Chapter 4:

Bibliometric Analysis of Cybersecurity Complexity in Cloud Computing

Emad Aliwa
İstanbul Topkapı University

doi: https://doi.org/10.66414/mls.978-1-0666009-1-5_4

Abstract

The growth and integration of cloud computing with other advanced technologies (such as Artificial Intelligence (AI) and other security technologies and architectures) have introduced different cybersecurity challenges and opportunities that require academic investigation. This research conducts a bibliometric analysis of 1,583 papers from Scopus database between 2010 to 2026 trying to address four main research aims: (1) publication growth and productivity, (2) active contributors in the field, (3) themes and evolution of cloud security, and (4) emerging and research directions. The findings reveal an exponential growth, with annual output rising from 3 papers in 2010 to 358 in 2025, highlighting an annual growth rate exceeding 30%. Keyword analysis also reveals technical security evolutions: from cloud architecture and basic security (2010–2015), through threat, privacy, risk and intelligent detection (2016–2020), to current state dominated AI-driven approaches and other cutting edge technologies such as blockchain, edge computing, quantum cryptography and decentralized security (2021–2026). The results also show increased security complexity due to the integration of advanced technologies and secure architectures with the cloud such as decentralized security (e.g. federated learning also known as distributed AI models), AI driven cybersecurity, zero-trust architectures, privacy-preserving computation and advanced cryptography such as post-quantum cryptography. These technologies are among the most challenging emerging research areas, yet they are the most promising regarding cloud computing. Finally, as cybersecurity technologies evolve, security complexity of the cloud will continue to grow.

Keywords: bibliometric analysis, cloud computing, cybersecurity complexity, cybersecurity evolution, artificial intelligence

1. Introduction

Cloud computing has changed the modern information technology, allowing access to resources including servers, storage, databases, and applications over the internet (Armbrust et al., 2010). This technology offers scalable, flexible, and cost-efficient service models, making it the backbone of digital transformation across different sectors such as healthcare, finance, government and education. According to a report, the global cloud computing market is expected to exceed $1 trillion in 2027 (Gartner, 2023). This shows its significant role in digital economy. However, the migration of business data and operations to cloud environments have created security challenges that demand review of the literature (Hussein, 2021).

Cybersecurity and cloud computing has emerged as important research field in information technology. The multi-tenancy model of cloud services (where multiple users share the same physical infrastructure) can create unique security risks that differ from traditional computing environments (Mell & Grance, 2011). For instance, data breaches, unauthorized access, service disruption, and insider threats represent some of the challenges that researchers and practitioners must address (Alouffi et al., 2021). Furthermore, the rapid evolution of cloud service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) presents distinct security considerations that require specialized research attention (Khoda Parast et al., 2022). The shared responsibility model in cloud computing also complicates the security responsibilities since both cloud service providers and cloud consumers must manage their security efforts to ensure comprehensive protection (Folorunso et al., 2024).

The literature on cybersecurity of cloud computing has grown gradually over the past decade, replicating the importance of this research area. Early studies focused primarily on identifying and classifying security vulnerabilities inherent in cloud service delivery models (Subashini & Kavitha, 2011; Tabrizchi & Kuchaki, 2020). Other researchers focus on addressing specific technical challenges, including data encryption, access

control mechanisms, intrusion detection systems, and secure computation protocols (Modi et al., 2013; Sun, 2020; Yang et al., 2020; Y. Zhang et al., 2020). More recently, the integration of cloud computing with emerging technologies such as the Internet of Things (IoT), edge computing, blockchain, and artificial intelligence has created new research directions that further increase cybersecurity challenges (Xu et al., 2022; Yang et al., 2020). Multi-cloud and hybrid cloud architectures (mixed environment of cloud and on premises computing) have added additional layers of complexity, requiring unique approaches to security management across hybrid environments (Tabrizchi & Kuchaki Rafsanjani, 2020; Zhang et al., 2020).

Despite the growth of the literature, there is a need for systematic mapping and analysis of this research field to identify research directions and challenges. Bibliometric analysis provides a quantitative methodology for mapping the structure of a research field to identify patterns of growth and knowledge gaps (Chen, 2017; Chen et al., 2023). While several previous studies have studied aspects of cloud computing security, few have provided a bibliometric analysis specifically focused on the complexity of cybersecurity in cloud environments using recent data. This chapter addresses this gap by performing a comprehensive bibliometric analysis of 1,583 publications extracted from Scopus database. This research is guided by the following four research questions:

RQ1: What is the volume and growth of research productivity in the field of cloud computing security?

RQ2: Who are the most productive and influential authors, sources, institutions, and countries, and what is the extent of collaboration in this field?

RQ3: What is the thematic structure of cloud computing security complexities, and how have research themes evolved over time?

RQ4: What are the currently emerging topics, how have the complexities of cloud security evolved, and what potential research trends do the data indicate?

Through bibliometric analysis of literature publications, this study aims to provide a data driven foundation for understanding the current state and future direction of cybersecurity research in cloud computing environments.

This chapter is organized in 7 sections as follows: Section1 provides introduction to this chapter. Section 2 illustrates the theoretical and conceptual background. Section 3 evaluates previous work and compares with this study. Section4 provides the methodology section. Section 5 and section 6 show data analysis, results and discussion. Finally, section 7 demonstrates conclusion and future research directions.

2. Theoretical and Conceptual Background

This section outlines the conceptual foundations across four interconnected domains; cloud computing security, cybersecurity complexity, cloud computing architectures, and emerging security technologies. Then, examines the relationships between these concepts. The aim is to establish a theoretical framework for interpreting bibliometric findings regarding research productivity, collaboration networks, thematic evolution and future research directions.

2.1. Cloud Computing Security

The National Institute of Standards and Technology (NIST) has formally defined cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (Mell & Grance, 2011). This definition highlights five essential characteristics; broad network access, rapid elasticity, measured service, on-demand self-service, and resource pooling. Each of these features carries direct security implications. Given that resources are pooled and accessed via public networks, the trust organizations traditionally placed in defenses are no longer valid (Subashini & Kavitha, 2011).

Subashini and Kavitha (2011) presented one of the first surveys of security issues across the three service delivery models, identifying data confidentiality, integrity, availability, and accountability as the four security pillars in cloud environments. Hashizume et al. (2013) further expanded this classification by identifying seven major threat categories namely; abuse of cloud services, insecure Application Programming Interface (APIs), malicious insiders, vulnerabilities in shared technologies, data loss or leakage, account or service hijacking, and unknown risk profiles. Each establishing differently across IaaS, PaaS, and SaaS deployment models. Subsequent studies confirmed the persistence of these threats and highlighted the expanded attack surface resulting from the uncontrolled nature of hypervisors, multi-tenancy, and the widespread integration of third-party services (Singh & Chatterjee, 2017).

Furthermore, cloud security is not merely a technical issue but also a governance challenge; the loss of physical control over infrastructure undermines traditional assurance mechanisms such as audits, digital forensics, and incident response (Jansen, 2011). A fundamental challenge identified in this literature is the need to balance the economic benefits of resource sharing against the requirements for protecting workloads that were not originally designed for shared infrastructure (Zhang et al., 2010).

2.2. Cybersecurity Complexity

Cybersecurity is defined as a complex socio-technical problem in which technological tools, human elements, organizational processes, and regulatory systems interact in non-linear and often unpredictable ways (Bodeau et al., 2011; Soomro et al., 2016). This complexity arises not only from the increasing sophisticated cyber-attacks methods but also from the diversity of systems requiring protection, the speed at which security vulnerabilities are discovered, and the costs of attacks versus defenses. Unlike physical security, cybersecurity requires defenders to maintain constant awareness of vulnerabilities across various attack surfaces, whereas attackers need to succeed only once (National Institute of Standards and Technology, 2018).

Bodeau et al. (2011) introduced the concept of cyber resilience to emphasize that prevention alone is insufficient, and organizations should assume that a breach will occur and design their systems to withstand, respond to, and recover from it. This perspective reframes security as an emergent property of system design rather than merely a checklist of controls. The NIST cybersecurity framework operationalizes this perspective through its five functions (Identify, Protect, Detect, Respond, and Recover) with each function addressing a different level of complexity (Barrett, 2018). The framework acknowledges that threats evolve faster than controls can be adopted and it prioritizes continuous improvement and risk-based decision making over static compliance.

Soomro et al. (2016) emphasized the human and managerial dimensions of this complexity, noting that the majority of security failures from inadequate training or governance gaps rather than technical vulnerabilities. The spread of regulation such as the EU's General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), and other sector specific national laws increase the issue. By fragmenting the compliance that cloud computing operators must navigate. Specifically, within the context of cloud computing, the stakeholders (providers, tenants, brokers, auditors, and regulators) creates interdependencies where in a single configuration error can spread across organizational boundaries (Hashizume et al., 2013).

2.3. Cloud Computing Architectures

Cloud computing architectures are traditionally classified into two dimensions: the service model and the deployment model. The service model dimension distinguishes between infrastructure as a service, platform as a service, and software as a service. Each defines a different level of abstraction through which the provider grants the customer access to resources (Mell & Grance, 2011; Zhang et al., 2010). The deployment model dimension distinguishes between public, private, and hybrid clouds, which differ based on the entity that owns, manages, and accesses the underlying infrastructure. Together, these dimensions form a design space

in which security responsibilities shift fundamentally: an IaaS customer retains control at the operating system level thereby bearing the bulk of the security burden whereas a SaaS customer delegates almost all security responsibilities to the provider, effectively inheriting the provider security posture (Rittinghouse & Ransome, 2010; Subashini & Kavitha, 2011).

Marston et al. in (2011) contextualized cloud computing architecture within the business, noting that the architectural choices made by organizations are driven less by technical efficiency than by cost, risk exposure, and the strategic value of the workloads being migrated. Wang et al. (2008) presented one of the earliest academic perspectives on cloud computing architecture, describing it as a combination of utility computing, distributed systems, and virtualization technologies. The virtualization layer typically implemented via hypervisors or container runtime environments is the architectural component that enables flexibility; however, it also represents the most critical attack surface as a single vulnerability in the hypervisor can compromise all virtual machines running on the host (Hashizume et al., 2013).

Modern cloud computing architectures have evolved from virtual machines to microservices, serverless functions, and container orchestration platforms such as Kubernetes. Shi et al. (2016), this architectural scope expanded to include the network edge, due to the rise of edge cloud computing architectures that place computing resources closer to data sources. This approach aims to reduce latency and bandwidth costs while raising new questions regarding physical security and trust. These architectural developments are not security neutral since each new layer of abstraction enhances the architectures of the cloud and also increases the number of components requiring hardening, monitoring, and updating thereby increasing the cybersecurity complexities.

2.4. Emerging Security Technologies

In response to architectural threats, a wave of emerging security technologies has surfaced, with machine learning and artificial intelligence gathering the most attention. Artificial intelligence and Machine Learning (ML) have emerged as security technologies for cloud environments, addressing the shortcomings of traditional, static, rule-based systems when facing dynamic attacks (Alzoubi et al., 2024). By leveraging automated pattern recognition, behavioral analytics, and predictive modeling, these technologies enhance capabilities for threat detection, access management, and security incident response across complex cloud architectures (Babaei et al., 2023).

Decentralized models are transforming how cloud computing models are trained, particularly through Federated Learning (FL); Algorithms are trained across edge devices and distributed servers without the need to transfer raw, private data to a central location (Albshaier et al., 2025; Devarapalem, 2025). Systematic reviews indicate that federated learning reduces privacy risks by 25% in sensitive domains and enhances threat detection capabilities by 40% within critical infrastructure, although 50% of implementation cases highlight challenges related to communication latency (Albshaier et al., 2025).

Despite this potential, several operational and technical vulnerabilities hinder the technology's widespread adoption. Susceptibility to adversarial machine learning attacks allows attackers to manipulate input data to poison training models or evade detection.

Furthermore, high computational overhead and latency make real-time model retraining a costly and resource-intensive process in multi-tenant systems (Sarraf & Pal, 2025). Furthermore, the lack of model interpretability and explainability undermines trust and the feasibility of regulatory auditing regarding automated cloud defense mechanisms (Alzoubi et al., 2024; Sarraf & Pal, 2025). Finally, data privacy requirements impose complexities on large scale training processes that necessitate massive behavioral datasets (Alzoubi et al., 2024).

Blockchain and distributed ledger technologies have been proposed as mechanisms to enhance the integrity, auditability, and decentralization of cloud computing security controls. A 2019 study examined the intersection of blockchain and artificial intelligence within cloud computing environments, identifying applications such as decentralized identity, tamper-resistant data logging, and verifiable computing (Salah et al., 2019). However, a study by Kolb et al. (2020) indicated that data transfer rates, latency, and energy consumption in public blockchains limit their applicability to specific scenario such as audit logs and supply chain tracking rather than general-purpose cloud computing security.

The Zero Trust architecture has emerged as a shift from a static based defense to the continuous verification of identity for every request. NIST Special Publication 800-207 established the Zero Trust concept as a set of logical components of policy engine, policy administrator, and policy enforcement point operating independently of network location (Rose et al., 2020). This model is highly suitable for cloud computing architectures, as it treats every interaction as untrusted, aligning naturally with the distributed and multi-tenant nature of cloud workloads.

Advancements in cryptography have led to the emergence of two additional sets of technologies. Fully homomorphic encryption enables computations to be performed on ciphertext without the need for decryption, promising the potential for fully confidential data processing on untrusted cloud infrastructure, although performance costs remain a barrier to widespread adoption (Armknecht et al., 2015). Post-quantum cryptography is being developed to handle the cryptographic breaches that large scale quantum computers will inflict upon encryption algorithms (Mosca, 2018).

2.5. Relationships Among the Main Concepts

The four concepts reviewed in this section are not independent research field rather, they form a tightly interconnected conceptual system. Cloud architectures define the structural attack surface: the choice of service model determines what the client can control, and the deployment

model choice determines which entities share the underlying infrastructure, while the architectural pattern (whether microservices, serverless, or edge computing) defines the pathways or touchpoints through which security vulnerabilities propagate. Cybersecurity complexity is a systemic condition arising from these architectural choices when exposed to diverse threat actors and varying regulatory frameworks; in other words, complexity is the product of architecture in the presence of adversaries.

Conversely, emerging security technologies represent responses developed by the research community to address specific facets of complexity within particular architectural configurations. The zero-trust principle emerged in response to the traditional network boundaries caused by cloud native architectures; "Confidential Computing" offers a solution to the inability of traditional encryption to protect data during processing; and machine learning-based detection technologies handle vast amounts of telemetry data that exceed human analytical capacity. Blockchain technology addresses the trust gaps among multiple parties that arise when cloud services are deployed across different organizations (Rose et al., 2020; Tabrizchi & Kuchaki Rafsanjani, 2020). However, each emerging technology brings its own new complexities. Machine learning models are vulnerable to attacks via adversarial examples and data poisoning. Isolated confidential computing environments remain susceptible to side-channel attacks. Blockchains present challenges regarding key management and scalability and the transition to quantum-resistant encryption systems (post-quantum migration) requires comprehensive coordination across entire cryptographic ecosystems (Buczak & Guven, 2016; Mosca, 2018). These defensive technologies become sources of new risks is precisely why bibliometric studies treat cloud computing security as an evolving, ongoing issue rather than a definitively resolved one.

3. Related Work

The evolution of cloud computing highlights a shift from traditional infrastructure concerns to multi-dimensional security challenges (Abdulle et al., 2026; Cai et al., 2015). Early bibliometric assessments identified security as active research area along with virtualization and distributed computing (Cai et al., 2015). Later analyses observing an average 15% annual increase in publications related to cloud security between 2010 and 2018 (Thiam et al., 2019). Despite this growth, recent studies indicate a persistent gap between published research and real-world challenges as nine out of ten security professionals are concerned about cloud security (Garg et al., 2019).

Recent research has increasingly focused on the role of advanced computational techniques (such as AI based detection and prevention techniques) in managing cloud threats and its architecture complexity (Alzoubi et al., 2024). Several studies have identified 2018 as a key year where AI cybersecurity research accelerated due to the availability of deep learning frameworks and datasets (Chuang & Chuang, 2026). Machine learning and deep learning models have also shown major effect in identifying and mitigating cloud security threats through anomaly detection and prevention systems and security automation (Alzoubi et al., 2024).

Beyond technical detection, some scholars have also examined specific security mechanisms and their socio-economic effects (Abdulle et al., 2026; Reddy et al., 2026). Scient metric analyses targeting access control and encryption techniques reveal research clusters in federated learning and post-quantum cryptography (Dayyabu et al., 2020). From an economic point of view, security is no longer just a technical requirement but a major cost factor effecting organizational adoption and investment decisions (Abdulle et al., 2026).

However, the complexity of cloud architecture introduces unique threats and uncertainties. Risks and uncertainties arise from supply chain stability such as outsourcing and vendor maturity, noting that the

complexity of interconnected systems of systems significantly increases the possibility of failure (Zied Milian et al., 2017). Cloud native systems (composed of containers and microservices communicating through distributed networks) present complex security risks that conventional countermeasures struggle to monitor (Chuang & Chuang, 2026). This complexity is further expanded by IoT devices integration which significantly increases the attack surface (Garg et al., 2019; Thiam et al., 2019).

While existing bibliometric studies have provided valuable overviews, the present study addresses this gap by studying cybersecurity complexity inherent in modern cloud environments. While existing sources provide high-level scientific mapping of the field, the present study addresses this gap by examining how cybersecurity complexity has evolved and how it creates a level of complexity that traditional defense mechanisms struggle to mitigate. Table 1 provides a comparison with related previous studies in the literature.

Table 1. A comparison with related previous studies in the literature

Paper	Focus Area	Methodology	Key Findings	Complexity Outlook
Abdulle et al., 2026	Cost-Benefit Analysis (CBA)	Bibliometric (Scopus)	Security is considered an emerging cost factor when adopting cloud computing.	Complexity arises from new cloud models like edge and serverless.
Alzoubi et al., 2024	ML & DL for cloud security	Bibliometric (Scopus)	Focus on anomaly detection, automation, and privacy.	Security addressed through neural network architectures
Thiam et al., 2019	Rise of cloud security (2010-2018)	Bibliometric (WoS)	15% annual growth; China, India, USA are top contributors.	Complexity mentioned regarding IoT and increased attack surfaces.
Cai et al., 2015	General cloud computing	Bibliometric (SCI-E, etc.)	Security is a top 5 research topic; mobile cloud is a future hotspot.	Identifies non-functional complexity: elasticity and adaptability.
Chuang & Chuang, 2026	Global cyber-attack trends	Bibliometric	Shift from reactive proactive AI-driven counter measues.	Cybersecurity is an interdisciplinary challenge with legal angles.
Dayyabu et al., 2020	Cloud security research	Bibliometric (Scopus)	IaaS is the most researched model; access control is a major gap.	Complexity in multi-tenancy and virtualization nature.

Garg et al., 2019	Emerging security trends	Bibliometric (Scopus)	Gap between research and industry.	Complexity in trust management and IoT integration.
Judijanto & Vandika, 2026	Cloud-native security	Bibliometric	Move toward DevSecOps, Kubernetes, and AI-driven models.	Complexity in temporary containers and distributed networks.
Reddy et al., 2026	Access control & encryption	Scientometric	blockchain security and post-quantum cryptography trends.	Fragmentation between technical factors and legal frameworks.
Zied Milian et al., 2017	Risks and uncertainties	Systematic review	Risks originate from vendor maturity and supply chain deliveries.	Addresses complexity of systems of systems'.
This study	Cybersecurity complexity and emerging research area	Bibliometric analysis (Scopus)	Analyzes the complex technological advancement	Complexity as the primary driver of modern vulnerabilities.

4. Research Methodology

4.1 Data Collection and Search Strategy

The data in this bibliometric analysis was extracted from Scopus database, which is one of the largest databases of peer-reviewed papers. The search query was designed to capture publications of cybersecurity and cloud computing. The search was conducted in August 2026, and the results were limited to English-language documents published between 2010 and 2026 to maintain consistency and relevance. The initial search generated a comprehensive set of papers, which was refined through a systematic filtering process (highlighted in figure1) to ensure the relevance and quality of the dataset.

The inclusion criteria required that papers be indexed in Scopus, published between 2010 and August 2026 (10 of August 2026 date of extracting the dataset which reflect almost 3 quarters of the year), written in English, and directly address topics related to cybersecurity in cloud computing. Both peer reviewed research articles and review papers were included to cover the literature. Conference papers, book chapters, and other non-journal document types were excluded to maintain consistency.

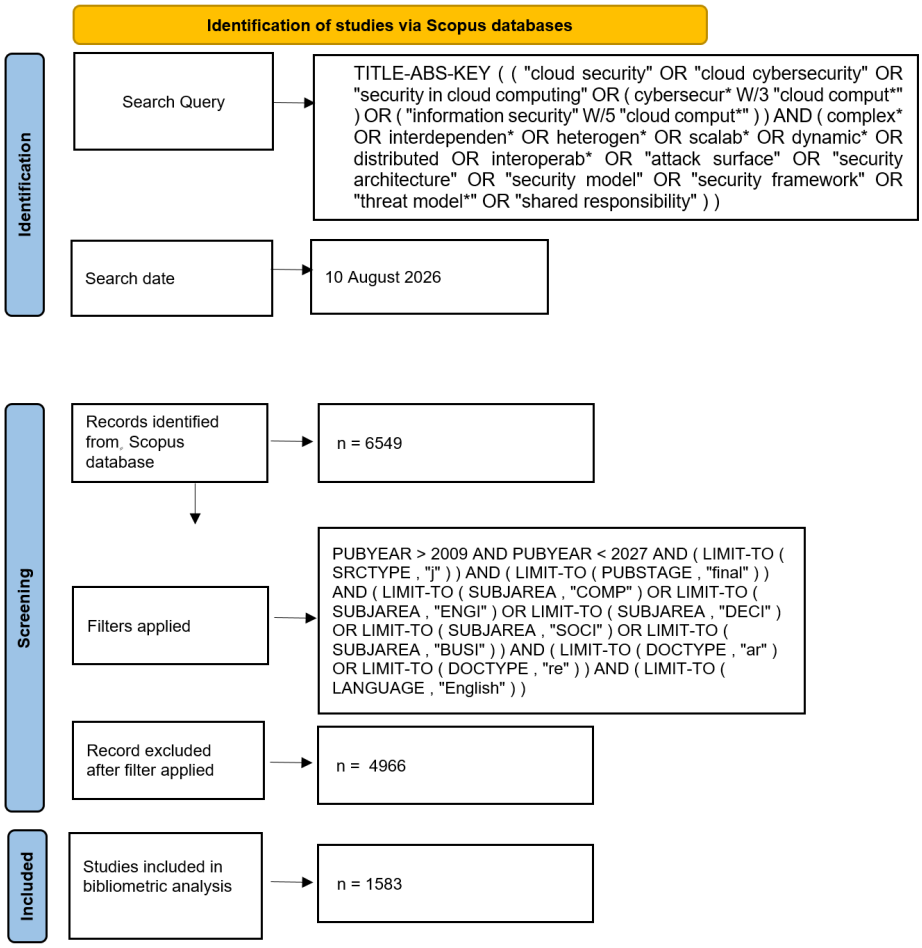


Figure 1. Search query, filtering, inclusion and exclusion mechanism

The final dataset (as shown in figure 2) includes 1,583 publications, including 1,488 research articles (94.0%) and 95 review papers (6.0%). This database provides a solid basis for performing bibliometric analysis that reflects the progress of research in this field.

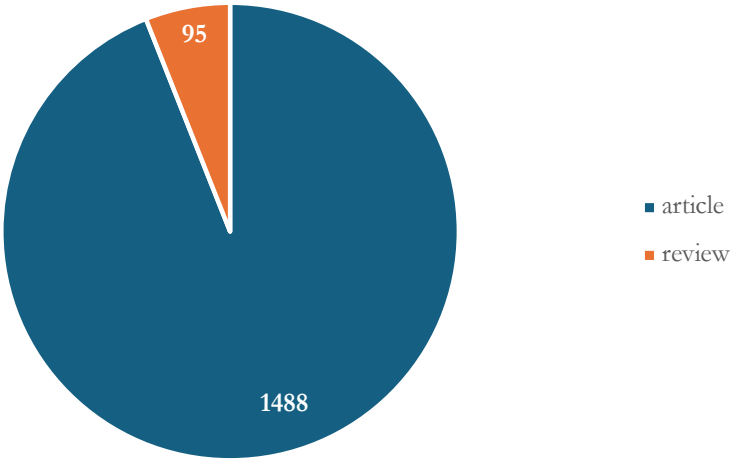


Figure 2. Distribution of papers containing 1,488 articles and 95 review papers

4.2. Analytical Framework

The bibliometric analysis was conducted using an analytical framework that included seven key dimensions:

1. Time-based publication trends analysis to identify growth patterns including calculating Compound Annual Growth Rates (CAGR).
2. Journal productivity analysis and Bradford's Law assessment to evaluate primary publisher and literature spreading across journals.
3. Author productivity analysis and Lotka's Law examination to understand the distribution of scientific output among researchers.
4. Geographical distribution analysis to map the global research at country and institutional levels.
5. Citation analysis, including total citations, average citations per paper, h-index calculation, and identification of the most cited papers.
6. Keyword frequency analysis, co-occurrence mapping, and tracking temporal subject development across three time periods.
7. International research collaboration analysis by creating a country-level collaboration heat map.

The graphs were created using Biblioshiny and Microsoft Excel to produce the results of various graphical formats, such as bar charts, pie charts, and heat maps. All data processing and analysis were performed using Bibliomtrix (Biblioshiny package within RStudio version 2026.05.1, build 225) to ensure reproducibility and minimize human error. Furthermore, the research based on questions ensures that each part of the analysis directly addresses one or more of the four research questions guiding this study.

5. Results and Analysis

5.1 Publication Volume and Growth Dynamics (RQ1)

The distribution of publications provides a comprehensive overview of the research progress and maturity of the field. As illustrated in Figure 3 and Table 2, the annual output of papers shows a sustained upward trend from 2010 to 2026. The earliest publications in the dataset date back to 2010, with only three publications recorded that year, reflecting the field's initial phase. This period coincides with the publication of the NIST definition of cloud computing, which provides a standardized framework for both industrial adoption and academic research. The field experienced a significant turning point between 2014 and 2015, with annual output increasing from 24 publications in 2014 to 43 in 2015, representing a yearly growth of 79.2%, indicating the beginning of academic interest in cloud computing security.

In 2015, this field experienced rapid growth. Annual output rose from 50 publications in 2016 to 96 in 2019, before temporarily declining to 73 in 2020. The post pandemic recovery was remarkably strong, with output increasing from 78 publications in 2021 to 156 in 2022 (a 100% increase) representing the largest year growth in the data. Growth then accelerated to 212 publications in 2024 and 358 in 2025. 2026 so far shows 202 publications, and this number is expected to rise as more papers are indexed. The line in Figure 3 highlights a steady growth of this field.

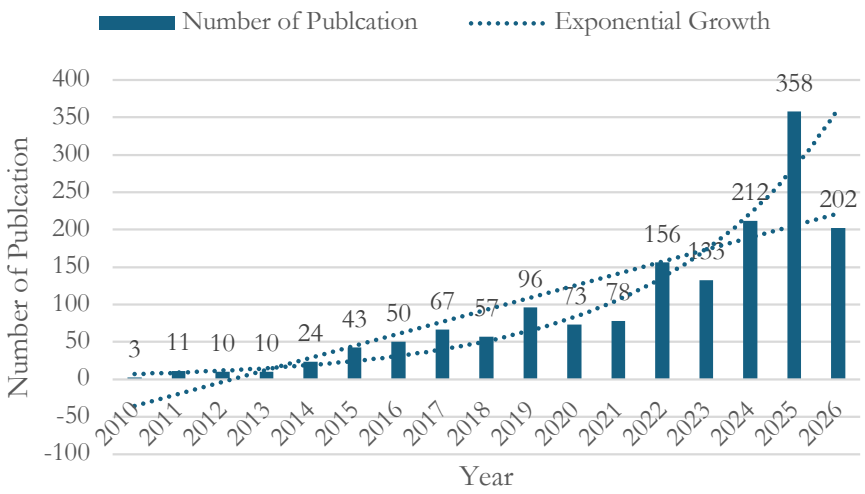


Figure 3. Annual publication trend in cloud computing cybersecurity research (2010-2026), shows steady exponential growth with a polynomial trend

Table 2. Annual distribution of publications in the field of cybersecurity for cloud computing (2010-2026)

Year	Publications	Percentage
2010	3	0.19%
2011	11	0.69%
2012	10	0.63%
2013	10	0.63%
2014	24	1.52%
2015	43	2.72%
2016	50	3.16%
2017	67	4.23%
2018	57	3.60%
2019	96	6.06%
2020	73	4.61%
2021	78	4.93%
2022	156	9.85%
2023	133	8.40%
2024	212	13.39%
2025	358	22.62%
2026	202	12.76%
Total	1,583	100.00%

5.2. Most Productive and Impactful Sources (RQ2)

Journal productivity analysis reveals the key publishing platforms shaping the cloud computing cybersecurity. As illustrated in Figure 4 and Table 3, Institute of Electrical and Electronics Engineers (IEEE Access) dominates with 74 publications (4.67% of total output), followed by Cluster Computing (38 publications, 2.40%), IEEE Transactions on Cloud Computing (37 publications, 2.34%), IEEE Transactions on Dependable and Secure Computing (32 publications, 2.02%) and the International Journal of Advanced Computer Science and Applications (30 publications, 1.90%). These five journals collectively account for 211 publications (13.33% of the total), indicating a medium level of focus on this field.

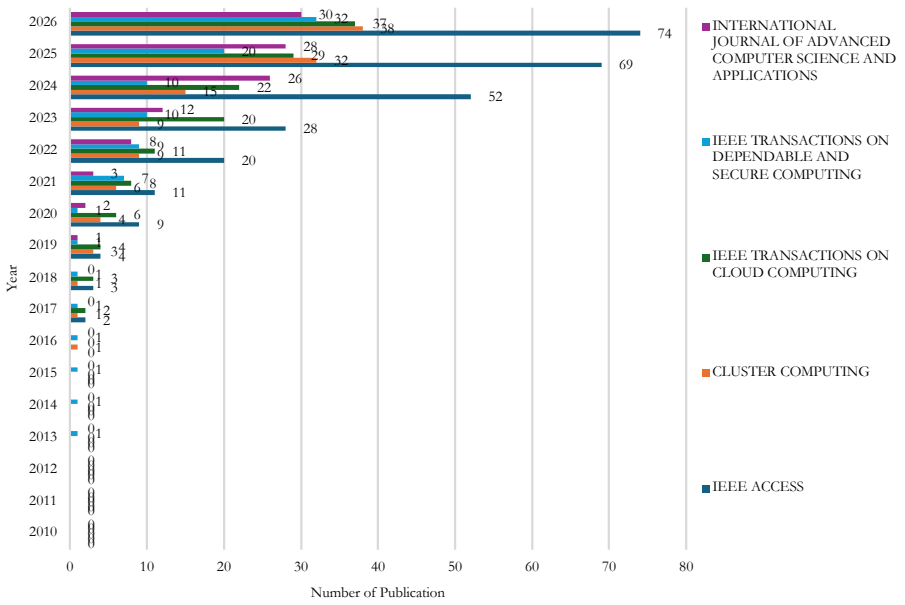


Figure 4. Productive journals in the field of cybersecurity research for cloud computing

Table 3. Top 15 journals in terms of productivity, number of publications, and citation impact

Rank	Journal	Papers	Total Cit.
1	IEEE Access	74	1,755
2	Cluster Computing	38	633
3	IEEE Trans. Cloud Computing	37	796
4	IEEE Trans. Dependable and Secure Computing	32	652
5	Int'l J. Adv. Comput. Sci. Appl.	30	N/A
6	Journal of Cloud Computing	28	801
7	J. Theoretical and Applied Info. Tech.	27	N/A
8	Computers and Security	25	N/A
9	IEEE Trans. Info. Forensics and Security	22	N/A
10	IEEE Trans. Services Computing	21	731
11	Future Generation Computer Systems	20	827
12	IEEE Internet of Things Journal	19	527
13	Applied Sciences (Switzerland)	19	N/A
14	Computers, Materials and Continua	18	N/A
15	Sensors	18	541

Analyzing the journal distribution using Bradford law (Brookes, 1985) reveals a three-region structure. As shown in figure 5, region 1 (the core) comprises 22 journals that contributed approximately 533 articles (one-third of the total), while region 2 contains 86 journals that contributed an additional 528 articles, and region 3 consists of 372 that contributed the remaining 522 articles. Bradford multiplier of 4.12 is slightly higher than the theoretical value of approximately 3.0, representing a moderate concentration of publications in the core journals. This distribution pattern is consistent with a stable publishing environment and a mature research field.

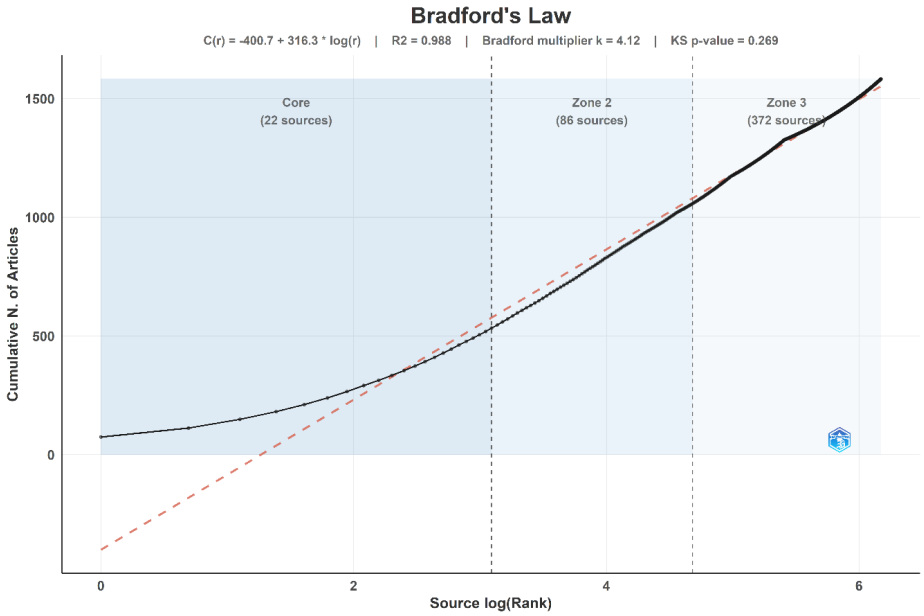


Figure 5. Core sources by Bradford's law

When considering the impact of citations rather than simply the volume of publications, the ranking changes significantly, as illustrated in figure 6. The journal Network and Computer Applications in the top of the list with a total of 3,087 citations from just 13 papers (an average of 237.5 citations per paper), followed by IEEE Access with 1,755 citations, then IEEE Communications Surveys and Tutorials (1,030 citations from 3 papers, an average of 343.3 citations per paper), and finally Future Generation Computer Systems (827 citations from 20 papers). Journal IEICE Transactions on Communications contributed a single paper that gathered 701 citations, demonstrating how a highly piece of work can significantly increase a journal citation count. These findings confirm the importance of considering quantitative and qualitative indicators when evaluating the publishing environment within a research field.

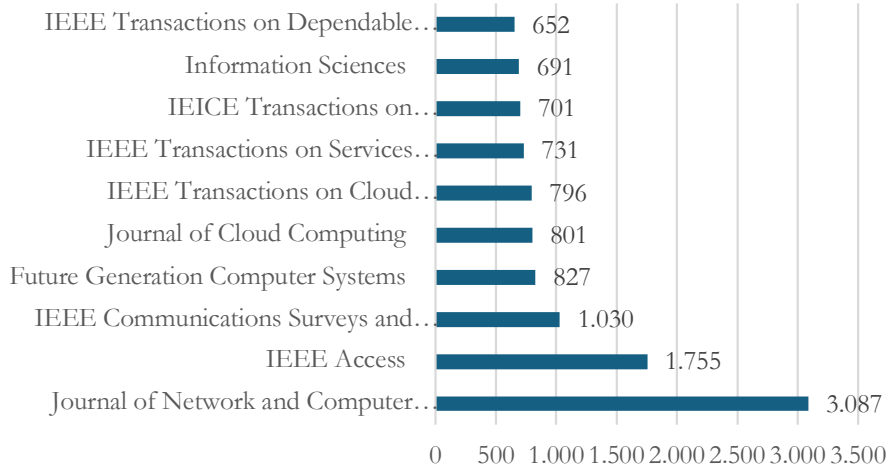


Figure 6. The top 10 journals ranked by total citations

5.3. Productive and Impactful Authors and Institutions (RQ2)

Analysis of author productivity reveals a highly skewed distribution consistent with Lotka's law of scientific productivity, which states that a small number of authors produce the majority of publications (Lotka, 1926). The most common authors in the dataset are from India and China origin based on the affiliation data, reflecting the geographic distribution of research output. Although the difference is small, the data show that the most common author country origin collectively represents a significant portion of total published output, with a steady research activity spanning 8 to 15 years. This pattern suggests the presence of specialized research groups and a long-term scientific commitment to this domain knowledge. As shown in figure 7 the distribution of productivity among authors follows an inverse squared approximation consistent with Lotka's classical formulation, where the number of authors publishing n papers is approximately proportional to $1/n^2$.

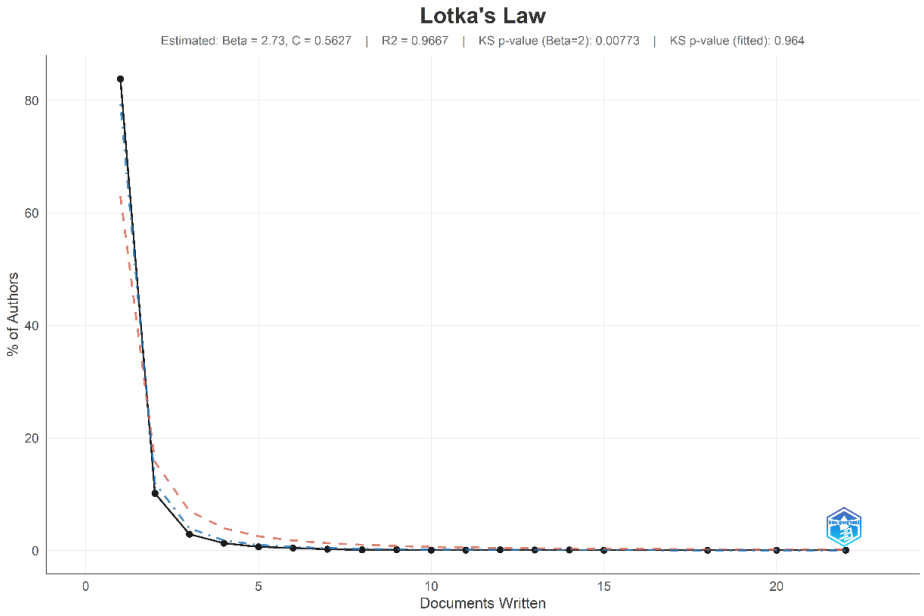


Figure 7. Author Productivity through Lotka's Law

The institutional analysis, illustrated in figure 8, shows that the most productive partnerships are mainly with Indian and Chinese universities. India's National Institutes of Technology (NIT) system leads the list with 35 partnerships, followed by Vellore Institute of Technology (25), Beijing University of Posts and Telecommunications (22), Xi'an Electronic University (22), and Anna University (22). These five institutions collectively form 126 partnerships, reflecting the concentration of research investment in cloud computing security at these universities. The strong performance of Indian institutions aligns with India's position as a leading data producer. Notably, King Abdulaziz University of Saudi Arabia appears among the top institutions, reflecting the Kingdom's increasing investment in cybersecurity research. The presence of Nanyang Technological University (Singapore) and the University of Melbourne (Australia) in the top 15 also demonstrates the research contributions of high-quality institutions outside the dominant India-China association. In terms of productive authors in the literature, figure 9 shows the top 10 most productive authors.

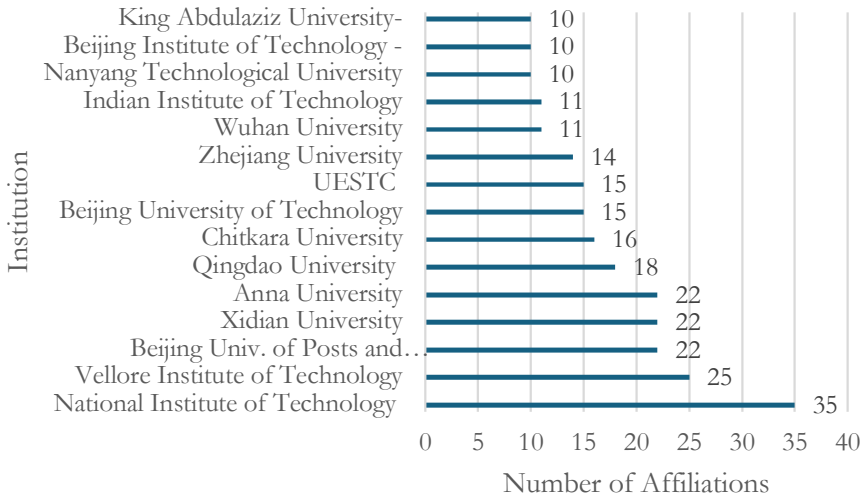


Figure 8. Top 15 productive institutions contributing to this field

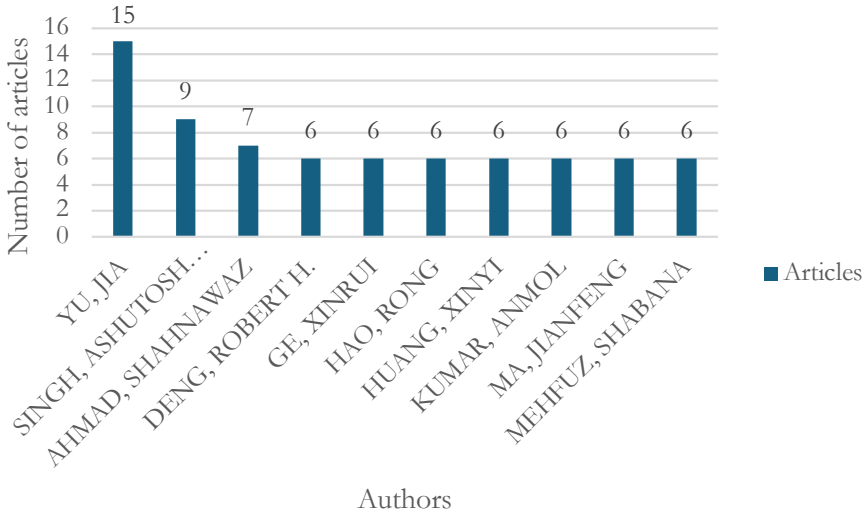


Figure 9. Most productive author

5.4. Geographic Distribution of Research (RQ2)

The geographical distribution of research production (as illustrated in figure 10) reveals a global concentration dominated by Asian countries. India leads the field with 619 affiliations (representing the largest share of total output), followed by China with 397. Together, these two countries account for over 64% of global research productivity in cloud computing

cybersecurity. This reflects their investments in higher education research, government funding, and rapid digital transformation of the economies. The US ranks third with 149 affiliations, followed by Saudi Arabia 130, the UK 87, Australia 66, and South Korea 53 affiliations.

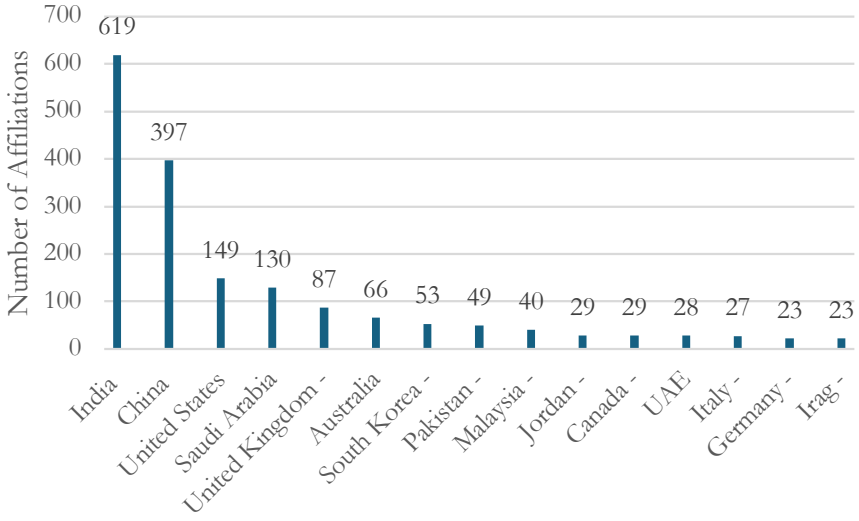


Figure 10. The top 15 countries/regions in terms of their affiliations in the field of cyber knowledge for cloud computing

The dominance of India and China can be accredited to several factors. First, both countries have implemented national strategies for cloud computing and cybersecurity, stimulating academic research in these areas. The cybersecurity policy of India and cybersecurity law of China have contributed to forming regulatory frameworks that demand more cybersecurity research (Mukhopadhyay, 2022; Sevenard, 2026). Second, the rapid growth of their IT sectors and the increasing adoption of cloud computing services across all sectors may have created strong demand for cybersecurity research. Third, both countries have large academic communities with a strong publishing culture, and their researchers regularly publish in open-access journals and IEEE journals that dominate the field (Feng & Garg, 2021). Saudi Arabia presence among the top five reflects its Vision 2030 program, which has funded numerous cybersecurity research centers and international joint ventures (Hussain, 2026). The low representation of African and Latin American countries

might indicate potential gaps in global research capabilities in cybersecurity, which requires attention.

5.5. Citation Analysis and Scholarly Impact (RQ2)

Citation analysis provides a quantitative measure of the scientific influence of research productions in specific field. The dataset accumulated 29,322 citations (average 18.52 citations per publication) with a median of 4.0 citations. The h-index for the dataset was 76, meaning that 76 research papers each received at least 76 citations. This significant value places the research area among the most influential in computer science. While this index is lower than those of more established fields, it is still notable given the field's relatively progressing.

As illustrated in Figure 11, the distribution of citations follows a highly skewed pattern which is common pattern in scientific literature. 333 publications (21.04%) remained uncited which is a moderate percentage compared to broader scientific fields. suggest that research in this area tends to gain traction over time. The largest group, (comprising 540 publications (34.11%) each received between one and five citations, followed by 243 publications (15.35%) with between 11 and 25 citations. Notably, 45 publications (2.84%) composed over 100 citations each which represents the highly influential core of the field. Only one publication exceeded 1,000 citations, highlighting the field reliance on a limited number of works that shaped its theoretical foundations.

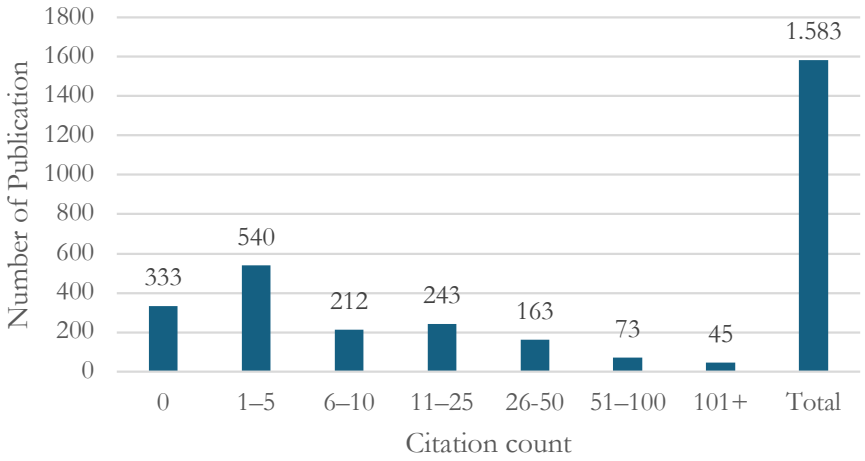


Figure 11. The distribution of publications by number of citations

The most cited study in the dataset shown in figure 12 and table 4 is Subashini and Kavitha's 2011 influential study on security issues in cloud computing service delivery models (Subashini & Kavitha, 2011). The paper collected 2,138 citations and is considered as a foundational reference in the field. This is followed by Stoyanova et al.'s comprehensive 2020 study on IoT forensics, which received 797 citations (Stoyanova et al., 2020). Fu et al.'s influential 2015 study on achieving effective cloud search services (Fu et al., 2015) received 701 citations. These highly cited studies represent the theoretical foundations which much of the subsequent research addressing fundamental challenges in cloud security such as IoT integration privacy preserving and cryptography. The range of publisher presenting the most cited papers such as ACM to IEEE and Elsevier publications giving the indication that influential publication is spread across the publishing environment rather than concentrated in a single publisher.

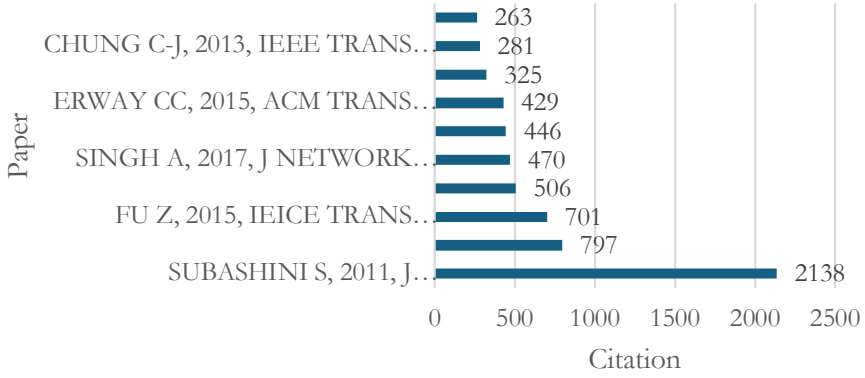


Figure 12. Most cited research papers in the dataset with authors and year, which represent foundational and highly influential works

Table 4. Most cited research papers in the dataset, which represent foundational and highly influential works

Paper	Total Citations
SUBASHINI S, 2011, J NETWORK COMPUT APPL	2138
STOYANOVA M, 2020, IEEE COMMUN SURV TUTOR	797
FU Z, 2015, IEICE TRANS COMMUN	701
ZHAO C, 2019, INF SCI	506
SINGH A, 2017, J NETWORK COMPUT APPL	470
YANG H, 2019, IISE TRANS	446
ERWAY CC, 2015, ACM TRANS INF SYST SECUR	429
BAUMANN A, 2015, ACM TRANS COMPUT SYST	325
CHUNG C-J, 2013, IEEE TRANS DEPENDABLE SECURE COMPUT	281
SHIRAZI SN, 2017, IEEE J SEL AREAS COMMUN	263

5.6 Thematic Structure and Evolution (RQ3)

Keyword analysis provides authors with a frame into the field structure and evolution. As illustrated in Figure 13, Figure 14, Figure 15 and Table 5, the most frequent occurring keywords are: cloud computing security (524 times), cloud computing (501 times), security (153 times), blockchain technology (77 times), machine learning (68 times), data security (67 times), cloud storage (59 times), encryption (57 times), and deep learning (57 times). The close alignment of cloud computing security and cloud computing as the two most common keywords highlights that this dataset effectively covers the intersection of these two fields. The

strong presence of blockchain technology, machine learning, and deep learning among the most frequent keywords also indicates the growing combination of emerging technologies with cloud computing security research.

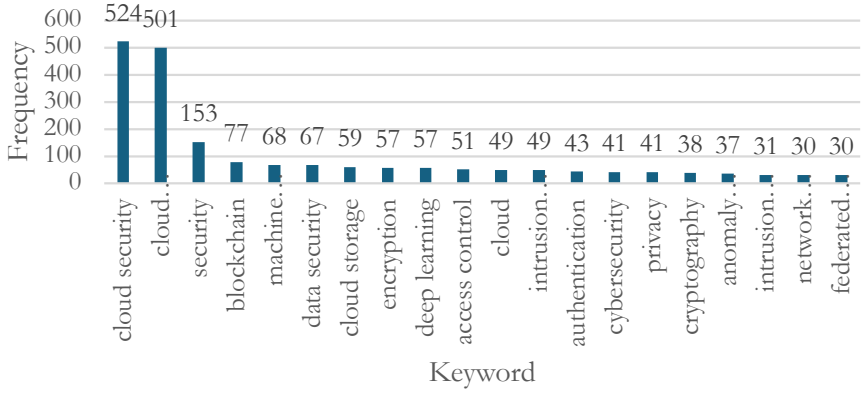


Figure 13. Top 20 author keywords, illustrating the thematic composition and research priorities within the field

Table 5. Author keywords ranked by frequency of occurrence

Rank	Keyword	Freq.
1	cloud security	524
2	cloud computing	501
3	security	153
4	blockchain	77
5	machine learning	68
6	data security	67
7	cloud storage	59
8	encryption	57
9	deep learning	57
10	access control	51
11	cloud	49
12	intrusion detection	49
13	authentication	43
14	cybersecurity	41
15	privacy	41
16	cryptography	38
17	anomaly detection	37
18	intrusion detection system	31
19	network security	30
20	federated learning	30

Keyword analysis reveals a clear three-stage thematic evolution, as illustrated in Figure 14. In the foundational stage (2010–2015), research focused mainly on core cloud computing security concepts, with prominent keywords such as cloud computing (56 times), cloud computing security (44 times), and security (12 times). This period was categorized by concentrated efforts to identify and address the fundamental security vulnerabilities in cloud computing service delivery models. The emergence of virtualization and SaaS models as top keywords reflects the technical focus of this early period.

The evolution stage (2016–2020) saw a widen of the research topics, with cloud computing security (216 times) and cloud computing (169 times) remaining dominant. Emerged topics such encryption (22 times), Distributed Denial-of-Service (DDoS) attacks (11 times), cloud storage (15 times), and privacy (11 times). The emergence of distributed denial-of-service attacks as a key term reflects growing concerns about these attacks targeting cloud infrastructure. The rise of privacy concerns also indicates a growing awareness of data protection challenges. This phase occurred with the rapid increase of cloud computing services across different sectors, accompanied by an expansion in the scope of threats.

The final phase (2021-2026) is categorized by the significant rise of AI-powered security and blockchain technology. The use of blockchain term increased 77 times while machine learning 68 times, deep learning 57 times, and federated learning 30 times. This phase represents a major shift toward intelligent, data driven security solutions that utilize advanced computing technologies. For example, utilization of AI models for detection, prevention, and response countermeasures to sophisticated cyber threats. Analysis of co-occurrence reveals strong thematic links, with the most prominent keyword pairs being cloud computing - cloud computing security (118 times), cloud computing - security (76 times), cloud computing - data security (34 times), and cloud computing security - machine learning (28 times), indicating the emergence of integrated research of multiple technology fields.

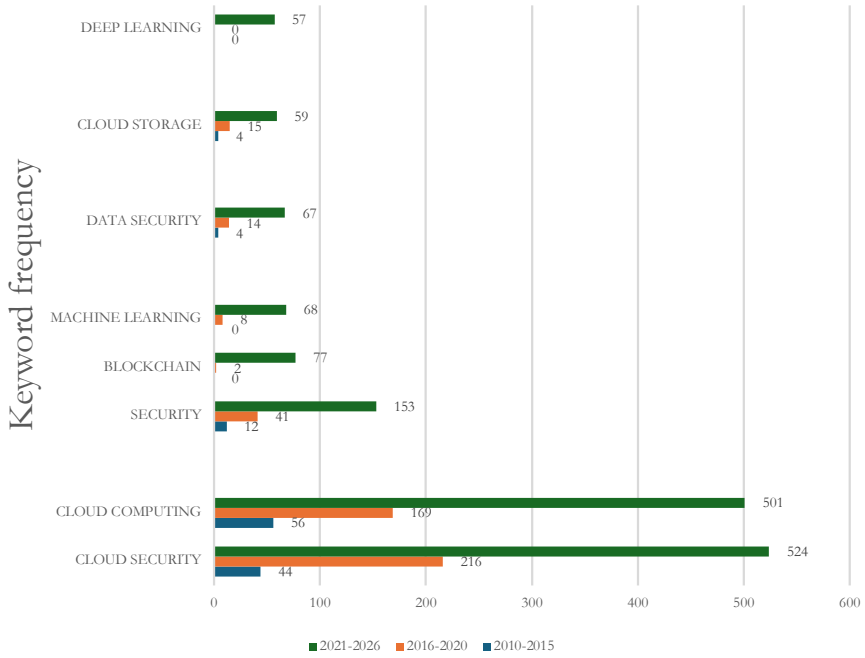


Figure 14. Thematic evolution of research keywords across three time periods (2010–2015, 2016–2020, 2021–2026).

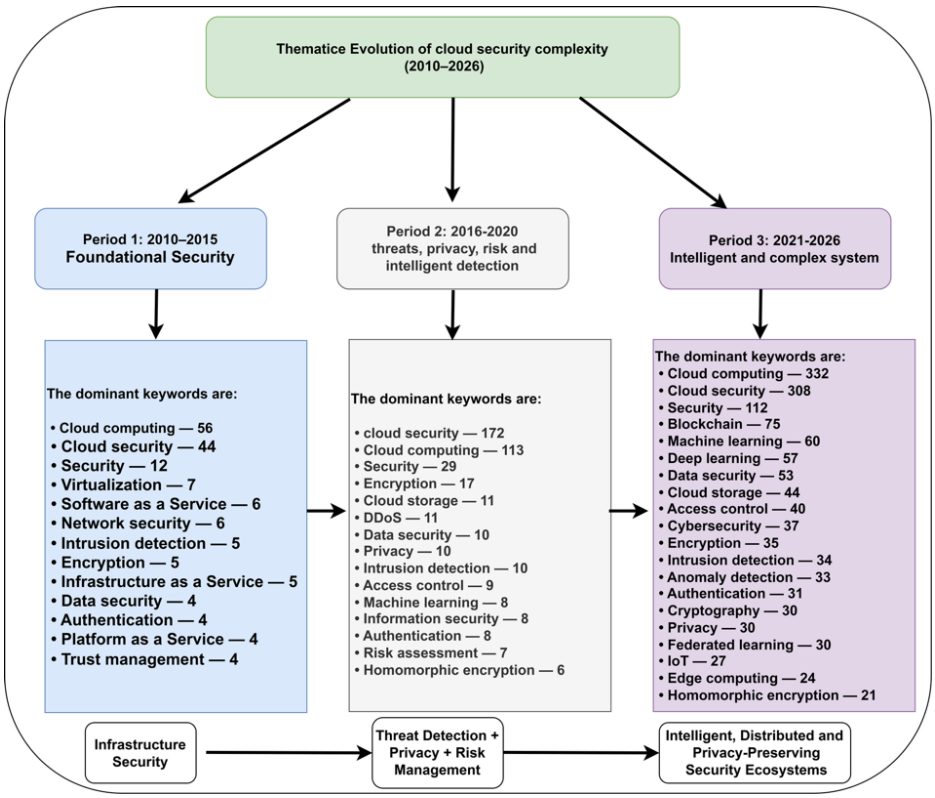


Figure 15. Thematic evolution of cloud security complexity and dominant keywords for each period

5.7. International Research Collaboration (RQ4)

The analysis of international research collaboration patterns provides insights into the global knowledge exchange network within this field. Among the 1,583 papers analyzed, 424 (26.84%) involved international collaborations between scholars from two or more countries whereas 1,156 publications (73.16%) originated from a single country. 3 records had no identified country in affiliation field. This suggests that while majority of research is conducted within national borders, a significant and growing percentage involves cross border partnerships. The relatively moderate rate of collaboration also indicates that this field has not yet reached the level of internationalization seen in more mature research areas, such as climate science, where international partnerships rates typically exceed 40%.

The heatmap in Table 6 illustrates the density and structure of international research cooperation among the ten most productive countries. The strongest collaborative links are between China and the United States (33 joint publications), Saudi Arabia and India (23), China and Australia (26), Saudi Arabia and Pakistan (19), and China and the United Kingdom (16). China's central position in the collaborative network reflects its dual role as a major producer of research and an active partner with institutions in Asia, North America, Europe. The strong links between Saudi Arabia and Pakistan, and between Saudi Arabia and India reflect Saudi Arabia's active investment in international research cooperation, particularly through scholarship programs that attract researchers from South Asian countries (Polizzi, 2026). The China-US collaboration is particularly important, bringing together the two largest economies and their strengths in cloud computing and cybersecurity research.

Table 6. Heat map of international cooperation showing the frequency of joint publications among the ten most productive countries

	China	**Saudi Arabia**	**India**	**USA**	**UK**	**Australia**	**Pakistan**	**Malaysia**	**UAE**	**Jordan**
China	0	16	14	33	16	26	11	6	2	2
Saudi Arabia	16	0	23	10	15	4	19	9	8	11
India	14	23	0	13	10	7	3	9	2	2
USA	33	10	13	0	6	3	2	4	4	1
United Kingdom	16	15	10	6	0	9	7	4	2	3
Australia	26	4	7	3	9	0	1	0	2	2
Pakistan	11	19	3	2	7	1	0	7	6	2
Malaysia	6	9	9	4	4	0	7	0	1	0
UAE	2	8	2	4	2	2	6	1	0	4
Jordan	2	11	2	1	3	2	2	0	4	0

The publisher analysis, shown in Figure 16, reveals the dominance of the IEEE institution in the publishing market with 290 publications, followed by Springer (211), Elsevier (184), and finally MDPI (100). IEEE dominance aligns with the field's strong focus on engineering and applied computer science. The combined output of the top five publishers

represents over 40% of total production, indicating a medium level of publisher focus. MDPI's presence reflects growing trend toward open access publishing which impacts the accessibility of research findings.

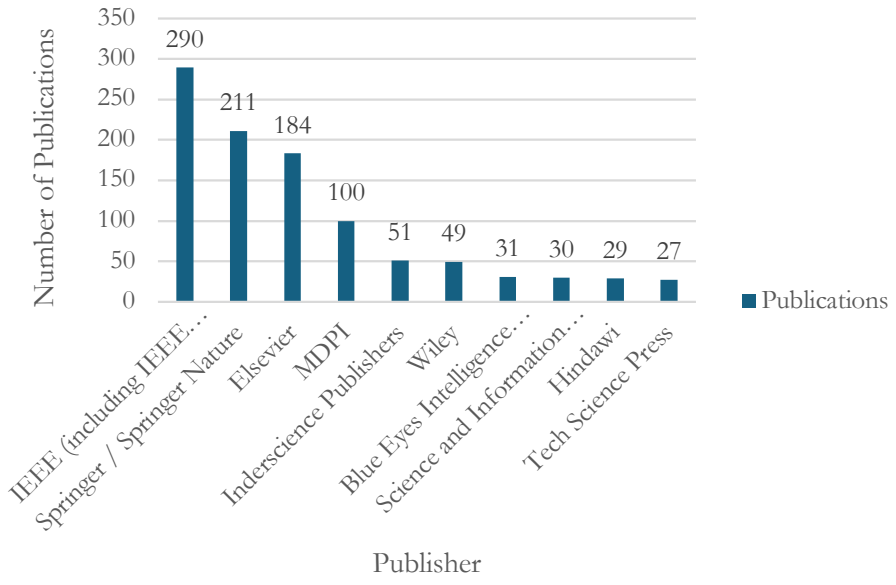


Figure 16. The top 10 publishers by publication volume, demonstrating the dominance of IEEE and Springer in this research field

6. Discussion

6.1. Analysis of Key Findings

The discussion chapter evaluates the growth, intellectual structure, and thematic shifts in research concerning the complexities of cloud cybersecurity between 2010 and 2026. It highlights the evolution of cloud security from isolated perimeter defenses to a systemic challenge embedded within dynamic, multi-cloud, and containerized systems of systems. Key findings include:

1. **Exponential growth in publications**: Research output expanded from three papers in 2010 to 358 in 2025 (a compound annual growth rate exceeding 30%), driven by the integration of artificial intelligence and the adoption of cloud native architectures.

2. **Geographic volume versus impact**: India and China account for over 64% of total publications, whereas Western institutions (USA, Canada, UK, and Australia) maintain higher citation rates and greater centrality within the research collaboration network.
3. **Citation distribution**: The dataset demonstrates strong cumulative impact (H-index of 76; 29,322 citations) but also reveals 21.04% of papers remaining uncited (median = 4.0 citations).
4. **Thematic Evolution**: Research has progressed through three distinct phases: the foundational phase focusing on service models such as IaaS and virtualization (2010–2015). The phase centered on cryptography-based access and data privacy (2016–2020). Finally, the phase involving AI-driven threat detecting and preventing, the zero trust model, and cloud native methodologies (2021–2026).

6.2. Comparative Summary of Related Work

1. **Publication Growth:** Points of convergence: The exponential rise noted in this study aligns with broader trends in research literature documenting sustained growth in cloud security research (Cai et al., 2015; Dayyabu et al., 2020; Garg et al., 2019; Thiam et al., 2019). Divergence: While early foundational studies recorded moderate annual growth rates of approximately 15% (Thiam et al., 2019), recent specialized analyses indicate accelerated growth exceeding 30–36% annually affected by the adoption of deep learning technologies after 2016 (Alzoubi et al., 2024), the rise in artificial intelligence research after 2018 (Chuang & Chuang, 2026), and research on access control after 2020 (Reddy et al., 2026).
2. **Geographic Output and Impact:** Dominance in volume: All studies confirm that China and India lead in the volume of global publications regarding cloud security (Dayyabu et al., 2020; Garg et al., 2019; Thiam et al., 2019), particularly in the fields of machine learning (India) and deep learning (China) (Alzoubi et al., 2024; Reddy et al., 2026).

3. **Evolution of the Concept of Complexity:** Phase One (1) (Foundational): Early research focused on the isolation of static virtual machines within service models and the risks associated with hypervisors (Cai et al., 2015; Dayyabu et al., 2020). Phase Two (2) (Expansion): The focus shifted toward searchable encryption, Attribute-Based Access Control (ABAC), and organizational uncertainty regarding vendor maturity (Garg et al., 2019; Thiam et al., 2019; Zied Milian et al., 2017). Phase Three (3) (Systemic Complexity): Recently, research frames complexity around microservices, observability through federated learning, and post-quantum cryptography (Alzoubi et al., 2024; Judijanto & Vandika, 2026; Reddy et al., 2026).
4. **International Collaboration**: The international co-authorship rate in this chapter (26.84%) reflects a notable increase compared to previous rates of 6.6% (Cai et al., 2015). This aligns with recent estimates indicating a co-authorship range of 20% to 25%, centering on collaborative involving the United States and China, as well as the Middle East and Asia (Abdulle et al., 2026; Reddy et al., 2026).

6.3. Contribution of the Chapter

This chapter enriches the body of knowledge regarding bibliometric studies of cloud security in the following ways:

Conceptualizing Cybersecurity Complexity: Unlike previous bibliometric studies that treated cloud security as a monolithic topic or focused on specific technical sub-domains, our work establishes the concept of "cybersecurity complexity" as an explicit theoretical framework. Here, we clarify how various factors including structural interdependencies in multi-cloud and evolved architecture and technologies and AI automation, converge to increase operational vulnerabilities.

We also provide the research evolution and complexity assessment of cloud computing security architectures and technologies, enabling clear direction of research field.

Analytical monitoring through 2026: We present an up-to-date assessment that keeps pace with the accelerated pace of post-pandemic research, tracking the rise of federated learning technologies and other cybersecurity practices.

6.4. Emerging Topics and Future Directions

Addressing the fourth research question RQ4, keyword evolution analysis identifies several emerging research areas that will shape the future of cloud computing security research. First, the term federated learning has emerged as a rapidly growing keyword (30 times during the period 2021–2026, after being very rare in previous periods). This reflects the increasing interest in privacy preserving machine learning models that enable collaborative model training without sharing raw data (Rahdari et al., 2025). This is crucial in cloud computing environments where data protection regulations such as the European GDPR regulation, enforce strict limitations on data processing and sharing. Future research is likely to focus on improving the efficiency of federated learning frameworks in multi cloud and hybrid computing environments.

Second, the integration of blockchain technology with cloud computing security represents a significant emerging trend. The inherent characteristics of blockchain technology enable innovative approaches to address cloud computing security challenges such as access control and data integrity and sovereignty (Wei et al., 2020). Keyword frequency analysis reveals that blockchain and cloud computing (20 occurrences) and blockchain and cloud computing security (16 occurrences) are among the strongest links which indicates a growing research in this area. Third, threat detection using deep learning (as evidenced by the strong occurrence of cloud computing security and deep learning, 24 occurrences) is rapidly evolving, and future trends are likely to include

interpretable artificial intelligence for security purposes, machine learning countermeasures, and real-time threat intelligence systems.

Fourth, edge computing security is a promising field driven by IoT devices and the need for low latency security processing at the network edge. The frequent use of the term edge computing (28 times) alongside cloud computing indicates growing research interest in security challenges of cloud edge computing architectures. Fifth, the relatively low frequency of terms such as symmetric encryption (27 times) and searchable encryption (27 times) suggests that advanced encryption techniques remain crucial research area, to enabling secure computing on encrypted cloud data. These emerging trends point to a future of cloud computing security characterized mainly by intelligence models, decentralization learning and privacy preserving cryptography.

6.5. Implications and Limitations

The findings of this study offer several important implications for researchers, practitioners, and policymakers. For researchers, the identification of emerging topics such as federated learning, blockchain-based security and edge computing security, opens directions for future research. The average rate of international collaboration suggests that researchers should actively pursue cross border partnerships to integrate diverse perspectives and regulatory frameworks into their work. For practitioners, the focus on impactful research in specific IEEE journals and Elsevier provides guidance on how to access the most influential studies. For policymakers, the geographic focus of the research output highlights the need to invest in cybersecurity research capabilities in underrepresented regions, particularly in Africa, Latin America, and small European countries to ensure balanced and resilient global cybersecurity knowledge base.

This study is subject to several limitations that should be acknowledged. Relying on a single database (Scopus) may lead to biased coverage. Furthermore, keyword-based search queries may not include all relevant publications, particularly those implicitly addressing cloud

computing security. Future research could complement this analysis with data from multiple databases, utilize more author identification algorithms such as Open Reseacher and Contributer ID (ORCID) based matching, and conduct citation context analysis to better understand the practical applications of published research. Despite these limitations, this study provides a solid foundation for understanding the growing cybersecurity complexities of cloud computing.

7. Conclusion

This bibliometric analysis provides a comprehensive, data-driven map of the cybersecurity complexity research in cloud computing, based on 1,583 publications extracted from Scopus database, covering the period from 2010 to 2026. The analysis is structured around four research questions that collectively address research maturity, active contributors, the evolution, and research directions in the field.

The key findings are summarized as follows: (1) first, the field is experiencing rapid growth, with annual output increasing from 3 research papers in 2010 to 358 papers in 2025, reflecting a CAGR exceeding 30%, and emphasizing the increasing importance of cloud computing security research. (2) Second, India and China mainly dominate the research domain, together accounting for more than 64% of global output, with IEEE being the leading publisher. (3) Third, this field demonstrates a solid academic impact, with an h-index of 76 and a total of 29,322 citations, supported by key research papers that each received over 700 citations.

Fourth, thematic development reveals a clear progression from foundational cloud computing security (2010–2015), through expansion to include threat detection, privacy and risk management (2016–2020), to the current AI-driven standard including machine learning, deep learning, blockchain technology, and federated learning (2021–2026). Fifth, international collaboration remains moderate at 26.84%, with the strongest relations between China and the United States, and between Saudi Arabia and India.

Identifying federated learning, blockchain-based security, edge computing security, symmetric encryption, and machine learning as the most promising emerging research directions provides a roadmap for future academic research. As cloud computing continues to evolve and integrate with emerging technologies, the challenges of cybersecurity will become increasingly complex requiring ongoing research collaboration efforts.

Declarations

Ethics Committee Approval: This chapter does not fall within the scope of research requiring ethics committee approval, such as studies involving the collection of data from participants through surveys, interviews, focus groups, observations, experiments, or other qualitative and quantitative approaches; the experimental or scientific use of humans or animals (including materials/data); clinical studies conducted on humans; studies conducted on animals; or retrospective studies subject to personal data protection legislation. Therefore, ethics committee approval was not deemed necessary.

Use of Artificial Intelligence: In this chapter, ChatGPT (OpenAI), Gemini, Consensus, and Manus were utilized for dataset analysis, language editing, and the summarization of papers and references. The author retains full responsibility for the content of the chapter.

Conflict of Interest: The author declares that there is no conflict of interest.

Funding: The author declares that this chapter received no financial support from any institution, project, or funding body.

Third-Party Materials and Permissions: No third-party figures, tables, images, or other materials requiring permission were used in this chapter. All figures and tables were prepared for this chapter and were not reproduced or adapted from third-party sources. The author confirms that no third-party materials requiring permission have been used in the chapter.

References

Abdulle, A. A., Jimale, A. D., Addow, M. A., & Nageye, A. Y. (2026). A bibliometric study of cost benefit analysis in cloud computing research. *Discover Applied Sciences*, *8*(7), 823. https://doi.org/10.1007/s42452-026-08872-y

Albshaier, L., Almarri, S., & Albuali, A. (2025). Federated learning for cloud and edge security: A systematic review of challenges and AI opportunities. *Electronics*, *14*(5), 1019. https://doi.org/10.3390/electronics14051019

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access*, *9*, 57792-57807. https://doi.org/10.1109/ACCESS.2021.3073203

Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. *Artificial Intelligence Review*, *57*(5), 132. https://doi.org/10.1007/s10462-024-10776-5

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58. https://doi.org/10.1145/1721654.1721672

Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Jäschke, A., Reuter, C. A., & Strand, M. (2015). *A guide to fully homomorphic encryption* (Paper 2015/1192). Cryptology ePrint Archive. https://eprint.iacr.org/2015/1192

Babaei, A., Kebria, P. M., Dalvand, M. M., & Nahavandi, S. (2023). *A review of machine learning-based security in cloud computing* (arXiv:2309.04911). arXiv. https://doi.org/10.48550/arXiv.2309.04911

Barrett, M. (2018). *Framework for improving critical infrastructure cybersecurity, version 1.1* (NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Bodeau, D., Graubart, R., Picciotto, J., & McQuaid, R. (2011). *Cyber resiliency engineering framework* (MTR110237). The MITRE Corporation.

Brookes, B. C. (1985). "Sources of information on specific subjects" by S. C. Bradford. *Journal of Information Science*, *10*(4), 173-175. https://doi.org/10.1177/016555158501000406

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

Cai, Y., Lu, W., Wang, L., & Xing, W. (2015). Cloud computing research analysis using bibliometric method. *International Journal of Software Engineering and Knowledge Engineering*, *25(3)*, 551-571. https://doi.org/10.1142/S0218194015400203

Chen, C. (2017). Science mapping: A systematic review of the literature. *Journal of Data and Information Science*, *2*(2), 1-40. https://doi.org/10.1515/jdis-2017-0006

Chen, H., Tsang, Y., & Wu, C. (2023). When text mining meets science mapping in the bibliometric analysis: A review and future opportunities. *International Journal of Engineering Business Management*, *15*, 18479790231222349. https://doi.org/10.1177/18479790231222349

Chuang, Y.-T., & Chuang, W.-Y. (2026). Bibliometric analysis and visualization of global trends in cyber-attacks and defenses. *International Journal of Data Science and Analytics*, *22*(1), 88. https://doi.org/10.1007/s41060-026-01069-x

Dayyabu, U. Y., Uppin, C., & Greenwood, J. (2020). A bibliometric analysis of cloud security research. *International Journal of Computer Engineering and Technology, 11*(4), 14-30.

Devarapalem, A. K. (2025). AI and machine learning for cloud security: A comprehensive survey of IDS and threat detection methods. In *2025 2nd Asian Conference on Intelligent Technologies (ACOIT)* (pp. 1-7). IEEE. https://doi.org/10.1109/ACOIT66109.2025.11436133

Feng, D. H., & Garg, A. (2021). India and China scientific collaborations at grass-root level: A new era. In A. Garg, C. H. Solanki, C. Bogireddy, & J. Liu (Eds.), *Proceedings of the 1st Indo-China Research Series in Geotechnical and Geoenvironmental Engineering* (pp. 175-194). Springer. https://doi.org/10.1007/978-981-33-4324-5_12

Folorunso, A., Adewa, A., Babalola, O., & Nwatu, C. E. (2024). A governance framework model for cloud computing: Role of AI, security, compliance, and management. *World Journal of Advanced Research and Reviews*, *24*(2), 1969-1982. https://doi.org/10.30574/wjarr.2024.24.2.3513

Fu, Z., Sun, X., Liu, Q., Zhou, L., & Shu, J. (2015). Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing. *IEICE Transactions on Communications*, *E98-B*(1), 190-200. https://doi.org/10.1587/transcom.E98.B.190

Garg, D., Sidhu, J., & Rani, S. (2019). Emerging trends in cloud computing security: A bibliometric analyses. *IET Software*, *13*(3), 223-231. https://doi.org/10.1049/iet-sen.2018.5222

Gartner. (2023, November 29). *Gartner says cloud will become a business necessity by 2028*. https://www.gartner.com/en/newsroom/press-releases/2023-11-29-gartner-says-cloud-will-become-a-business-necessity-by-2028

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 5. https://doi.org/10.1186/1869-0238-4-5

Hussain, C. B. M. (2026). Real-time AI-driven cybersecurity analytics dashboards for critical-infrastructure protection under Saudi Vision 2030: An NCA- and SDAIA-aligned governance-to-execution framework. *Nexus Science Review*, *1*(2), 1-18. https://doi.org/10.66104/berfcb18

Hussein, A. A. (2021). Data migration need, strategy, challenges, methodology, categories, risks, uses with cloud computing, and improvements in its using with cloud using suggested proposed model (DMig 1). *Journal of Information Security*, *12*(1), 79-103. https://doi.org/10.4236/jis.2021.121004

Jansen, W. A. (2011). Cloud hooks: Security and privacy issues in cloud computing. In *2011 44th Hawaii International Conference on System Sciences* (pp. 1-10). IEEE. https://doi.org/10.1109/HICSS.2011.103

Judijanto, L., & Vandika, A. Y. (2026). Cloud-native security in informatics: A bibliometric analysis of emerging research. *West Science Social and Humanities Studies*, *4(7)*, 948-959. https://doi.org/10.58812/wsshs.v4i07.3011

Khoda Parast, F., Sindhav, C., Nikam, S., Izadi Yekta, H., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, *114*, 102580. https://doi.org/10.1016/j.cose.2021.102580

Kolb, J., AbdelBaky, M., Katz, R. H., & Culler, D. E. (2020). Core concepts, challenges, and future directions in blockchain: A centralized tutorial. *ACM Computing Surveys*, *53*(1), 9. https://doi.org/10.1145/3366370

Lotka, A. J. (1926). The frequency distribution of scientific productivity. *Journal of the Washington Academy of Sciences*, *16*(12), 317-323.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176-189. https://doi.org/10.1016/j.dss.2010.12.006

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST Special Publication 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, *36*(1), 42-57. https://doi.org/10.1016/j.jnca.2012.05.003

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38-41. https://doi.org/10.1109/MSP.2018.3761723

Mukhopadhyay, D. (2022). Cybersecurity in India. *Communications of the ACM*, *65*(11), 98-102. https://doi.org/10.1145/3554910

Polizzi, G. L. (2026). The case of Saudi Arabia. In EU *science diplomacy in the Middle East: A comparative study of Jordan, Israel, and Saudi Arabia* (pp. 127-168). Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-23392-9_5

Rahdari, A., Keshavarz, E., Nowroozi, E., Taheri, R., Hajizadeh, M., Mohammadi, M., Sinaei, S., & Bauschert, T. (2025). A survey on privacy and security in distributed cloud computing: Exploring federated learning and beyond. *IEEE Open Journal of the Communications Society*, *6*, 3710-3744. https://doi.org/10.1109/OJCOMS.2025.3560034

Reddy, R. A., Pasha, S. N., & Kumari, D. S. (2026). Scientometric analysis of data privacy and cloud security: Research trends in access control and encryption techniques. In *2026 Sixth International Conference on Advances in Electrical, Computing, Communications and Sustainable Technologies (ICAECT)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICAECT68478.2026.11426087

Rittinghouse, J. W., & Ransome, J. F. (2010). *Cloud computing: Implementation, management, and security*. CRC Press.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. *IEEE Access*, *7*, 10127-10149. https://doi.org/10.1109/ACCESS.2018.2890507

Sarraf, G., & Pal, V. (2025). Autonomous threat detection and response in cloud security: A comprehensive survey of AI-driven strategies. *International Journal of Emerging Research in Engineering and Technology*, *6*(4), 111-121. https://doi.org/10.63282/3050-922X.IJERET-V6I4P114

Sevenard, I. (2026). Mutual norm socialization through knowledge-security restrictions in Sino-German academic cooperation. *Asian Review of Political Economy*, *5*(1), 3. https://doi.org/10.1007/s44216-026-00072-0

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, *3*(5), 637-646. https://doi.org/10.1109/JIOT.2016.2579198

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, 88-115. https://doi.org/10.1016/j.jnca.2016.11.027

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, *22*(2), 1191-1221. https://doi.org/10.1109/COMST.2019.2962586

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications*, *160*, 102642. https://doi.org/10.1016/j.jnca.2020.102642

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493-9532. https://doi.org/10.1007/s11227-020-03213-1

Thiam, L. S., Dargahi, T., & Dehghantanha, A. (2019). Bibliometric analysis on the rise of cloud security. In A. Dehghantanha & K.-K. R. Choo (Eds.), *Handbook of big data and IoT security* (pp. 329-344). Springer. https://doi.org/10.1007/978-3-030-10543-3_14

Wang, L., Tao, J., Kunze, M., Castellanos, A. C., Kramer, D., & Karl, W. (2008). Scientific cloud computing: Early definition and experience. In *2008 10th IEEE International Conference on High Performance Computing and Communications* (pp. 825-830). IEEE. https://doi.org/10.1109/HPCC.2008.38

Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, *102*, 902-911. https://doi.org/10.1016/j.future.2019.09.028

Xu, S., Ning, J., Li, Y., Zhang, Y., Xu, G., Huang, X., & Deng, R. H. (2022). Match in my way: Fine-grained bilateral access control for secure cloud-fog computing. *IEEE Transactions on Dependable and Secure Computing*, *19*(2), 1064-1077. https://doi.org/10.1109/TDSC.2020.3001557

Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, *8*, 131723-131740. https://doi.org/10.1109/ACCESS.2020.3009876

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, *1*(1), 7-18. https://doi.org/10.1007/s13174-010-0007-6

Zhang, Y., Deng, R. H., Xu, S., Sun, J., Li, Q., & Zheng, D. (2020). Attribute-based encryption for cloud computing access control: A survey. *ACM Computing Surveys, 53*(4), 83. https://doi.org/10.1145/3398036

Zied Milian, E., Mesquita Spinola, M., & Monteiro Carvalho, M. (2017). Risks and uncertainties in cloud computing: Literature review, trends and gaps. *IEEE Latin America Transactions*, *15*(2), 349-357. https://doi.org/10.1109/TLA.2017.7854632