West Science Social and Humanities Studies
Vol. 4, No. 07, July 2026, pp. 948-959

Cloud-Native Security in Informatics: A Bibliometric Analysis of Emerging Research

Loso Judijanto[1], Arnes Yuli Vandika[2]
[1] IPOSS Jakarta, Indonesia
[2] Universitas Bandar Lampung

Article Info

Article history:

Received Jul, 2026
Revised Jul, 2026
Accepted Jul, 2026

Keywords:

Cloud-Native Security
Cloud Computing
Cybersecurity
DevSecOps
Kubernetes
Bibliometric Analysis

ABSTRACT

Fast development of cloud computing technologies has led to the emergence of cloud-native architecture, which created both new possibilities and challenges in the area of informatics, in particular cybersecurity. Being a set of flexible and scalable cloud-native technologies, such as containers, microservices, Kubernetes and DevOps, cloud-native environments imply complex security risks, such as data protection, network, identity and dynamic infrastructure management. The purpose of this study is to investigate the evolution, scientific structure and future research directions in cloud-native security by means of bibliometric approach. Academic publications were identified within relevant databases and analyzed by means of VOSviewer software to uncover trends in publications, co-occurrence of keywords, citation structures, authors' collaborations and international scientific networks. The results show that cloud-native security research started from basic issues, such as cloud computing, network security, and container technologies to develop into more sophisticated areas, such as DevSecOps, automation, artificial intelligence, anomaly detection, intrusion detection and intelligent cybersecurity systems. The analysis also indicates that the United States has a dominant role in global research contributions, supported by strong collaborations with countries such as India, the United Kingdom, Italy, France, and South Korea. Highly cited studies demonstrate that current research priorities focus on secure cloud architectures, serverless computing, cloud-native observability, container isolation, and autonomous security management. This study provides a comprehensive understanding of the research landscape and highlights future directions toward AI-driven security frameworks, zero-trust architectures, and automated defense mechanisms for resilient cloud-native ecosystems.

Corresponding Author:

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

1. INTRODUCTION

The fast development of cloud computing technology has brought about a radical change in the area of informatics, making it possible to implement, operate and scale up applications in an efficient and flexible manner [1], [2]. Cloud-native

architecture has been introduced in order to exploit cloud capabilities as opposed to monolithic software architecture which had been used earlier [3]. It is characterized by microservices, containerization and orchestration that ensure scalability, resilience and agility. By abstracting infrastructure management, cloud-native architecture makes it possible for enterprises to concentrate on innovation, application performance and service delivery rather than operations [4].

There are inherent security risks posed by cloud-native systems that differ greatly from those present in the conventional IT systems. The cloud-native systems are more dynamic than other systems because they consist of ephemeral containers, microservices, and serverless functions communicating with each other through distributed networks [5], [6]. All of these can pose risks to the system, for example, container risks, orchestration risks, and identity and access management risks. Distributed systems make it hard for the system to be visible and monitored; therefore, conventional security measures cannot be effective.

Due to various cyber threats, such as ransomware, data breaches, and supply chain attacks, there is an increased need for effective cloud-native security [7]. Companies are under pressure from regulations to provide data privacy and compliance with standards, such as GDPR, HIPAA, and ISO/IEC 27001. Apart from external threats, insider threats and misconfigurations continue to be major factors of cloud-native insecurity. With the rapid adoption of cloud-native technologies in areas, such as healthcare, banking, and e-commerce, secure deployment and maintenance have become a crucial part of enterprise security management [8].

Although cloud-native security has become increasingly crucial, the research field in this domain lacks coherence. Some researchers and professionals have considered particular elements of security, such as containerization, runtime threat detection, and policy enforcement, but their research lacks coherence as well [9]. Moreover, the speed of technological advancement frequently leads to new knowledge creation that surpasses the current scholarly discourse about cloud-native technologies. In other words, the gap between practices and research in this field keeps on growing. Bibliometric analysis can be a helpful tool to determine the intellectual structure and trends of the cloud-native security body of knowledge.

There is a connection between informatics and cloud-native security research that has been developed recently because of the importance of using data-driven methods, analytics and machine learning approaches in detecting risks and threats [10]. Using big datasets allows cloud-native systems to incorporate security analysis tools into the software development process and implement preemptive measures to counter threats. The interaction of informatics and cloud-native security calls for an awareness of recent trends, themes and significant works within the field of research.

In spite of the growing usage of cloud-native architectures and the increased attention to security issues, the academic literature is fragmented and does not consolidate the available knowledge in sub-disciplines like container security, orchestration security, and runtime security. It makes the identification of important trends, evaluation of methods, and prioritization of further research problematic. If there is no structure in the existing academic literature, the important problems can be overlooked and the best practices cannot be adopted properly by all informatics specialists. That is why there is a need for conducting a bibliometric analysis in order to identify the state of art in research, trends and understudied fields in the field of cloud-native security. The purpose of the research is the bibliometric analysis of emerging research in cloud-native security.

2. METHODS

The present research uses the bibliometric analysis method to analyze the state of research on cloud-native security in

informatics. Bibliometric analysis allows for systematic analysis of publication dynamics, citation networks, and thematic trends, thus providing a way to reveal the intellectual structure of a research field [11]. Using quantitative analysis of publication metadata including authors' names, keywords, affiliations, and citations, bibliometrics provides a means to objectively analyze scientific literature, identify influential publications, and detect emerging research areas. It is especially useful when researching fast-developing fields such as cloud-native security, which have a vast literature base difficult to analyze using conventional methods.

For the data collection process, the Scopus database was used, since it indexes peer-reviewed journals, conference papers, and book chapters in informatics and computer science. The following search query terms were used in the search for documents: “cloud-native,” “security,” “container security,” “microservices,” “serverless computing.” For the time frame, it was limited to 2015-2026, to obtain up-to-date data and the most recent research articles. The inclusion criteria were as follows: only the articles published in English and written on cloud-native security within an informatics context, and indexed either in peer-reviewed journals or conference papers. Duplicates were excluded, and then title, authors, abstract, keywords, affiliation, year of publication, and citations were exported for further analysis.

For the analysis of the processed Scopus data, VOSviewer, a software application developed for creating and analyzing bibliometric networks, was used [12]. With VOSviewer, one can conduct analyses of co-authorship, co-citations, and keywords co-occurrences to find the most prominent authors, journals, organizations, and research themes in the field of cloud-native security. With the help of network maps, one can visualize clusters of related topics, collaboration among authors and organizations, as well as changes in the research focus over time. Thus, the research methodology helps to give an overview of the developing scholarly field of cloud-native security.

3. RESULTS AND DISCUSSION

3.1 Keyword Co-Occurrence Network

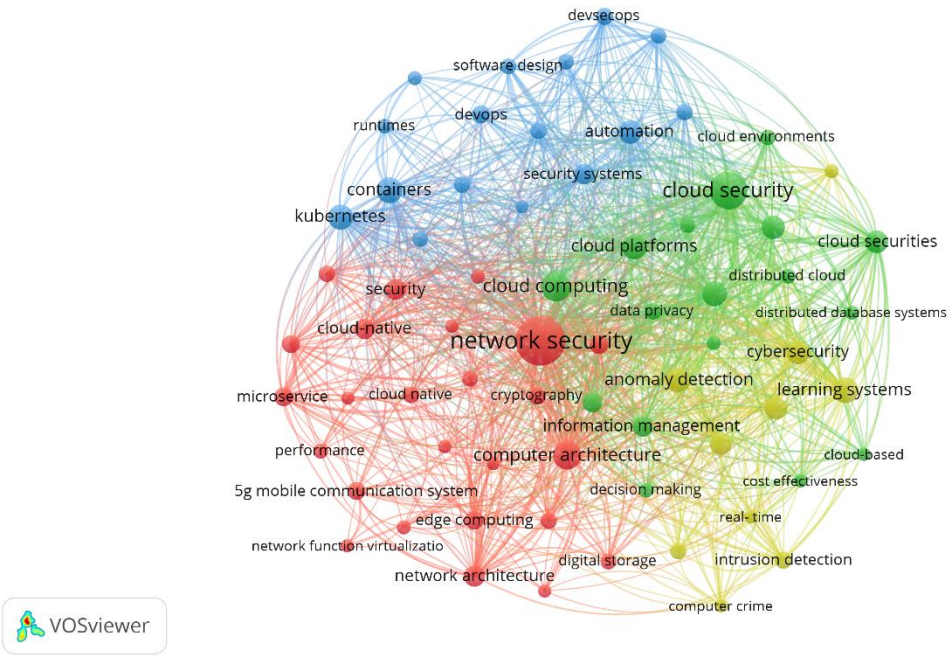

Figure 1. Network Visualization

Source: Data Analysis Result, 2026

As can be seen in Figure 1, this figure provides an overview of the intellectual structure and thematic relationships in cloud-native security informatics research. In the network presented here, there are a number of clusters connected to each other with different colors denoting various major themes that have been emerged through research in this domain. In the network presented here, the size of each node denotes the frequency of the occurrence of the keyword while the lines between nodes denote the strength of relationships between keywords.

The cluster in red denotes the dimension related to security and networking in cloud-native research. The terms used as keywords, namely network security, security, cloud-native, cloud computing, cryptography, microservice, network architecture, and computer architecture, show that the earliest studies done were centered on the need to secure cloud infrastructure. It shows concerns related to the protection of communication networks, creating secure architecture, and maintaining confidentiality and integrity in cloud infrastructure. There is a clear link between cloud-native and network security, which means that security issues are part of architecture transition.

The blue group indicates the software engineering and cloud-native development environment. Key phrases such as containers, Kubernetes, DevOps, DevSecOps, automation, software architecture, and runtimes emphasize the growing need for securing software development processes in cloud-native environments. The blue group implies that there is a growing interest among researchers in studying how security can be integrated into the software lifecycle process as opposed to being regarded as an independent operation. The connection between DevSecOps and other key phrases emphasizes the growing implementation of security automation and CI/CD process in contemporary cloud-native application development.

The green cluster stands for advanced cloud security management and distributed computing. Such keywords as cloud security, cloud environments, cloud platforms, distributed cloud, cloud services, distributed database systems, and data privacy signify research dedicated to securing cloud ecosystems from an organizational and infrastructural point of view. In this way, the green cluster deals with issues related to multi-cloud and distributed environments, such as privacy protection, security of data management, and resistance to cyber attacks. There is no doubt about the close relationship between cloud security and cloud computing as security is always considered when discussing scalable cloud solutions.

The yellow cluster highlights emerging intelligent security approaches and future research directions. Keywords such as cybersecurity, anomaly detection, learning systems, intrusion detection, real-time, and computer crime demonstrate the increasing integration of artificial intelligence and machine learning techniques into cloud-native security mechanisms. This indicates a shift from traditional rule-based security approaches toward adaptive and predictive security solutions capable of identifying complex threats in dynamic cloud environments.

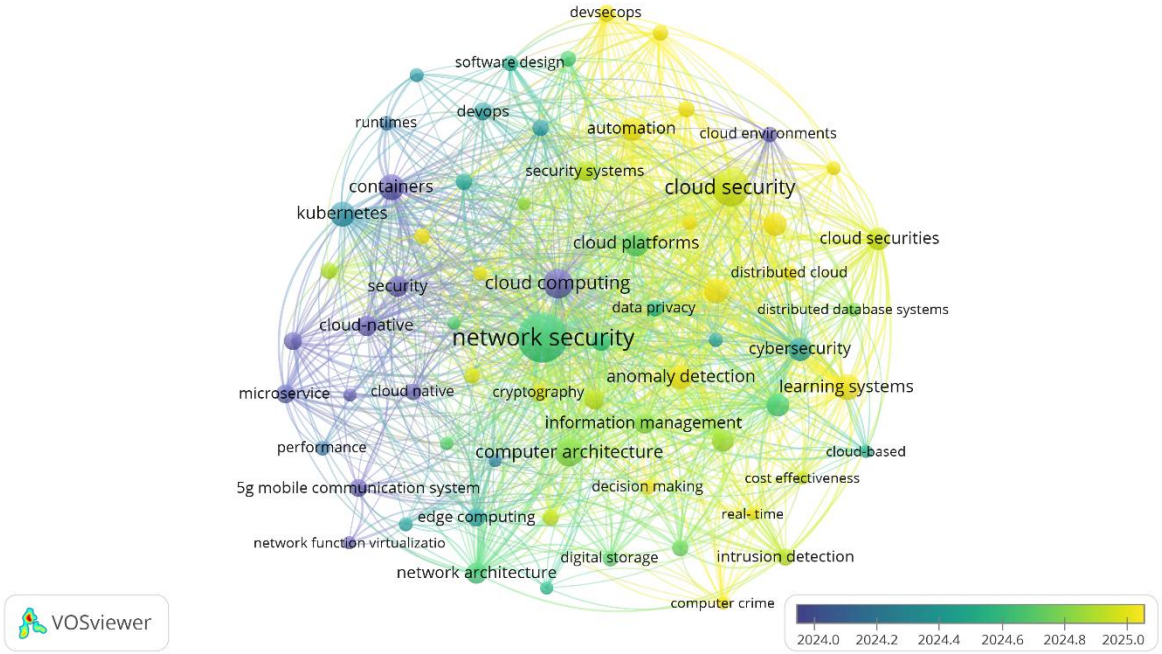

Figure 2. Overlay Visualization
Source: Data Analysis Result, 2026

Temporal evolution of cloud-native security research in informatics is presented in Figure 2 below. The color coding here denotes the average year of publication for the keywords used, whereby the darker the blue, the earlier the topic was researched, while the lighter yellow color shows the relatively newer research topics. From the visual representation, it is clear that the earlier topics include cloud-native, containers, Kubernetes, microservice, network architecture, and network security.

Emerging research trends are highlighted in the form of yellow colored keywords such as cloud security, cloud securities, DevSecOps, automation, cybersecurity, learning systems, anomaly detection, and intrusion detection. These emerging research themes show a move from the conventional infrastructure-based protection approach towards the use of advanced security mechanisms that are intelligent and automated. The rising popularity of DevSecOps and automation shows that the contemporary research is focused on incorporating security techniques in the development processes of software systems.

It can be seen from the results of the overlay analysis that cloud-native security has evolved from architecture-centric research to cutting-edge intelligent security solutions. Previous studies focused on cloud architecture security and container security, whereas latest studies increasingly cover topics such as AI/machine learning based threat detection, real-time monitoring, and automated security. This shows that the future of cloud-native security will likely consist of researching how to integrate cloud-native architectures with AI-powered cybersecurity solutions and zero-trust methodologies.

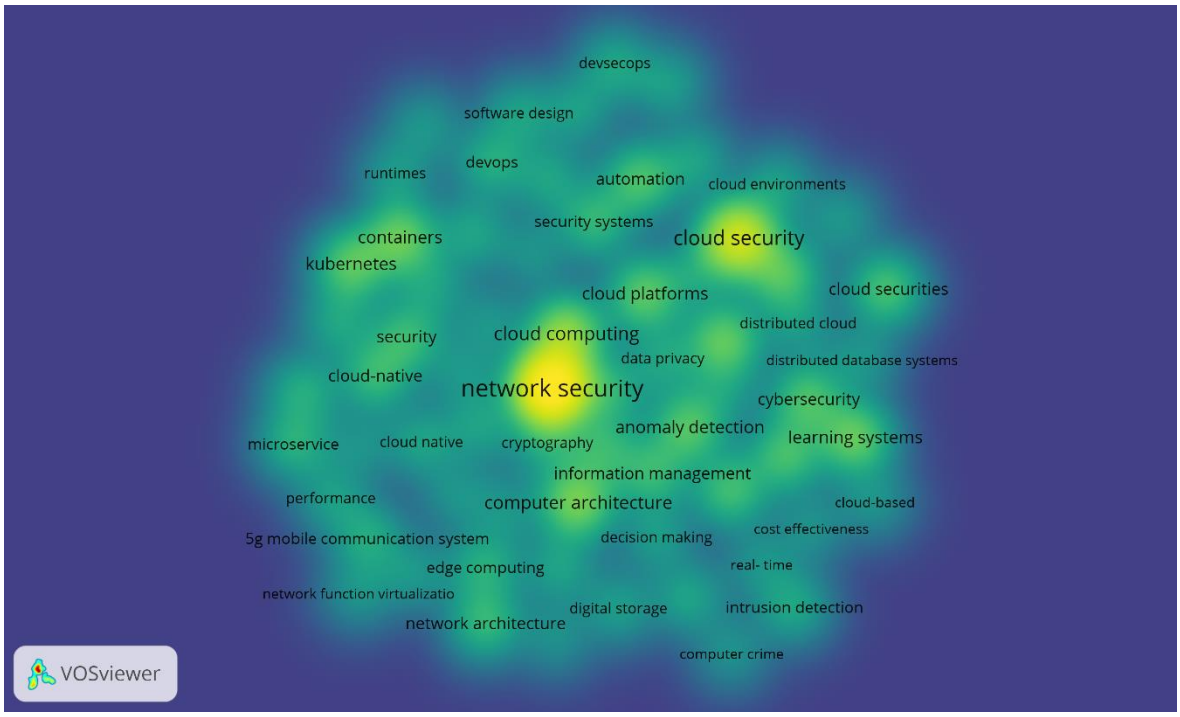

Figure 3. Density Visualization

Source: Data Analysis Result, 2026

The research topic concentration and intensities in the field of cloud-native security in informatics are shown in Figure 3 above. In this case, the intensity of color shows how frequent and significant the keywords are, where more brightly colored areas mean the keywords have more research density. The most notable areas in the map are those that revolve around cloud security, network security, and cloud computing, thus showing that these keywords are what make up the primary research discussion. The visualization further emphasizes some of the developing interconnected themes like cybersecurity, anomaly detection, learning systems, DevSecOps, automation, containers, and Kubernetes. Such topics reveal the rising trend of research on the combination of intelligent solutions and automation in cloud security frameworks. The high density of connections between cloud security, cybersecurity, and anomaly detection reveals that the recent research has been focused more on threat detection and automated solutions.

3.2 Co-Authorship Analysis

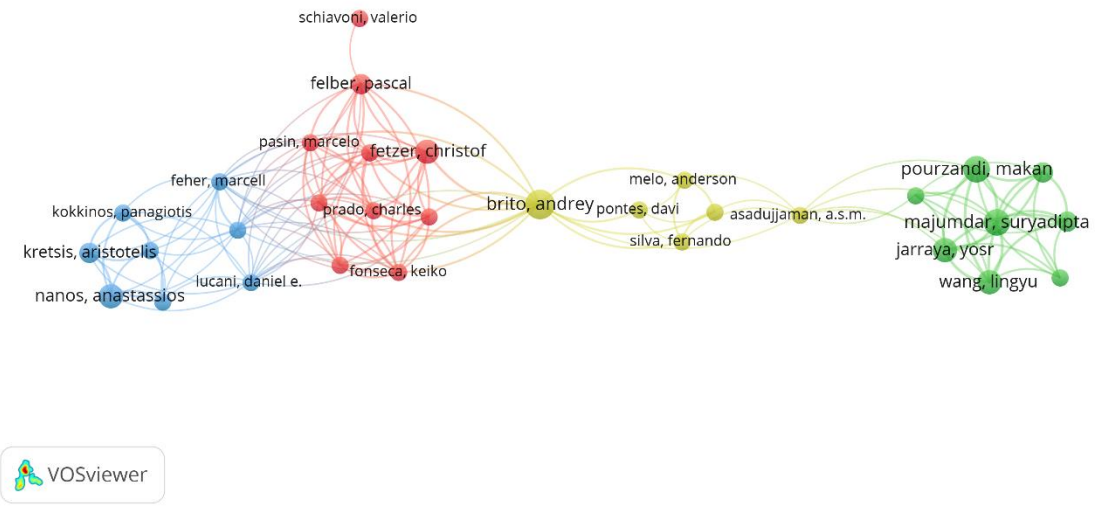

Figure 4. Author Visualization
Source: Data Analysis Result, 2026

Figure 4 shows the relationship and cooperation between authors in the field of cloud-native security in informatics. There are multiple clusters, colored differently, which represent the groups of authors cooperating or working within similar research topics. The largest group, marked red, includes the following authors: Felber, Pascal; Fetzer, Christof; Pautasso, Cesare; Prado, Charles; Fonseca, Keiko. This group can be seen as a very well-cooperated one, working on topics of distributed systems, cloud architectures, and secure software environment. The blue group includes such authors as Kretzis, Aristotelis; Kokkino, Panagiotis; Nanos, Anastasios; and Lucani, Daniel E. It is another research group having relatively independent cooperation with other members of the group. The green group, including such authors as Majumdar, Suryadipta; Pourzandi, Makan; Jarraya, Yosr; and Wang, Lingyu, can be seen as another cooperation network, focused more specifically on cybersecurity, cloud security mechanisms, and privacy issues. Links between the clusters, especially with such influential authors as Brito, Andrey, and Ponte, David, represent the knowledge exchange between different research communities.

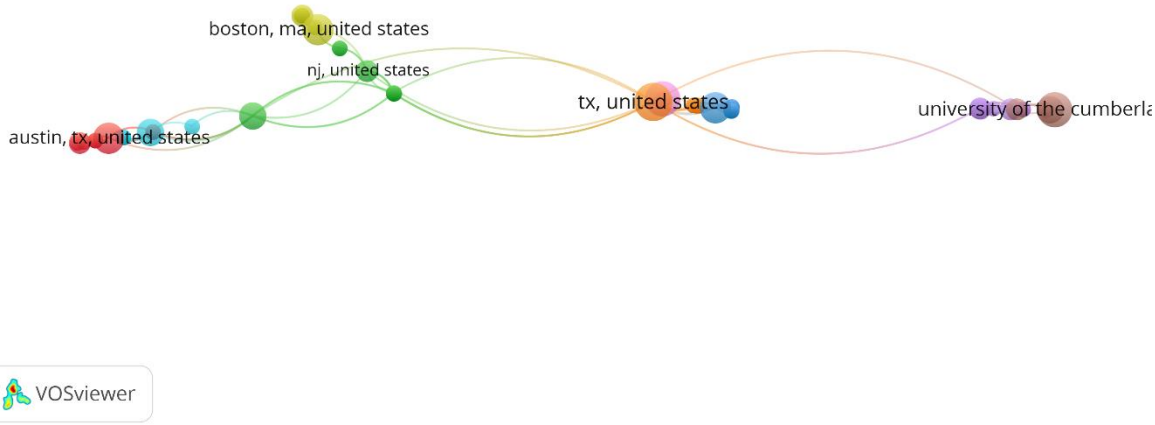

Figure 5. Institution Visualization
Source: Data Analysis Result, 2026

The geographical distribution and collaboration of research contributors in cloud-native security in informatics are presented in Figure 5 below. As can be seen, collaboration in research in this field takes place mainly in the United States, with cities like Austin, Boston, NJ (New Jersey), and TX (Texas) being the connected nodes. This country emerges as the major hub for collaboration in this field of study and research, which shows considerable contributions made by American scientists. The connections between these nodes show how cooperation among research groups takes place in different geographical areas. Furthermore, the University of the Cumberland also emerges as one of the connected nodes, showing contributions made by other universities too.

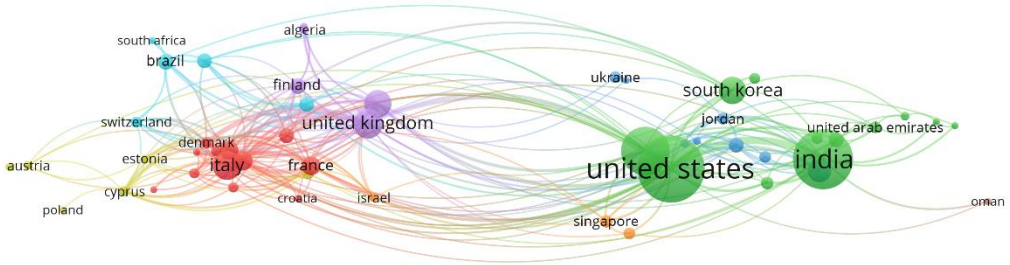

Figure 6. Country Visualization
Source: Data Analysis Result, 2026

The global research collaboration trend in the area of cloud-native security in informatics is presented in Figure 6. The network shows that the United States is the largest and most influential country in contributing to the research area since it has the biggest node and is connected to many other countries through several links. This implies that the country has a lead position in the research collaboration process in the field of cloud-native security. Other countries contributing to the research area include India, the United Kingdom, Italy, France, and South Korea.

The map indicates the presence of a number of collaboration clusters in different regions. European countries such as the United Kingdom, Italy, France, Denmark, Austria, Poland, and Finland make up a well-connected cluster, which is indicative of intense research collaboration among the Europeans on matters pertaining to cybersecurity, cloud computing, and distributed systems. On the other hand, Asian researchers from India, South Korea, Jordan, Singapore, and the United Arab Emirates have increasingly been engaging in collaboration in their research work concerning cloud security applications.

3.3 Citation Analysis

Table 1. Top Cited Research

Citations	Authors and year	Title
265	[13]	Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research
202	[14]	Cloud-Native Applications
178	[15]	The Serverless Computing Survey: A Technical Primer for Design Architecture
103	[16]	Iot Forensics: Challenges for the Ioa Era
102	[17]	X-Containers: Breaking Down Barriers to Improve Performance and Isolation of Cloud-Native Containers

Citations	Authors and year	Title
67	[18]	Disrupting healthcare silos: Addressing data volume, velocity and variety with a cloud-native healthcare data ingestion service
61	[19]	Security in Cloud-Native Services: A Survey
61	[20]	E-BPF: A New Approach to Cloud-Native Observability, Networking and Security for Current (5G) and Future Mobile Networks (6G and Beyond)
61	[21]	Spatially Explicit Seagrass Extent Mapping Across the Entire Mediterranean
61	[22]	TeraFlow: Secured autonomic traffic management for a tera of SDN flows

Source: Scopus, 2026

In Table 1 are listed some of the highest cited works that have contributed to the creation of cloud-native security and general cloud computing. The most influential article in terms of citation numbers is [13] with 265 citations and its subject concerns the metrics of the performance evaluation of cloud, fog, and edge computing which proves the significance of benchmarking and evaluation of distributed computing systems. The second article in the list, [14], which is cited 202 times, touches upon the topic of cloud-native applications and gives the basic knowledge of cloud-native architecture and its differences from traditional cloud systems. The third in the list is research conducted by [15] on the topic of serverless computing which has 178 citations and shows the relevance of serverless architectures as an important part of cloud-native ecosystem. Other cited researches concern such topics as IoT forensics, cloud-native container isolation, cloud-native data management for healthcare, and secure network management. In particular, such articles as [19] on cloud-native security and [23] on eBPF-based cloud-native observability and security show the trend towards enhancing security mechanisms.

4. CONCLUSION

The results of this bibliometric study offer a complete review of the evolution, intellectual structure, and research trends related to cloud-native security in informatics. The results show that cloud-native security has evolved into a growing area of research due to the growing application of cloud computing, container technology, microservices, and distributed computing. The keyword analysis suggests that initial research has been mainly concerned with the protection of cloud infrastructure, network security, containerization, and cloud-native architectures, but the current research is oriented towards more advanced methodologies in the form of DevSecOps, automation, threat detection through artificial intelligence, anomaly detection, and intelligent cybersecurity systems. Research collaboration shows that research efforts are widely distributed across the globe, with the United States being the most active participant in the process, followed by other nations like India, the United Kingdom, Italy, and others. Most-cited publications prove that the area has evolved from cloud performance and architectural studies to more specific areas such as serverless computing, cloud-native secure services, container isolation, observability, and autonomous security management.

REFERENCES

[1] M. Moore, T. K. Kuppusamy, and J. Cappos, "Artemis: Defanging Software Supply Chain Attacks in Multi-repository Update Systems," in *ACM International Conference Proceeding Series*, New York University, New York City, United States: Association for Computing Machinery, 2023, pp. 83–97. doi: 10.1145/3627106.3627129.

[2] R. Behravesh, D. Coroama, M. Nikroo, M. Gholami, N. Agrawala, and R. N. Mitra, "AI-Driven Traffic Steering xApp for Open RAN: A Cloud-Native Quantum-Safe Approach," in *Proceedings of the 11th IEEE International Conference on Network Softwarization, NetSoft 2025*, V. P., C. W., F. C., S. R., and T. M., Eds., Net Reply, London, United Kingdom: Institute of Electrical and Electronics Engineers Inc., 2025, pp. 49–54. doi: 10.1109/NetSoft64993.2025.11080591.

[3] P. Raj, N. Gayathri, and G. J. W. Kathrine, *Artificial Intelligence for Precision Agriculture*. Edge AI Division, Reliance Jio Platforms Ltd. (JPL), Bangalore, India: CRC Press, 2024. doi: 10.1201/9781003504900.

[4] S. R. Goniwada, *Cloud Native Architecture and Design: A Handbook for Modern Day Architecture and Design with Enterprise-Grade Examples*. Bangalore, United States: Apress Media LLC, 2021. doi: 10.1007/978-1-4842-7226-8.

[5] T. Baptista, R. Jesus, L. B. Silva, and C. Costa, "Scalable Digital Pathology Platform Over Standard Cloud Native Technologies," in *Proceedings - IEEE Symposium on Computers and Communications*, Bmd Software, Ílhavo, Portugal: Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ISCC55528.2022.9912933.

[6] F. Yashu, S. M. Rochester, and M. Saqib, "Optimizing Intra-Container Communication with Memory Protection Keys: A Novel Approach to Secure and Efficient Microservice Interaction," in *2025 International Conference on Business Intelligence for Technology Innovation, ICBITI 2025*, Stony Brook University, Dept. of Computer Science, United States: Institute of Electrical and Electronics Engineers Inc., 2025. doi: 10.1109/ICBITI65527.2025.11501025.

[7] R. Kottapalli *et al.*, "Optimizing Alzheimer's Data Analysis Through Multi-Cloud Integration: A Performance and Reliability Approach," *Results Control Optim.*, vol. 23, 2026, doi: 10.1016/j.rico.2026.100687.

[8] A. Alzahrani, "Cognitive ZTNA: A Neuro-Symbolic AI Approach for Adaptive and Explainable Zero Trust Access Control," *Mathematics*, vol. 14, no. 7, 2026, doi: 10.3390/math14071211.

[9] S. Kriaa, S. Papillon, L. Jagadeesan, and V. Mendiratta, "Better Safe than Sorry: Modeling Reliability and Security in Replicated SDN Controllers," in *2020 16th International Conference on the Design of Reliable Communication Networks, DRCN 2020*, Nokia Bell-Labs, Nozay, France: Institute of Electrical and Electronics Engineers Inc., 2020. doi: 10.1109/DRCN48652.2020.1570604424.

[10] T. M. Chettier, V. A. K. Boyina, S. Jorepalli, C. Singh, and N. Gupta, "Scalable Explainable AI with a Cloud-Native Approach for Cybersecurity Threat Detection," in *Proceedings - 3rd International Conference on Advancement in Computation and Computer Technologies, InCACCT 2025*, K. R., K. R., G. M., and G. M., Eds., South Windsor, 06074, CT, United States: Institute of Electrical and Electronics Engineers Inc., 2025, pp. 686–691. doi: 10.1109/InCACCT65424.2025.11011376.

[11] 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.

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

[13] M. S. Aslanpour, S. S. Gill, and A. N. Toosi, "Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research," *Internet of Things (Netherlands)*, vol. 12, 2020, doi: 10.1016/j.iot.2020.100273.

[14] D. Gannon, R. Barga, and N. Sundaresan, "Cloud-Native Applications," *IEEE Cloud Comput.*, vol. 4, no. 5, pp. 16–21, 2017, doi: 10.1109/MCC.2017.4250939.

[15] Z. Li, L. Guo, J. Cheng, Q. Chen, B. He, and M. Guo, "The Serverless Computing Survey: A Technical Primer for Design Architecture," *ACM Comput. Surv.*, vol. 54, no. 10, 2022, doi: 10.1145/3508360.

[16] A. Macdermott, T. Baker, and Q. Shi, "Iot Forensics: Challenges for the Ioa Era," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, Department of Computer Science, Liverpool John Moores University, Liverpool, United Kingdom: Institute of Electrical and Electronics Engineers Inc., 2018, pp. 1–5. doi: 10.1109/NTMS.2018.8328748.

[17] Z. Shen *et al.*, "X-Containers: Breaking Down Barriers to Improve Performance and Isolation of Cloud-Native Containers," in *International Conference on Architectural Support for Programming Languages and Operating Systems - ASPLOS*, University of California, Berkeley, United States: Association for Computing Machinery, 2019, pp. 121–135. doi: 10.1145/3297858.3304016.

[18] R. Ranchal *et al.*, "Disrupting healthcare silos: Addressing data volume, velocity and variety with a cloud-native healthcare data ingestion service," *IEEE J. Biomed. Heal. Informatics*, vol. 24, no. 11, pp. 3182–3188, 2020, doi: 10.1109/JBHI.2020.3001518.

[19] T. Theodoropoulos *et al.*, "Security in Cloud-Native Services: A Survey," *J. Cybersecurity Priv.*, vol. 3, no. 4, pp. 758–793, 2023, doi: 10.3390/jcp3040034.

[20] D. Soldani *et al.*, "E-BPF: A New Approach to Cloud-Native Observability, Networking and Security for Current (5G) and Future Mobile Networks (6G and Beyond)," *IEEE Access*, vol. 11, pp. 57174–57202, 2023, doi: 10.1109/ACCESS.2023.3281480.

[21] D. Traganos *et al.*, "Spatially Explicit Seagrass Extent Mapping Across the Entire Mediterranean," *Front. Mar. Sci.*, vol. 9, 2022, doi: 10.3389/fmars.2022.871799.

[22] R. Vilalta *et al.*, "TeraFlow: Secured autonomic traffic management for a tera of SDN flows," in *2021 Joint European Conference on Networks and Communications and 6G Summit, EuCNC/6G Summit 2021*, Centre Tecnològic de

Telecomunicacions de Catalunya (CTTC/CERCA), Castelldefels, Spain: Institute of Electrical and Electronics Engineers Inc., 2021, pp. 377–382. doi: 10.1109/EuCNC/6GSummit51104.2021.9482469.

[23] F. Ponce, J. Soldani, C. Taramasco, A. Brogi, and H. Astudillo, "Beyond Security: Understanding the Multiple Impacts of Security Smells for Microservices," *CLEI Eletronic J.*, vol. 27, no. 2, 2024, doi: 10.19153/cleiej.27.2.6.