**West Science Information System and Technology**
Vol. 4, No. 02, August 2026, pp. 220~232

# Zero Trust Architecture Research Trends: A Bibliometric Study

**Loso Judijanto[1], Rizki Dewantara[2]**
[1] IPOSS Jakarta, Indonesia
[2] Universitas Islam Negeri Siber Syekh Nurjati Cirebon

**Article Info**

***Article history:***

Received Aug, 2026
Revised Aug, 2026
Accepted Aug, 2026

***Keywords:***

Zero Trust Architecture
Zero Trust Security
Cybersecurity
Bibliometric Analysis
Network Security

**ABSTRACT**

Rapid evolution of cyber threats, cloud computing and digital transformation have led to increased need for adaptive and resilient cybersecurity framework. Zero Trust Architecture (ZTA) has been developed as an advanced security model that is designed to overcome limitations of the existing approaches based on perimeter-based security through its features of continuous verification, least-privilege access, and identity-centric protection. This paper is devoted to analyzing the global research development, intellectual structure and trends of Zero Trust Architecture through the use of bibliometric analysis methodology. The data for analysis were collected from Scopus database by means of keywords relating to "Zero Trust Architecture" and "Zero Trust Security" and then were analyzed using VOSviewer tool. The aspects that are covered by the analysis include the dynamics of publications, citation impact, influential authors, international and country collaboration, co-occurrence of keywords, themes and research patterns. It can be concluded from the findings that ZTA research has expanded greatly and is mostly concentrated on topics of network security, authentication, trusted computing, network architecture, and access control. Also, the recent trends in ZTA research indicate increased use of ZTA in combination with new technologies, including artificial intelligence, machine learning, blockchain, IoT, federated learning and cloud computing. Collaboration analysis reveals the international and interdisciplinary character of ZTA research, which involves contributions from different countries, scientific institutions and cybersecurity communities. The results of the research allow understanding the evolution of ZTA and identifying future opportunities in the area of intelligent, adaptive and decentralized cybersecurity architectures.



***Corresponding Author:***

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

## 1. INTRODUCTION

Changes within digital environments have greatly impacted the field of cybersecurity, making protection of information assets, applications, users, and networks ever more complex for businesses [1]. The emergence of cloud computing, Internet of Things (IoT), mobile computing, and distributed digital services has made the organization's exposure to attacks larger than what the organization's network alone can contain. Traditional cybersecurity strategies

that follow the paradigm of perimeters defense have proved to be inadequate when dealing with today's cyber threats [2], [3]. It is evident from data breaches, ransomware attacks, insider threats, and advanced persistent threats that one cannot assess the level of trust based only on whether something is internal or external to the network. This implies the need for a new approach, which should be focused on continuous validation, dynamic access control, and risk-based decisions [4], [5].

Zero Trust Architecture (ZTA) is one of the leading paradigms of cybersecurity developed to counter the aforementioned challenges. ZTA was first introduced under the idea of "zero trust" by [6], [7], which operates according to the principle of "never trust, always verify" and implies that every access attempt must be authenticated, authorized, and evaluated before the user gains access to organizational resources. ZTA contrasts with other security frameworks by not focusing on securing organizational networks but applying the principles of identity-centricity, least privilege, and micro-segmentation to reduce access attempts and potential harm caused by a security incident. The concept of Zero Trust Architecture has been further defined by the National Institute of Standards and Technology (NIST) as a cybersecurity framework, which operates with the assumption of no implicit trust depending on physical and network location and continuous evaluation of access attempts using multiple contextual information (e.g., user identity, device, and environment) [8], [9].

The rising popularity of digital transformation projects has sparked interest in Zero Trust Architecture from both theoretical and practical perspectives. Cloud migration, hybrid work environments, and the development of digital services have led organizations to realize the shortcomings of existing security approaches and the importance of having flexible security approaches in place. Specifically, the increased popularity of remote work due to the outbreak of the COVID-19 pandemic has raised issues of identity management, endpoint security, and the potential of breaches related to unauthorized access. Therefore, Zero Trust Architecture has been viewed as a possible strategy for protecting distributed organizational environments through the use of technologies like identity and access management (IAM), multi-factor authentication (MFA), software-defined networking (SDN), artificial intelligence-based threat detection, and security analytics [10], [11].

Even though Zero Trust Architecture has been recognized increasingly more often in practice, there is fragmentation within the academic literature that discusses this topic because of the interdisciplinarity of the field and fast-paced technological progress. Some existing studies have covered a number of issues related to Zero Trust Architecture such as authentication, cloud security, access control, network segmentation, and organizational readiness. However, scientific results are scattered over many journals, conferences, and scientific domains, which makes it challenging to pinpoint main themes, trends, key contributors, and possible knowledge gaps within the body of literature. Bibliometric analysis offers a suitable methodology for systematic exploration of scientific publications in large volumes through the examination of publication patterns, citation patterns, collaboration patterns, and themes [12].

The requirement for a systematic assessment of research trends in Zero Trust Architecture is becoming more critical with the continuous changing threat environment and an increasing shift towards implementing a zero trust security architecture by organizations. While there exist many conceptual and technical studies on how to implement the Zero Trust Architecture, no significant studies have yet analyzed the knowledge structure and evolution pattern in this area. The knowledge of publications, influential papers, research topics, methodology, and upcoming research themes could help the readers immensely. For that reason, it is necessary to look into the research domain through the bibliometric perspective

to assess the current level of maturity of research in Zero Trust Architecture.

Despite the significance of Zero Trust Architecture as a cyber security framework, the current state of knowledge in this field has not been integrated into one coherent body of literature due to the absence of a holistic intellectual history of this topic. In other words, previous research has mainly concentrated on the technical side of the concept, while no attention has been paid to the study of global publications trends, the most influential studies, collaboration, concept evolution, and research agendas in the area. Such a fragmented approach makes it difficult to obtain a comprehensive picture of Zero Trust Architecture research as well as identify unsolved problems in this field.

This research intends to conduct an analysis of global trends in literature on Zero Trust Architecture using bibliometric methods. Particularly, this study is aimed at studying the patterns of publications in the area, prominent authors, journals, institutes, and countries making contributions to Zero Trust Architecture researches, and analyzing citation patterns and new themes of research. Using bibliometric methods, this research gives a detailed analysis of the intellectual structure of literature on Zero Trust Architecture and shows directions for further research.

## 2. METHODS

This research uses the bibliometric analysis technique to analyze the development and research trends of Zero Trust Architecture (ZTA). Bibliometric analysis is a quantitative research technique that can be used to assess scientific publications by recognizing patterns of publications, citation structures, intellectual connections, and new research directions in a certain knowledge domain [12]. This method was chosen for the research because Zero Trust Architecture is an interdisciplinary and dynamic research field that includes cybersecurity, information systems, networking, cloud computing, and digital transformation. Through bibliometric analysis, this study intends to have an in-depth understanding of the development, structure, and evolution of research on ZTA instead of focusing only on its technical implementation. The research will undergo several steps including the selection of the database, retrieval of the literature, cleaning of data, analysis of performance, and science mapping analysis.

The data collection procedure involved use of the Scopus database as the main platform to access scientific articles owing to the wide range of peer-reviewed scientific works available in it and because it is applicable for bibliometric analysis. The searching process aimed at accessing scientific publications concerning Zero Trust Architecture by applying certain keywords such as “zero trust architecture,” “zero trust security,” “zero trust network” among others that can be found in the title, abstract and keywords of articles. Only relevant document types such as journal articles and conferences papers were used in the searching process, whereas unrelated publications were excluded. The retrieved data comprised information about the publication such as the name of the publication, authors and their affiliation, citations, keywords and references.

Analysis of the cleaned data set was done through bibliometric visualization and mapping approaches assisted by VOSviewer tool. Some of the approaches used included performance analysis and science mapping analysis. Performance analysis was carried out for the identification of publication trends, citation impact, productive authors, influential sources, and contributions at country level. On the other hand, science mapping analysis was used to find the relationships between authors, institutions, keywords, and themes of study using approaches such as co-authorship analysis, co-occurrence analysis, and citation network analysis. In particular, keyword co-occurrence analysis was done to find the main themes and emerging areas of study related to Zero Trust Architecture.

## 3. RESULTS AND DISCUSSION

### 3.1 Co-Authorship Analysis

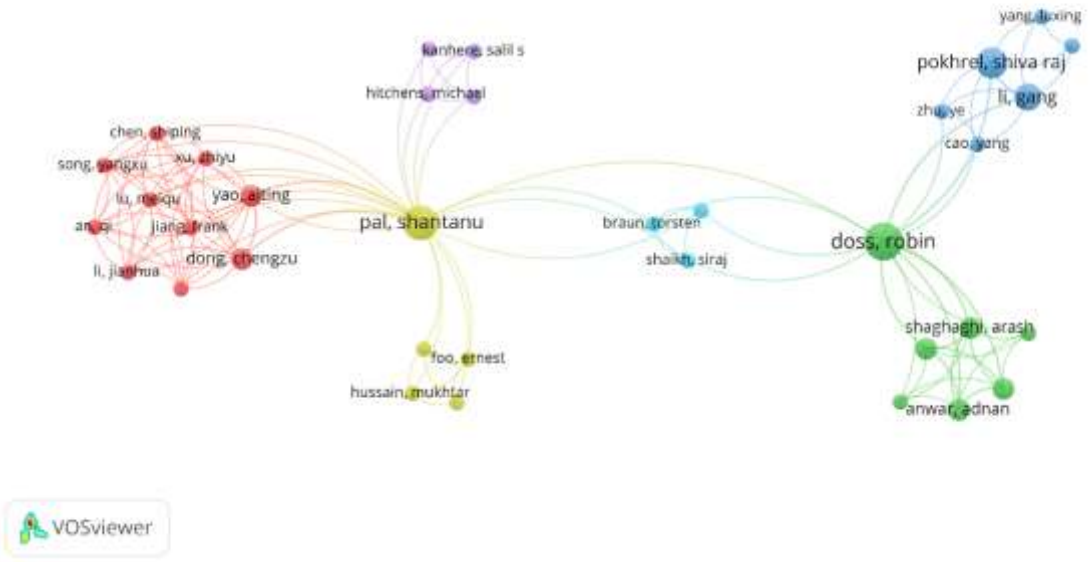


Figure 1. Author-Level Visualization
*Source: Data Analysis*

The collaborative relationship of the researchers on the ZTA is illustrated in Figure 1. The network is characterized by the presence of a number of different clusters, which are highlighted in different colors depending on the degree of collaboration between the authors or their contribution to the same research area. The most highly interconnected nodes are those of Doss, Robin, Pal, Shantanu, and Pokhrel, Shiva Raj, which belong to the influential authors possessing a greater degree of collaboration and centrality in the research network.

It is clear from the visualization that the ZTA research area involves collaboration between multiple research groups rather than one dominant research group. The red cluster in the middle that comprises authors such as Dong, Chengzu, Yao, Aiting, and Li, Jianhua is indicative of a research stream in relation to technical aspects of security and system-level approaches, whereas the green and blue clusters consisting of authors like Doss, Robin, Pokhrel, Shiva Raj, et al., show the way in which ZTA research has proceeded in relation to cybersecurity applications, authentication, and security management. The existence of bridging authors, namely Pal, Shantanu and Doss, Robin, points to the fact that ZTA research has been carried out in a multidisciplinary manner linking security models with their implementation.

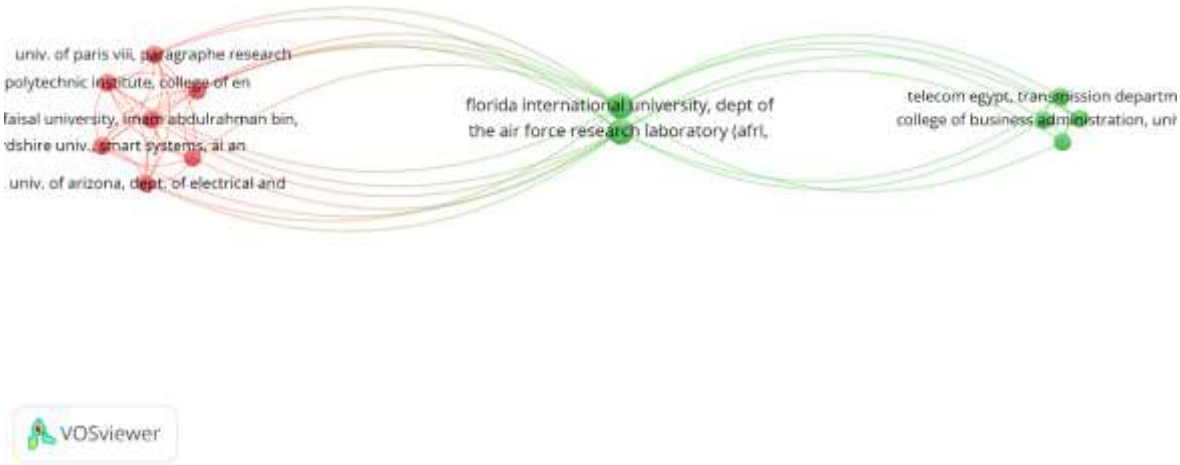


Figure 2. Institution-Level Visualization
*Source: Data Analysis*

Figure 2 represents the relations between organizations involved in the development of Zero Trust Architecture (ZTA). In this graph, one can notice that there are many institutional groups, which are related to each other through collaboration links, thereby indicating the fact that the research in Zero Trust architecture has evolved in collaboration between institutions of education, research labs and industry-related organizations. Both Florida International University and Department of the Air Force Research Laboratory (AFRL) stand out as central nodes because they are highly connected with many other institutions, thus showing the significance of these two organizations as collaboration centers. Other organizations, such as the universities of the United States, telecommunication organizations and international academic institutions, have been observed to be interconnected, thereby showing that the research on Zero Trust is a global phenomenon.
.

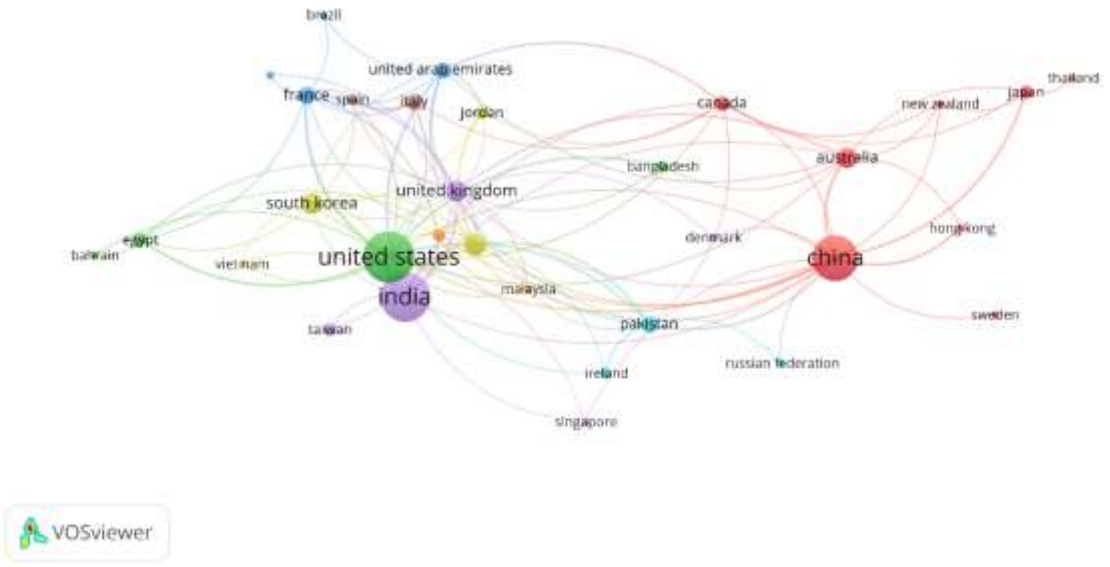


Figure 3. Country-Level Visualization
*Source: Data Analysis*

The network shown in Figure 3 shows the worldwide distribution and patterns of international collaboration of ZTA research. From the figure below, one can see that there are several nations which are well-connected through research activities, and they are the most prominent nations as far as ZTA research is concerned because of large sizes of nodes and collaborations between them. For instance, United States is a well-connected hub in the middle of the network where several other research clusters from Asia, Europe and many other regions are attached. This shows that the nation plays a major role in cybersecurity research and Zero Trust research and development. In addition, China is another nation that occupies a strategic position in collaboration with countries like Australia, Canada, Japan and New Zealand.

It should also be noted that the visualization illustrates the fact that ZTA research has evolved into an internationally cooperative endeavor with the participation of research clusters from many countries across the globe, namely those from Europe, Asia, North America, and even the Middle East. Such countries as the United Kingdom, South Korea, Australia, Canada, and Singapore have become connecting nodes that help in exchanging knowledge between research clusters. The variety of international connections proves that Zero Trust Architecture does not represent any geographical specificity but rather represents an internationally significant issue related to cybersecurity that is relevant to all countries due to such problems as cloud computing and cyberattacks.

### 3.2 Citation Analysis

Table 1. The Most Impactful Literatures

| Citations | Authors and year | Title |
|---|---|---|
| 340 | [13] | Zero Trust Architecture (ZTA): A Comprehensive Survey |
| 233 | [14] | A Survey on Zero Trust Architecture: Challenges and Future Trends |
| 203 | [15] | A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture |

| Citations | Authors and year | Title |
|---|---|---|
| 186 | [16] | Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN |
| 148 | [17] | Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions |
| 119 | [18] | Migrating to Zero Trust Architecture: Reviews and Challenges |
| 101 | [19] | Decentralized Federated Graph Learning With Lightweight Zero Trust Architecture for Next-Generation Networking Security |
| 94 | [20] | Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures |
| 88 | [21] | A Comprehensive Framework for Migrating to Zero Trust Architecture |
| 74 | [22] | Augmenting Zero Trust Network Architecture to enhance security in virtual power plants |

*Source: Scopus, 2026*

The most influential literature in ZTA research is presented in Table 1, which contains information on the most cited works that have played an important role in forming the field of ZTA research. The most cited article is [13], which is called "Zero Trust Architecture (ZTA): A Comprehensive Survey" and includes 340 citations. Thus, it has played a significant role in building theoretical foundations as an important work providing information about the principles of ZTA, its elements, and problems of implementation. The second most cited work is [14], which is titled "A Survey on Zero Trust Architecture: Challenges and Future Trends" and includes 233 citations. It has contributed to theoretical foundations by addressing the problems and prospects of future research. Other highly influential publications are devoted to particular applications of ZTA in terms of different technological aspects, such as 5G smart healthcare security [15], 5G/6G network security with machine learning [16], and Web3 security architecture [17]. In general, it can be concluded that initial ZTA research was focused on the formation of theoretical basis and problem identification.

It can be seen from the citation network that there is a trend of moving towards the practical aspect and implementation of ZTA within domains. The papers, such as [18] and [21], discuss migration policies and implementation approaches, which represent problems related to organizational transition from existing security architecture to ZTA. Recent papers, such as [23] on decentralized federated graph learning, [20] on industrial IoT cybersecurity, and [22] on virtual power plant, represent how ZTA is combined with modern technological advancements like AI, IoT, and critical infrastructure cybersecurity.

### 3.3 Keyword Co-Occurrence Analysis

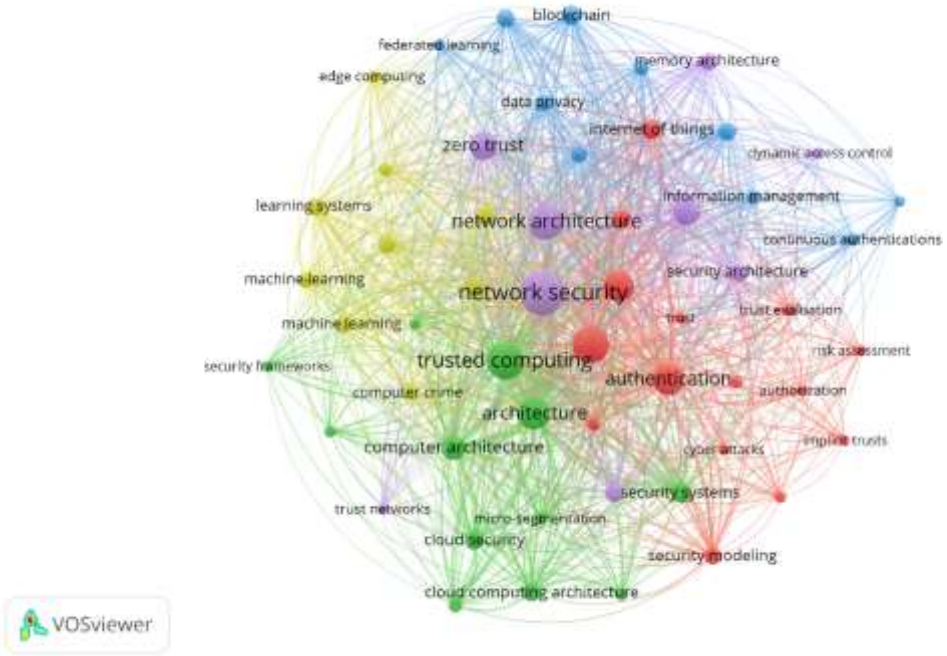


Figure 4. Network Visualization
*Source: Data Analysis*

Figure 4 illustrates the intellectual structure and major research themes within Zero Trust Architecture (ZTA) studies. The network demonstrates a highly interconnected research landscape, where multiple keywords are linked through strong co-occurrence relationships, indicating that ZTA research has developed as a multidisciplinary field involving cybersecurity, network engineering, cloud computing, artificial intelligence, and emerging digital technologies. The size of each node represents the frequency of keyword occurrence, while the connecting lines indicate the strength of relationships between research topics. Keywords such as "network security," "authentication," "trusted computing," "network architecture," and "zero trust" appear as dominant nodes, suggesting that these concepts represent the central foundations of ZTA research.

The red cluster denotes research related to security solutions, identity management, and access control schemes. Usage of keywords such as authentication, authorization, trust assessment, risk assessment, security architecture, and cyber-attacks shows that a large part of ZTA literature deals with the move from the old-fashioned perimeter-based security system to continuous verification and access control. This cluster corresponds to the primary idea of Zero Trust – continuous verification of users, devices, and applications before access is granted. It proves the direct connection between the concepts of authentication, authorization, and risk assessment.

The green cluster reveals the connection between trusted computing, cloud security, and protection of the network infrastructure. The key terms like trusted computing, cloud security, micro-segmentation, trust networks, computer architecture, and cloud computing architecture show that ZTA becomes more popular in the realm of distributed computing. The green cluster implies that researchers explore how the principles of Zero Trust can be used to protect current infrastructures where traditional network borders lose their effectiveness due to the transition to the cloud, the use of remote access, and hybrid IT infrastructures.

The blue cluster encompasses new directions in technology linked to advanced computing environments and intelligent

security solutions. The terms blockchain, Internet of Things, data privacy, federated learning, edge computing, and dynamic access control are among keywords suggesting that current research in ZTA goes far beyond traditional approaches to cybersecurity. In other words, researchers are studying the role of innovative technologies in facilitating decentralization, protecting privacy, and making security decisions. The relationship between Zero Trust and technologies like blockchain and machine learning illustrates increasing interest in designing autonomous and intelligent security systems.

The yellow keyword cluster focuses on the use of artificial intelligence and machine learning techniques within the Zero Trust ecosystem. The keywords such as machine learning, machine-learning, learning systems, and edge computing are indicative of an emerging research trend in the direction of the application of intelligent algorithms for threat detection, anomaly detection, and automation of the trust assessment process. The overall network of keywords suggests an emergence of ZTA research as a shift from a conventional security architecture framework to a holistic cybersecurity framework incorporating identity management, cloud architecture, artificial intelligence, and decentralization.

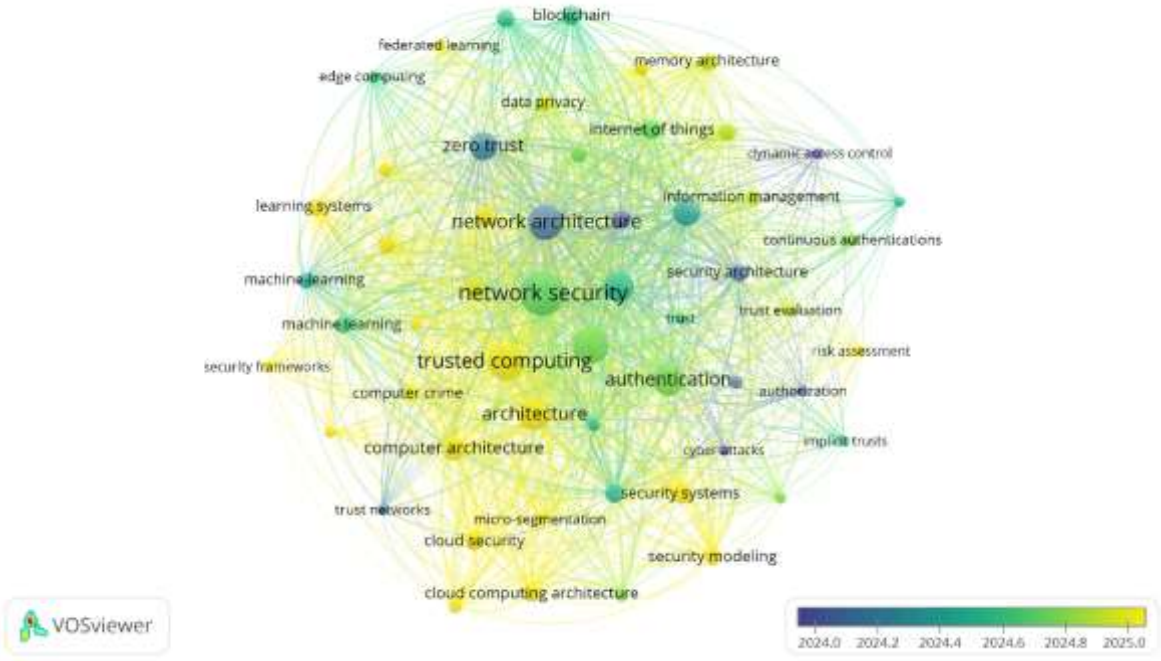


Figure 5. Overlay Visualization
*Source: Data Analysis*

Figure 5 illustrates the temporal development of research topics related to Zero Trust Architecture (ZTA) based on keyword emergence over time. The color gradient represents the average publication year of keywords, where darker colors indicate earlier research attention and yellow-green colors represent more recent research trends. The visualization shows that foundational concepts such as network security, network architecture, trusted computing, authentication, and architecture have been consistently central within ZTA research. These topics represent the early development phase of Zero Trust studies, focusing on establishing security principles, identity verification mechanisms, and architectural models for replacing traditional perimeter-based security approaches.

The recent trends in research are depicted by those keywords which have a light shade of yellow-green color, which means their relevance is increasing nowadays. For example, the following subjects are relevant: machine learning, learning systems, architecture of cloud computing, cloud security, micro-segmentation, security modeling, and dynamic access control, and all of them point at the increasing tendency of developing intelligent solutions in terms of security. Thus, it can be concluded that modern ZTA research tends to go further than just simple authentication and access control to more advanced solutions which combine artificial intelligence and distributed computing.

The overlay map also draws attention to the growth of research on ZTA in relation to cutting-edge technologies, such as blockchain, federated learning, IoT, edge computing, and data privacy. They are presented as new research topics related to the problem of protecting the ever-more decentralized digital environments. Keyword development reveals that Zero Trust Architecture has moved beyond its origin as a networking security approach and has become a cybersecurity approach for cloud, intelligent, and connected systems. The future research on Zero Trust will probably focus on adaptive approaches which involve AI, privacy-preserving techniques, and decentralized security solutions.

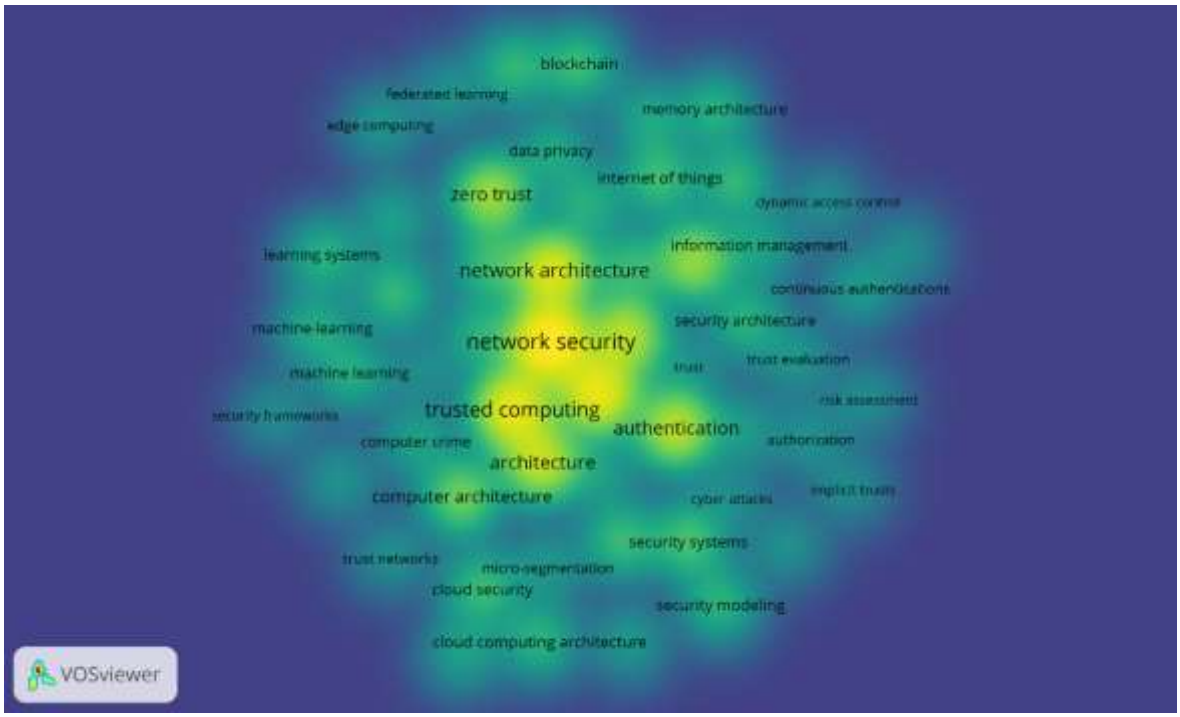


Figure 6. Density Visualization
*Source: Data Analysis*

Figure 6 shows the distribution and significance of the research on the most important themes within Zero Trust Architecture (ZTA). This color gradation shows how dense keywords are found in particular regions, where bright colors show high research density and high association between most important themes. Network security, trusted computing, authentication, network architecture, and architecture have been shown to be the most prominent research fields, because they show the highest keyword density regions. They show the concept of the most important research on ZTA and prove that research concentrated on security models with constant verification and identity access control in networks.

The presented visualization also highlights some of the new and related research areas which can be considered as an

extension to the scope of Zero Trust research. Such fields as machine learning, cloud security, microsegmentation, Internet of Things, blockchain, federated learning, edge computing, and data privacy are present in low-density but still strategically important areas. It shows how ZTA is evolving from being just a protection solution for the network into the solution that covers all cybersecurity needs in order to protect complex digital ecosystems. It can be noted that further researches will likely be more interested in using intelligent approaches, decentralized systems, and adaptive access control systems in order to implement Zero Trust.

**Discussion**

It should be noted that the bibliometric review of the ZTA-related literature shows that there has been considerable intellectual development in this field and it has changed from being a niche cybersecurity idea to becoming a full-fledged security approach for contemporary digital ecosystems. From the trends in publications and citations, one can conclude that the early influential papers were mostly concerned with the definition of the ZTA principles, components, and implementation problems. For instance, highly cited publications such as Syed et al. (2022) and He et al. (2022) show that the importance of foundational literature reviews in laying the theoretical basis for ZTA is determined by such concepts as identity-centric security, continuous verification, least-privilege access, and the weaknesses of perimeter-based security.

The collaboration networks' analysis clearly shows that research on ZTA has progressed via wide-scale cooperation of countries and institutions. Countries like the United States, China, and India being among the top three contributors can be attributed to their significant contribution towards cybersecurity innovations and protecting digital infrastructures. The fact that there are many well-connected authors, institutions, and countries reveals that interdisciplinary collaboration is essential in ZTA research and must involve experts in cybersecurity, network engineering, information technology research, and defense. Such collaboration pattern corresponds to the nature of ZTA implementation process since it cannot be solved only from the technological perspective, but needs to have a complex solution including security architecture and organizational governance.

Keyword analysis reveals how the development of ZTA research has progressed from traditional methods of network security to more adaptive, intelligent, and distributed approaches to security. Main topics like network security, authentication, trusted computing, network architecture, and authorization show that the management of identity and trust assessment continuously are the core pillars of Zero Trust deployment. However, recent research trends show an increased connection to new technologies like artificial intelligence, machine learning, blockchain technology, IoT, federated learning, and edge computing. This trend shows how future Zero Trust architecture may use intelligent decision-making systems that will dynamically assess security threats and adapt access policies accordingly. The increased focus on cloud security and micro-segmentation is also caused by the change in enterprise environment, where traditional network perimeter becomes ineffective because of the use of distributed computing.

## 4. CONCLUSION

This bibliometric study presents a detailed analysis of the development of Zero Trust Architecture (ZTA), its intellectual structure, and possible directions for future research. The results reveal that ZTA research has seen great progress due to the growing number of cybersecurity threats, use of cloud technologies, digital transformations, and limitations of conventional perimeter-oriented security approaches. The citation analysis helps identify the seminal works that have greatly influenced the field of study, including the research devoted to Zero Trust Architecture principles, migration to it, and its implementation in cybersecurity systems. Also, the analysis of collaboration allows

identifying that ZTA research has been conducted by the means of close international and institutional collaboration, and the main contributors among countries have been the USA, China, and India. According to the keywords analysis, the topics covered in the current research include network security, authentication, trusted computing, and access control, and the emerging trends are related to artificial intelligence, machine learning, blockchain technology, Internet of Things, federated learning, and cloud security architectures. Therefore, it is evident that Zero Trust Architecture has evolved from being just an approach to network security to becoming a cybersecurity approach, which supports adaptability, intelligence, and decentralization of security measures. The future research should be concentrated on the design of autonomous Zero Trust systems, inter-platform compatibility issues, addressing privacy and governance concerns, and empirical evaluation of ZTA deployment.

## REFERENCES


[1] R. Dube, "A Taxonomy of Segmentation in Network Security," *IEEE Access*, vol. 14, pp. 16921–16935, 2026, doi: 10.1109/ACCESS.2026.3658250.

[2] J. J. Salvo, "Security in a Complex Non-deterministic World: Towards a Quantum Secure Industrial Internet 'qSII&,'" in *AMSec 2021 - Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security, co-located with CCS 2021*, Cognitive Blocks AI Inc., Schenectady, NY, United States: Association for Computing Machinery, Inc, 2021, pp. 1–2. doi: 10.1145/3462223.3485597.

[3] Z. Xie, L. Wang, H. Wu, X. Zhang, L. Wang, and H. Yang, "SUNET: Framework, Security, and Privacy," in *Proceedings - 2024 International Conference on Satellite Internet, SAT-NET 2024*, Southeast University, School of Cyber Science and Engineering, Nanjing, 211189, China: Institute of Electrical and Electronics Engineers Inc., 2024, pp. 30–36. doi: 10.1109/SAT-NET62854.2024.00014.

[4] P. K. Dhillon, J. Jyoti, and S. Kalra, "Shielding IoT-Driven Healthcare: A Secure and Lightweight Authentication Protocol for Patient Data Protection," *Quantum-Enhanced Cloud AI: The Next Frontier in Machine Learning and Deep Learning*. Bentham Science Publishers, Department of Computer Science, Guru Nanak Dev University, Regional Campus Jalandhar, Punjab, Jalandhar, India, pp. 205–223, 2026. doi: 10.2174/9798898813215126010015.

[5] S. Sudarsan, A. Patel, C. Upadhyay, V. Gudur, and P. Matam, "Secure Prompt Engineering Patterns for Cloud LLM Agents," in *2026 IEEE 5th International Conference on AI in Cybersecurity, ICAIC 2026*, Kindercare Learning Companies, Portland, United States: Institute of Electrical and Electronics Engineers Inc., 2026. doi: 10.1109/ICAIC67076.2026.11395764.

[6] M. A. Vincenzo, N. J. Lowen, A. Gandawidjaja, and A. Kurniawan, "Comparing and Evaluating the Effectiveness of File Activity-Based Authentication Compared to Multi Factor Authentication," in *2026 Middle East and North Africa Communications Conference, MENACOMM 2026*, Bina Nusantara University, Jakarta, Indonesia: Institute of Electrical and Electronics Engineers Inc., 2026. doi: 10.1109/MENACOMM69507.2026.11532935.

[7] G. C. Cuenca and A. P. Domínguez, "Securing enterprise communications: Human-centric practices and emerging research," *Comput. Secur.*, vol. 168, 2026, doi: 10.1016/j.cose.2026.104954.

[8] A. Mittal, "AI-Enabled DevSecOps for Secure Cloud Deployments," *Revolutionizing the Cloud: Generative AI, Security, and Sustainability*. Springer Nature, University of the Cumberlands, Williamsburg, KY, United States, pp. 323–347, 2026. doi: 10.1007/978-3-032-07479-9_16.

[9] R. Vijayalakskmi *et al.*, "ASIC-Based AI Accelerator with Quantum-Inspired Optimization for Blockchain Validation and Fraud Detection," in *International Conference on AI-Driven Innovations and Applications, IC-AIDA 2026 - Conference Proceedings*, Anna University, Rajalakshmi Institute of Technology, Department of Computer Science and Business System, Chennai, India: Institute of Electrical and Electronics Engineers Inc., 2026. doi: 10.1109/IC-AIDA68291.2026.11564453.

[10] D. Kim, S. Park, D. Kim, and I. You, "The NFT Transition for Certificates of Mobile Network," *J. Internet Technol.*, vol. 27, no. 3, pp. 323–336, 2026, doi: 10.70003/160792642026052703004.

[11] W. B. Glisson and J. T. McDonald, "Cyber Operations, Defense, and Forensics Minitrack," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, B. T.X., Ed., Louisiana Tech University,

United States: IEEE Computer Society, 2025, pp. 7090–7091. [Online]. Available: https://www.scopus.com/pages/publications/105005137891?origin=resultslist

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

[13] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.

[14] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A Survey on Zero Trust Architecture: Challenges and Future Trends," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/6476274.

[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] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Comput. Networks*, vol. 217, 2022, doi: 10.1016/j.comnet.2022.109358.

[17] P. P. Ray, "Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions," *Internet Things Cyber-Physical Syst.*, vol. 3, pp. 213–248, 2023, doi: 10.1016/j.iotcps.2023.05.003.

[18] S. Teerakanok, T. Uehara, and A. Inomata, "Migrating to Zero Trust Architecture: Reviews and Challenges," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/9947347.

[19] X. Zhou *et al.*, "Decentralized Federated Graph Learning With Lightweight Zero Trust Architecture for Next-Generation Networking Security," *IEEE J. Sel. Areas Commun.*, vol. 43, no. 6, pp. 1908–1922, 2025, doi: 10.1109/JSAC.2025.3560012.

[20] C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," *Ad Hoc Networks*, vol. 156, 2024, doi: 10.1016/j.adhoc.2024.103414.

[21] P. Phiayura and S. Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture," *IEEE Access*, vol. 11, pp. 19487–19511, 2023, doi: 10.1109/ACCESS.2023.3248622.

[22] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, "Augmenting Zero Trust Network Architecture to enhance security in virtual power plants," *Energy Reports*, vol. 8, pp. 1309–1320, 2022, doi: 10.1016/j.egyr.2021.11.272.

[23] J. Ma *et al.*, "ZTKA: A Zero-Trust Based Kernel Encryption Architecture for Transparent Data Protection," in *Proceedings of the International Conference on Computer Supported Cooperative Work in Design, CSCWD*, S. W., S. W., A. M.-H., M. N., B. J.-P., L. J., Z. J., Z. H., and P. K., Eds., Institute of Information Engineering, Chinese Academy of Sciences, China: Institute of Electrical and Electronics Engineers Inc., 2025, pp. 1981–1986. doi: 10.1109/CSCWD64889.2025.11033649.