defense strategy against threats.

3.2 Citation Analysis

Table 1. The Most Impactful Literatures

Citations	Authors and year	Title
195	[15]	A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture
124	[16]	A federated learning-based zero trust intrusion detection system for Internet of Things
124	[17]	Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology
102	[18]	A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions
81	[19]	Access Control Policy Enforcement for Zero-Trust-Networking
79	[20]	Pseudo trust: Zero-knowledge authentication in anonymous P2Ps
73	[21]	Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation
61	[22]	The design of a reliable reputation system
58	[23]	Blockchain-Enabled Intrusion Detection and Prevention System of APTs Within Zero Trust Architecture
57	[9]	A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model

Source: Scopus, 2026

Table 1 illustrates some of the most cited literature within Zero Trust Security that has been the driving force behind the emergence of Zero Trust Security research as an academic field. For example, [15] paper, which was cited 195 times, proposed a security awareness and protection mechanism for the 5G smart healthcare using Zero Trust Architecture. Thus, one can see the significance of Zero Trust architecture and its potential to secure the vital digital infrastructure. On the other hand, [16] and [17], cited 124 times each, pay special attention to the modern approaches of federated learning intrusion detection in IoT environment and secure sharing of medical images in blockchain technology, respectively. Thus, one can conclude that the current Zero Trust research has gone far from conventional approaches to securing network infrastructure and moved towards more advanced security techniques, decentralization, and privacy protection. Finally, [19] research on access control policy enforcement and [20] paper on zero-knowledge authentication constitute

important contributions that set the stage for identity management and trust verification in Zero Trust framework. Furthermore, studies focusing on cloud intrusion detection, blockchain-based threat prevention, network slicing security, and comparative analyses of Zero Trust frameworks demonstrate the continuous evolution of the field toward adaptive, distributed, and AI-supported cybersecurity solutions.

3.3 Density Visualization

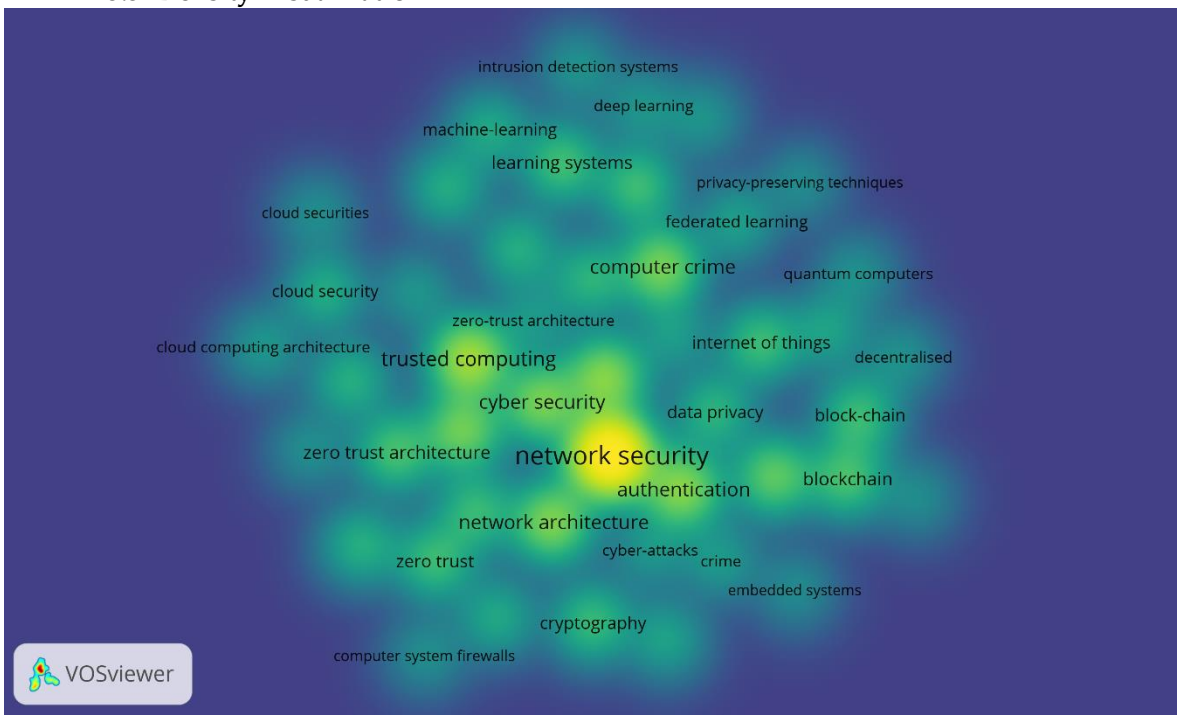

Figure 3. Density Visualization
Source: Data Analysis Result, 2026

The research emphasis and theme intensity for the domain of Zero Trust Security in computer networks is presented in Figure 3. Yellow zones denote the most research-intensive keywords with a high frequency of occurrence, while green and blue zones denote less concentrated themes. Network security turns out to be the hotspot with the highest concentration, which means it serves as the key research foundation for different studies in Zero Trust domain. Other concentrated themes are cyber security, trusted computing, authentication, and zero trust architecture. This suggests that current research mainly focuses on the development of secure identities and secure networks as alternatives to conventional security frameworks. This visualization also demonstrates several emerging areas of research linked to the major security themes such as machine learning, deep learning, federated learning, intrusion detection systems, cloud security, Internet of Things, and blockchain. All these themes occur in the less active but developing research areas, which shows that there is a shift towards developing smart, distributed, and adaptive approaches to Zero Trust. As for the occurrence of security techniques based on AI and privacy protection technologies, it suggests that future Zero Trust research will be focused on automating threat identification and dynamic access control.

3.4 Co-Authorship Analysis

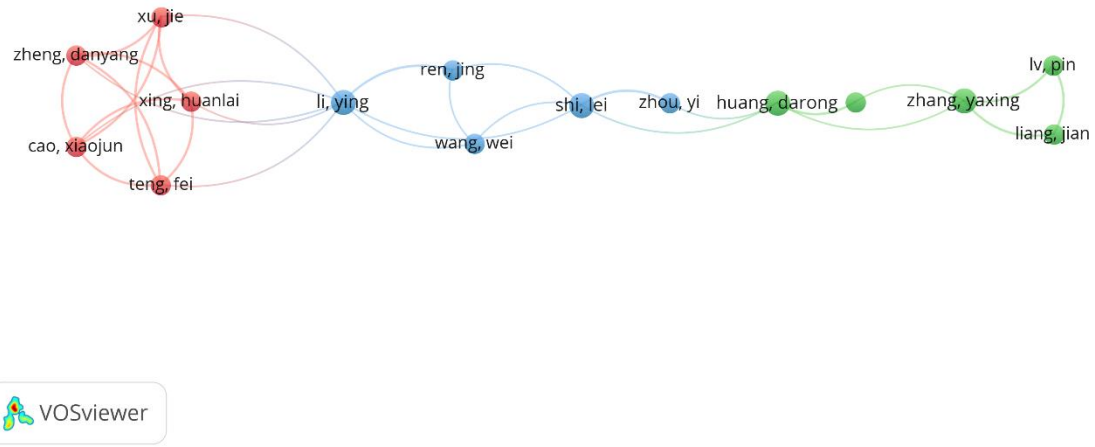

Figure 4. Author Visualization
Source: Data Analysis Result, 2026

Figure 4 presents the collaborative network of the leading scholars in the research area of Zero Trust Security and computer network security. In the network, there are some distinct author groups that can be seen in different colors. This means the author groups that are collaborating within their respective research areas. For example, in the red cluster on the left hand side, there are some authors like Xu Jie, Zheng Danyang, Xing Huanlai, Teng Fei, and Cao Xiaojun. It shows some internal collaboration patterns and indicates a compact research group that is working on the foundation and/or application part of Zero Trust related security. In addition, the blue cluster includes some authors such as Li Ying, Ren Jing, Wang Wei, and Shi Lei. This author group works as a bridge for the researchers in different research fields through collaborative links. It can be noted from the figure above that research on Zero Trust Security has fragmented but interrelated collaborations among authors. The lack of connectivity among clusters signifies that research is conducted in special groups rather than within an integrated collaboration network at the global level. But several authors like Li Ying and Shi Lei can be considered connecting researchers between clusters.

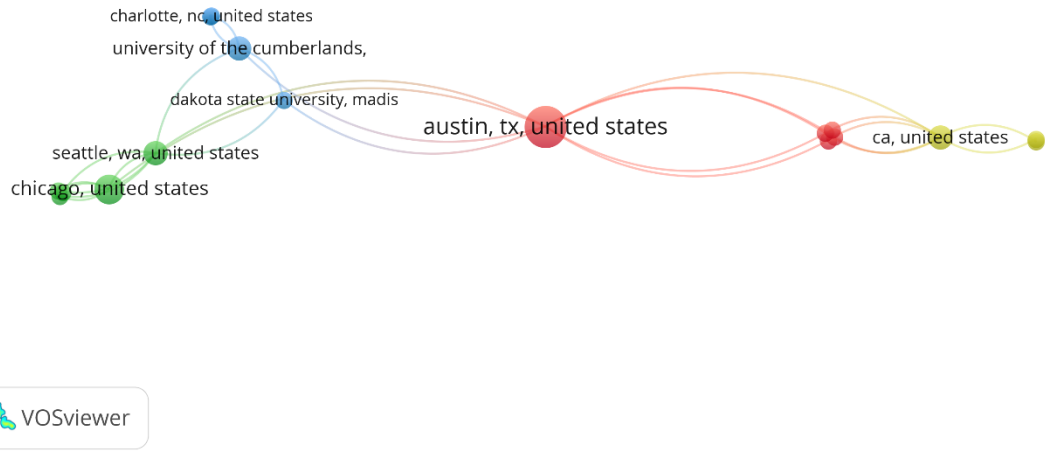

Figure 5. Institution Visualization
Source: Data Analysis Result, 2026

The relationships between various institutions participating in Zero Trust Security Research have been illustrated in Figure 5. It can be seen that collaboration in research is mainly limited to institutions and research groups based in the US, where Austin, TX, United States stands out as the main central node with the highest connectivity to other institutions. This clearly suggests that research institutions in Austin play a vital role as a collaborative node in the field. Other institutions and their locations, such as University of the Cumberlands, Dakota State University, Seattle, Chicago, and institutions based in California, constitute clusters that contribute to cybersecurity research.

This visual also shows that collaboration within organizations is still fairly limited and geographically bound. Some small clusters are linked together via large hubs, which implies that the exchange of information takes place mainly through particular academic and research networks instead of any universal collaboration system across the globe. The dominance of institutions in the USA clearly proves the importance of American research circles for the development of the Zero Trust Security framework, especially when it comes to network security, cybersecurity models, and new security architecture designs.

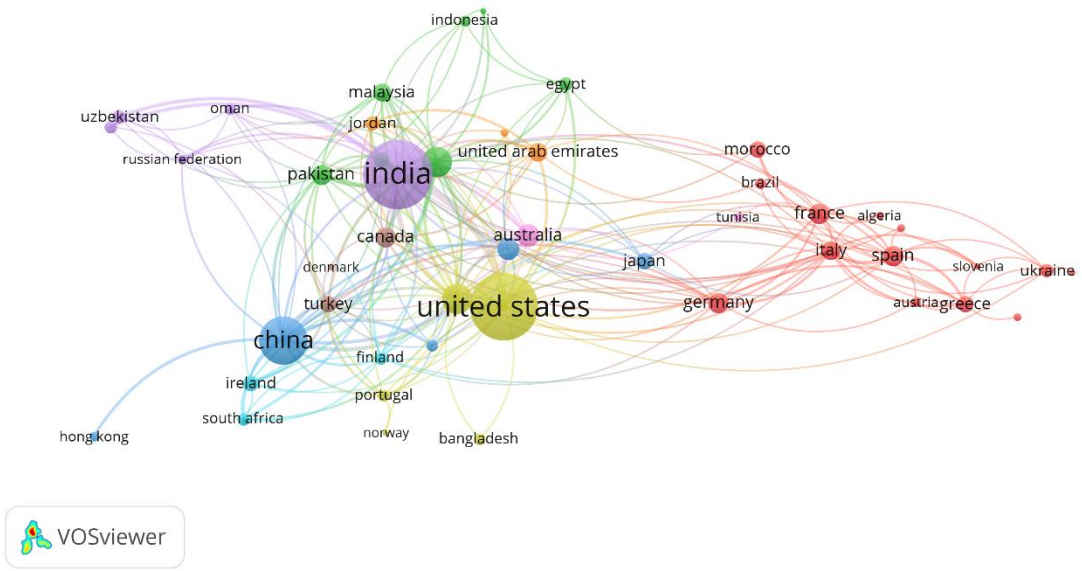

Figure 6. Country Visualization
Source: Data Analysis Result, 2026

Figure 6 shows the international collaborative research in the subject of Zero Trust Security of computer networks. From the graph, it is seen that the research activity is spread in several regions and that the most active participants in this area are the United States, India, and China due to their node sizes and strengths. It can be observed that the United States is the collaboration center with strong connections to many countries like India, China, Germany, France, Australia, Japan, and Canada. The visualization also identifies a number of regional cooperation clusters. The red cluster includes the research cooperation networks of Europe which consist of nations like France, Italy, Spain, Germany, Austria, Greece, Ukraine, and Slovenia. The green and blue clusters include Asian and mixed regional cooperation networks wherein India and China serve as important research centers associated with nations like Indonesia, Malaysia, Pakistan, Japan, and South Africa. This clearly shows that the concept of Zero Trust Security has become a global area of research interest owing to cybersecurity threats and the need for network security.

CONCLUSION

Bibliometric analysis offers a holistic view of the evolution, intellectual structure, and trends in Zero Trust Security in Computer Networks. Findings show that Zero Trust has evolved from an access control approach to a full cybersecurity paradigm that combines network security, authentication, trusted computing, cloud security, artificial intelligence, blockchain, and IoT security. Keyword analysis shows that network security, cybersecurity, and Zero Trust Architecture are key themes of the research. In addition, recent researches pay much attention to intelligent security approaches, which include machine learning, deep learning, federated learning, and privacy preservation techniques. Citation analysis shows that key researches cover topics such as secure authentication, intrusion detection, blockchain security, and implementation of Zero Trust Architecture in novel fields like 5G healthcare, cloud computing, and IoT networks. Collaboration analyses show that research development in Zero Trust Architecture has been greatly driven by the most prominent countries like the USA, India, and China, but global institutional collaboration is quite narrow. In this context, it is evident that the Zero Trust Security is a growing field of study which is multi-disciplinary in nature due to the requirement of adaptive, identity-based, and

continuously monitored security systems. The future scope of study should include designing AI-enabled Zero Trust security architecture, designing scalable security systems, and collaboration on a global level.

REFERENCES

[1] V. Negi and P. Negi, "AI-Enabled Trustworthiness in Edge Zero Trust Architectures," in *Proceedings of the IEEE International Conference on AI Engineering and Innovations, AIEI 2026*, Microsoft Corporation, CA, United States: Institute of Electrical and Electronics Engineers Inc., 2026. doi: 10.1109/AIEI69164.2026.11497002.

[2] S. Durgaprasad and A. M. Abdul, "Deep Learning-Driven Quantum-Resilient Zerotrust Architecture for Secure Multi-Cloud Container Migration," in *2026 2nd International Conference on Intelligent Systems and Computational Networks, ICISCN 2026*, Gitam Deemed To Be University, Department Of Computer Science And Engineering, Hyderabad, India: Institute of Electrical and Electronics Engineers Inc., 2026. doi: 10.1109/ICISCN67954.2026.11566608.

[3] S. Barmpounakis *et al.*, "Early Validation of 6G Concepts," *6G to Build a Sustainable Future*. wiley, WINGS ICT Solutions, Athens, Greece, pp. 293–333, 2026. doi: 10.1002/9781394363605.ch8.

[4] D. A. Kumar, S. Teja Vustela, A. S. Budalapati, and Y. Gude, "ForensiTrust: A Real-Time Risk-based User Behavior Analytics Framework for Cybercrime Detection and Forensic Readiness," in *Proceedings of 9th International Conference on Inventive Computation Technologies, ICICT 2026*, Lakireddy Bali Reddy College Of Engineering, Department Of Computer Science And Engineering, Mylavaram, India: Institute of Electrical and Electronics Engineers Inc., 2026, pp. 852–858. doi: 10.1109/ICICT68280.2026.11510946.

[5] A. Santorsola, A. Migliau, and S. Caporusso, "Reinforcement Learning Agents for Simulating Normal and Malicious Actions in Cyber Range Scenarios," in *CEUR Workshop Proceedings*, D. C. and M. A., Eds., BV-Tech s.p.a., Milan, 20123, Italy: CEUR-WS, 2022, pp. 1–16. [Online]. Available: https://www.scopus.com/pages/publications/85142091667?origin=resultslist

[6] K. U. Nisa, F. Algarni, M. T. Quasim, N. Alqarameen, R. Jahan, and S. I. Ansarullah, "Comparative Analysis of Approaches in the Zero Trust Network Model," in *Lecture Notes in Networks and Systems*, V. B., D. C. S., S. A., T. N., and S. S., Eds., Department of Artificial Intelligence, College of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia: Springer Science and Business Media Deutschland GmbH, 2026, pp. 23–31. doi: 10.1007/978-3-032-24926-5_3.

[7] R. Campbell, "Detection and Mitigation of Mythos-Class Frontier Model Capabilities: A Layered Reference Architecture," *Computers*, vol. 15, no. 6, 2026, doi: 10.3390/computers15060331.

[8] G. Lokesh, M. S. N. Ahamed, T. Charan, S. R. A. S. Khadri, S. Rahul, and M. G. Reddy, "Multimodal Phishing Website Detection using Hybrid Deep Learning and Ensemble Techniques," in *Proceedings of 6th International Conference on Expert Clouds and Applications, ICOECA 2026*, G. Pullaiah College of Engineering and Technology, Department of Computer Science and Engineering, AP, Kurnool, India: Institute of Electrical and Electronics Engineers Inc., 2026, pp. 1536–1541. doi: 10.1109/ICOECA68095.2026.11485075.

[9] P. Dhiman *et al.*, "A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model," *Sensors*, vol. 24, no. 4, 2024, doi: 10.3390/s24041328.

[10] A. Goel and B. Thangaraju, "Authenticating Distributed Systems Using SPIRE over Kubernetes Cluster," in *2022 IEEE International Conference on Electronics, Computing and Communication Technologies, CONECCT 2022*, Bangalore (IIITB), International Institute of Information Technology, India: Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/CONECCT55679.2022.9865835.

[11] A. Alsaleh, N. Alotaibi, S. Alaskar, K. Saleem, M. Benmalek, and K.-D. Haouam, "A Security Architecture for Hybrid Paas Mitigating Identity, Network, and Application Risks," in *2026 Middle East and North Africa Communications Conference, MENACOMM 2026*, College of Engineering, Al Yamamah University, Computer Engineering Department, Riyadh, 11512, Saudi Arabia: Institute of Electrical and Electronics Engineers Inc., 2026. doi: 10.1109/MENACOMM69507.2026.11532616.

[12] L. Xie, X. Zhao, and Y. Xiao, "Research on zero trust security architecture and continuous authentication mechanism for cloud platform networks," in *Proceedings of SPIE - The International Society for Optical Engineering*, Y. Y., Ed., China Three Gorges Corporation, Hubei, Wuhan, 430000, China: SPIE, 2026. doi: 10.1117/12.3109506.

[13] P. Devaraj, S. A. Chaman Basha, N. N. Panarkuzhiyil Santhosh, and N. Panda, "A Post-Quantum Secure Architecture for 6G-Enabled Smart Hospitals: A Multi-Layered Cryptographic Framework," *Futur. Internet*, vol. 18, no. 3, 2026, doi: 10.3390/fi18030165.

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

[15] B. Chen *et al.*, "A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10248–10263, 2021, doi: 10.1109/JIOT.2020.3041042.

[16] D. Javeed, M. S. Saeed, M. Adil, P. Kumar, and A. Jolfaei, "A federated learning-based zero trust intrusion detection system for Internet of Things," *Ad Hoc Networks*, vol. 162, 2024, doi: 10.1016/j.adhoc.2024.103540.

[17] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 1, 2020, doi: 10.1186/s12911-020-01275-y.

[18] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu, and M. Liyanage, "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions," *IEEE Commun. Surv. Tutorials*, vol. 26, no. 1, pp. 534–570, 2024, doi: 10.1109/COMST.2023.3312349.

[19] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access Control Policy Enforcement for Zero-Trust-Networking," in *29th Irish Signals and Systems Conference, ISSC 2018*, Software Research Institute, Athlone Institute of Technology, Athlone, Ireland: Institute of Electrical and Electronics Engineers Inc., 2018. doi: 10.1109/ISSC.2018.8585365.

[20] L. Lu *et al.*, "Pseudo trust: Zero-knowledge authentication in anonymous P2Ps," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 10, pp. 1325–1337, 2008, doi: 10.1109/TPDS.2008.15.

[21] V. Balamurugan and R. Saravanan, "Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation," *Cluster Comput.*, vol. 22, pp. 13027–13039, 2019, doi: 10.1007/s10586-017-1187-7.

[22] G. Swamynathan, K. C. Almeroth, and B. Y. Zhao, "The design of a reliable reputation system," *Electron. Commer. Res.*, vol. 10, no. 3, pp. 239–270, 2010, doi: 10.1007/s10660-010-9064-y.

[23] L. Alevizos, M. H. Eiza, V. T. Ta, Q. Shi, and J. Read, "Blockchain-Enabled Intrusion Detection and Prevention System of APTs Within Zero Trust Architecture," *IEEE Access*, vol. 10, pp. 89270–89288, 2022, doi: 10.1109/ACCESS.2022.3200165.