

# Blockchain for Cloud Security: A Systematic Exploration of the Current Research Landscape

Bhavna Sharma<sup>1</sup>, Susheela Hooda<sup>2\*</sup> and Rajesh Kumar Kaushal<sup>3</sup>

<sup>1,2,3</sup>Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India  
sharma.bhavna341@gmail.com<sup>1</sup>, susheelahooda@gmail.com<sup>2\*</sup>, rajesh.kaushal@chitkara.edu.in<sup>3</sup>

Received: 14<sup>th</sup> June, 2026; Revised: 20<sup>th</sup> July 2026; Accepted: 20<sup>th</sup> August, 2026; Available Online: 05<sup>th</sup> September 2026

## ABSTRACT

Cloud computing has become a fundamental component of modern information technology, providing scalable, flexible, and cost-effective computing services. However, its widespread adoption has introduced critical security challenges, including data breaches, unauthorized access, privacy concerns, and limited transparency in data management. Blockchain technology has emerged as a promising solution to address these challenges through its decentralised, immutable, and transparent architecture. This study conducts a systematic bibliometric analysis of blockchain-enabled cloud security research based on 228 Scopus-indexed publications. Using Biblioshiny and VOSviewer, the study analyzes publication trends, author networks, journal impact, keyword patterns, thematic evolution, and the intellectual structure of the research field. The study examines predominant blockchain-based security mechanisms, including smart contracts, attribute-based encryption, homomorphic encryption, consensus mechanisms, data provenance, and public key cryptography, together with widely adopted blockchain frameworks such as Hyperledger Fabric, Hyperledger Besu, Ethereum, Quorum, and Corda. The findings indicate sustained growth in blockchain-enabled cloud security research, with increasing emphasis on privacy preservation, secure access control, cryptographic protection, and enterprise-oriented permissioned blockchain architectures. Despite these advancements, challenges related to scalability, interoperability, computational overhead, regulatory compliance, and practical deployment remain significant. The study also identifies emerging research opportunities in lightweight blockchain architectures, privacy-preserving computation, cross-chain interoperability, artificial intelligence integration, and secure smart contract verification. Overall, this work provides a comprehensive overview of the research landscape and offers valuable insights for researchers and practitioners developing scalable, privacy preserving, and secure blockchain-enabled cloud security solutions.

**Keywords:** Cloud Security, Blockchain Technology, Cryptography, Cloud Computing, Bibliometric Study.

**How to cite this article:** Sharma B, Hooda S, Kaushal RK., Blockchain for Cloud Security: A Systematic Exploration of the Current Research Landscape Int J Drug Deliv Technol. 2026;16(8): 15-33; DOI: 10.25258/ijddt.16.8.2

**Source of support:** Nil.

**Conflict of interest:** None

## 1 INTRODUCTION

Cloud computing has become fundamental to modern IT infrastructure, providing scalable, cost-efficient, on-demand services to organisations. It offers shared resources—applications, storage, networking, and services—that can be dynamically scaled to meet organizational needs, improving operational efficiency while reducing infrastructure costs (Ali et al. 2015; Subramanian and Jeyaraj 2018). However, cloud systems face significant security vulnerabilities inherent to their centralised architecture. Traditional cloud infrastructures lack decentralization, transparency, and immutable audit trails, making them vulnerable to multiple threats: unauthorized access, data tampering, denial-of-service attacks, and single points of failure. (Singh and Chatterjee 2017; Tripathi et al. 2023). These constraints also highlight the need for a strong and decentralized security model that is both immutable and transparent in cloud environments. To address these vulnerabilities, blockchain is a viable paradigm that could help solve several issues arising from existing cloud architectures. The inherent features of blockchain, including immutability,

decentralisation, and cryptographic security, can improve cloud security systems by providing controlled access, data provenance, and trust-based interactions among distributed users and entities (Tripathi et al. 2023; Bao et al. 2024; Elhadari et al. 2025). The integration of blockchain and cloud computing offers a decentralised solution to overcome the security, transparency and trust issues of traditional cloud computing architectures. Below are summarized the key benefits of blockchain integration that will improve transparency, security and privacy in cloud ecosystems.

1. It provides verifiable and tamper-proof data management through different hashing and consensus mechanisms.
2. Its decentralised nature eliminates need of a third-party intermediary.
3. Smart contracts provide automated access control, minimizing the risk of unauthorised access and data leakage.

\*Author for Correspondence: susheelahooda@gmail.com

4. The immutable nature of blockchain enables reliable auditing and tracking of transactions.
5. The distributed nature of blockchain enhances fault tolerance and ensures the continuous availability of the data to the users.

Blockchain technology offers a promising solution for enhancing cloud security through transparent audit trails, immutable records, and cryptographic mechanisms (Ahmed 2025; Alghamdi et al. 2024; Dorsala et al. 2021). Despite these benefits, the integration of cloud computing with blockchain is still an emerging area with various technical and practical challenges to overcome (Bao et al. 2024; Khan et al. 2024). However, practical cloud security deployment is still evolving, and several challenges, such as system integration, scalability, and consensus-related limitations, need to be continuously addressed to facilitate its widespread adoption. (Ullah and Ullah 2024; Ullah et al. 2024; H. Han et al. 2022).

### 1.1 Motivation

Cloud computing expansion has introduced critical security and privacy challenges, including threats to data integrity, trust management, and access control (Ullah et al. 2024; H. Han et al. 2022). Blockchain technology offers a promising solution through its inherent properties: decentralization, immutability, and cryptographic security (H. Han et al. 2022; Boughdiri et al. 2025; Jain et al. 2025). However, despite growing interest in blockchain-enabled cloud security, several technical and operational limitations remain unaddressed. To address this gap, this study provides a comprehensive review of blockchain-based security mechanisms that enhance transparency and trust while preserving privacy in cloud environments.

### 1.2 Objectives of the study

This study presents a systematic review and bibliometric analysis of research investigating blockchain-enabled approaches to enhance security in cloud environments. It identifies relevant sources and key research areas through author network analysis, keyword co-occurrence patterns, and thematic mapping using VOSviewer and Biblioshiny. Furthermore, different blockchain frameworks, consensus mechanisms, and the role of cryptography are also discussed. Through a systematic review of existing literature, this study identifies key challenges that must be addressed to develop secure and efficient cloud systems. The study further highlights future research directions and provides insights into how blockchain and cryptographic techniques can strengthen cloud security.

### 1.3 Research Questions

**RQ1:** What are the major research trends and thematic developments in the field of cloud security enhancement using blockchain technology?

**RQ2:** Which bibliometric tools, blockchain-based security methods, and frameworks are predominantly discussed in the existing literature for enhancing cloud security?

**RQ3:** What are the key challenges, research gaps, and future research opportunities identified in this domain?

The research questions are designed to explore key aspects of blockchain integration for enhancing cloud security. RQ1 aims to explore major research areas, prominent authors, and thematic development within this field. RQ2 focuses on identifying widely adopted bibliometric analysis tools, blockchain-based security techniques, and frameworks discussed in the literature. Subsequently, RQ3 explores different challenges, research gaps and future directions in this particular field. Some key contributions are discussed below.

1. It identifies key research areas and emerging themes related to blockchain-enabled cloud security.
2. It maps the research landscape by visualizing collaborative networks among institutions, authors, and countries.
3. It analyzes research trends, citation networks, and keyword occurrences to reveal the evolution of dominant research themes over time.
4. It highlights key challenges, emerging trends, and future research directions for blockchain-based cloud security.

This paper is organized into various sections: The Introduction section presents the background, motivation, and objectives of the study. Section 2 presents the background study and related work in the domain of blockchain-enabled cloud security. Section 3 discusses methodology, where the data collection and the PRISMA approach are designed to find relevant articles for further study. Section 5 presents the results and discussion, including bibliometric analyses generated using Biblioshiny and VOSviewer. It also discusses key challenges, research gaps, and future research directions. Finally, the conclusion summarizes the key findings and contributions of the study.

## 2 RELATED WORK

Recent studies have explored blockchain-based frameworks, cryptographic techniques, and consensus mechanisms to address cloud security challenges such as data breaches, access control, and data integrity. However, interoperability, scalability, and performance remain key challenges in existing solutions. The following studies examine blockchain-based approaches for improving security and efficiency in cloud environments.

### 2.1 Cloud Security Using Blockchain Technology

Sharma et al. (Sharma et al. 2021) developed a blockchain-based cloud storage infrastructure utilizing Merkle roots for verification, implementing robust data integrity and fine-grained access control mechanisms. The proposed approach eliminated the single point of failure while providing a trust-based environment. However, some challenges, like scalability and transaction processing delays, were present under a substantial volume of data. Li et al. (Li et al. 2024) presented a

decentralised storage system consisting of storage equilibrium strategies and data duplication. This architecture implemented encryption methods and segregated secret data sharing among distributed nodes. Blockchain technology plays a vital role in maintaining immutability, user authentication, and confidentiality of sensitive information. Yang et al. (Yang et al. 2021) described a distributed access control architecture that prevents unauthorized access to the sensitive information on cloud platforms. The proposed framework provides fine-grained access control, ensuring secure and auditable access to sensitive information. It ensures the immutability of the transactions and supports auditability. Verma et al. (Verma et al. 2025) proposed a secure access management architecture for cloud systems using blockchain. The use of smart contracts automates access management procedures, ensuring that only authorized entities are allowed to access the specific information. Cryptographic methods protect the transmission and preservation of information security, reducing reliance on third-party verification and improving security. Ahmed et al. (Ahmed 2025a) discussed an analysis of blockchain-based cybersecurity approaches for cloud infrastructure, using a systematic review of the literature. The review examined decentralization, cryptographic mechanisms, immutability, and cloud security vulnerabilities. From the analysis, it can be observed that blockchain ensures data integrity, authentication, transparency, and eliminates reliance on traditional centralised authorities.

## 2.2 Blockchain-Based Data Privacy and Access Control

Shi et al. (Shi et al. 2020) introduced blockchain techniques for EHR management, focusing on the security and privacy of healthcare data. The study identified key privacy requirements, including confidentiality, auditability, integrity, availability, and anonymity. The authors discussed that blockchain enhances EHR security, data integrity, and allows audit control features. However, scalability, computational overhead, and limited standardization remain significant challenges. Tanwar et al. (Tanwar et al. 2020) presented a blockchain-based electronic medical record system for healthcare 4.0. This study utilises AES encryption along with an Access Control Policy Algorithm that could enhance the fine-grained access control of sensitive information. The proposed framework utilizes consensus mechanisms, distributed ledgers and peer-to-peer networks for efficient data dissemination. The authors demonstrated that blockchain eliminates the single point of failure while maintaining data integrity. Han et al. (Y. Han et al. 2022) discussed blockchain use cases in the healthcare domain. An Ethereum-based blockchain framework was developed to monitor patient data remotely, and ensure data availability across the network. The authors focused on integrating secure multi-party computing (MPC) protocols in a blockchain network, which ensured patient autonomy over sensitive healthcare information. However, computational overhead and efficient management of large data volumes remain challenges. Dubovitskaya et al.

(Dubovitskaya 2020) proposed ACTION-EHR, which is designed as a patient-centric blockchain framework. Hyperledger Fabric was used as a blockchain framework in collaboration with Stony Brook University Hospital for cancer treatment data management. This study utilized HL7 FHIR for health record representation and demonstrated greater patient control over clinical information. Significant challenges remain, including integration with legacy hospital infrastructures and compliance with regulatory requirements. Ali et al. (Ali 2025) proposed a Blockchain-based Federated Learning (BFL) model in the context of IoT-integrated healthcare systems. This paradigm combines federated learning with blockchain to support collaborative model development without exchanging raw data. The approach combines Zero-Knowledge Proofs (ZKP) with Homomorphic Encryption (HE) for privacy protection. Experimental results showed a 19.7% increase in throughput and 87% reduction in latency compared to state-of-the-art frameworks. However, implementation complexity and computational overhead remain significant challenges.

These studies demonstrate that blockchain significantly improves privacy protection and access control through cryptographic techniques and decentralized architectures. However, scalability, computational overhead, and implementation complexity remain major challenges.

## 2.3 Privacy-Preserving Security Mechanisms in Sensitive Data Environments

Tawfik et al. (Tawfik 2025) described the AC-Health Chain scheme for fine-grained access control in healthcare. The proposed framework allows patients to manage privacy settings and uses AES encryption with IPFS storage and permanent blockchain storage. The patient-centric approach enables identity verification through the blockchain chaincode. The study proved that patients' control over their medical information strongly enhances privacy management. Xu et al. (Xu et al. 2024) presented PRHBS, a privacy-preserving and redactable healthcare blockchain structure. It provides compliance for several aspects of the GDPR, including "right to erasure" by means of trapdoor-mediated chameleon-hash and attribute-based encryption. Moreover, security testing demonstrated that the framework provides robustness against unauthorized access with comparable computational cost. The framework combines differential privacy with federated learning to improve confidentiality while supporting collaborative analytics without exposing plaintext medical information. Experimental studies on the Ethereum blockchain indicated efficient transaction processing with optimized resource usage. This study was able to provide strong privacy guarantees with relatively good analytical performance. Yang et al. (Yang et al. 2022) proposed a revocable attribute-based encryption e-health record sharing scheme with multiple authorization authorities. Blockchain technology provides decentralised authority management, thereby reducing dependence on centralised authorities. Cloud infrastructure pre-decryption optimization overcomes concerns related to user

computation. Performance measurement offers reliable security deployment along with reduced operational expenses. Dou et al. (Dou et al. 2025) developed a secure medical data framework combining attribute-based encryption and blockchain technology. Attribute-based encryption provides advanced authorization management using the attribute-specific description approach, and blockchain provides a secure distributed environment for information exchange. The edge infrastructure with blockchain propagation reduces computational resource limitations. Additionally, the framework demonstrated enhanced security for sensitive medical records. Overall, these studies highlight the growing adoption of privacy-preserving cryptographic techniques, although practical deployment and computational efficiency remain important research challenges.

#### 2.4 Consensus Mechanisms and Blockchain Frameworks

Muneshwara et al. (Muneshwara et al. 2023) introduced a novel consensus protocol called the Enhanced Proof of Stake (ePoS) algorithm. The study addressed the weaknesses of conventional PoS systems, such as consensus time and transaction processing speed. The enhanced consensus decreases the time taken to finalize consensus while increasing transaction throughput and decreasing energy usage in comparison with traditional PoS approaches. Ganache-based experimental evaluations verified that the proposed algorithm for blockchain in IoT healthcare ecosystems outperforms the conventional approach. Rahman et al. (Rahman 2024) analyzed various consensus mechanisms in use with blockchain for enhancing the security of healthcare access. Various consensus models, such as Proof-of-Work (PoW), PoS, and different types of Byzantine Fault Tolerance, were reviewed in this study. The study highlighted that the choice of consensus mechanism influences network performance features, including transaction speed, computation resource use, and scalability of the network. The analysis showed that Practical Byzantine Fault

Tolerance performs well on permissioned healthcare networks and have better control over participant validation. Vinayasree et al. (Vinayasree et al. 2024) introduced a scalable and secure blockchain-based healthcare system that combines Practical Byzantine Fault Tolerance with sharding infrastructure. It incorporates cryptographic constructions and an advanced consensus method to improve consensus efficiency under varying distributed node settings, even in the presence of malicious nodes. The proposed framework demonstrated that sharding with PBFT improves scalability while reducing consensus time. The architecture achieved reliable security enforcement at the design level, yet retained the high transaction processing throughput appropriate for widespread medical information exchange. Oki et al. (Agbeyangi et al. 2024) presented Hyperledger Fabric deployment for Electronic Health Record (EHR) management. This study focused on the modular architecture and permissioned consensus protocols by Hyperledger Fabric to achieve enterprise-grade security without the need for excessive computational resources. The study showed how a permissioned model can improve system performance and support healthcare-related regulatory requirements. The results demonstrated that Hyperledger Fabric is an effective approach for healthcare institutions. Chakraverti et al. (Chakraverti 2025) designed the whole blockchain system based on an optimized permissioned Raft and Byzantine Fault Tolerance HEO-PRAFT consensus mechanism. The approach also leverages a human evolution optimization algorithm to facilitate a dynamic validator selection that accelerates consensus while maintaining security properties. It uses the Elliptic Curve Proxy Re-encryption scheme combined with the Structural Preserving Scheme authentication protocol to secure complete patient information. Overall, permissioned blockchain frameworks combined with efficient consensus mechanisms provide improved security and performance, although scalability and validator management continue to require further investigation.

**Table 1:** Comparative analysis of existing blockchain-based studies

| Reference                | Year | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|--------------------------|------|---|---|---|---|---|---|---|---|---|
| Sharma et al. [16]       | 2021 | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Li et al. [17]           | 2024 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Yang et al. [18]         | 2021 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Verma et al. [19]        | 2025 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Ahmed et al. [20]        | 2025 | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ |
| Shi et al. [21]          | 2020 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| Tanwar et al. [22]       | 2020 | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ |
| Han et al. [23]          | 2022 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ |
| Dubovitskaya et al. [24] | 2020 | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ |
| Ali et al. [25]          | 2025 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Tawfik et al. [26]       | 2025 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Xu et al. [27]           | 2024 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Yang et al. [28]         | 2022 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Dou et al. [29]          | 2025 | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Muneshwara et al. [30]   | 2023 | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ |

|                         |      |   |   |   |   |   |   |   |   |   |   |
|-------------------------|------|---|---|---|---|---|---|---|---|---|---|
| Rahman et al. [31]      | 2024 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| Vinayasree et al. [32]  | 2024 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Agbeyangi et al. [33]   | 2024 | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ |
| Chakraverti et al. [34] | 2025 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |

**Note:** 1–Blockchain Basics, 2–Consensus Protocols, 3–Data Privacy, 4–Secure Data Sharing, 5–Scalability, 6–Access Control, 7–Performance Optimization, 8–Integration with Cloud, 9–Practical Implementation. = Topic covered; = Topic not covered.

Table 1 presents a comparative analysis of existing blockchain-based cloud security studies across nine key evaluation criteria. The comparison shows that access control, data privacy, and practical implementation are discussed in most of the studies, whereas secure data sharing, consensus protocols, cloud integration, and performance optimization are comparatively less covered, reflecting differing research priorities. Overall, the comparison highlights the strengths and limitations of existing studies and establishes the foundation for the subsequent bibliometric analyses.

### 3 RESEARCH METHODOLOGY

This study adopts a bibliometric analysis approach to investigate the global research landscape on blockchain-based cloud security. The workflow consists of data collection, screening, bibliometric analysis, visualization,

and interpretation of the selected literature. The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines were used to facilitate a systematic process for identifying, screening, and selecting relevant publications for bibliometric analysis (Pham and Le 2024). Figure 1 presents the PRISMA workflow used for publication selection. The methodology comprises two stages: (a) selection process and (b) inclusion and exclusion criteria.

#### 3.1 Selection Process

The Scopus database was selected because of its extensive multidisciplinary coverage, comprehensive bibliographic metadata, and compatibility with bibliometric analysis tools such as Biblioshiny and VOSviewer. It was used to retrieve publications related to blockchain technology and cloud security. Search strings were developed using keywords associated with blockchain technology and cloud security to identify relevant articles, conference papers, review papers, and book chapters. During the identification phase, a total of 366 records were retrieved from the Scopus database.

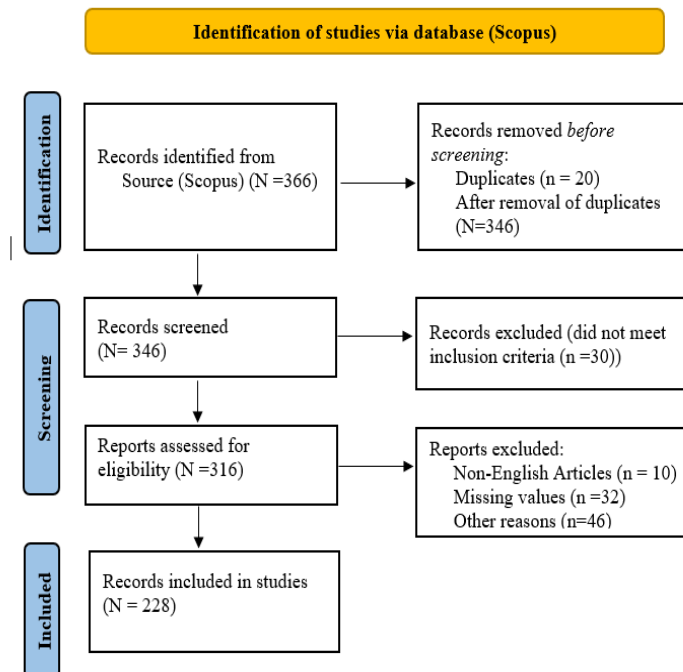


**Figure 1:** PRISMA flow diagram for article selection process

Duplicate records were removed before the screening stage. The remaining records were screened according to the predefined inclusion and exclusion criteria. Records with missing bibliographic information, non-English language, or limited relevance to the study were excluded.

Following the screening and selection process, 228 Scopus-indexed publications published between 2019 and early 2025 were retained for the final bibliometric analysis. Table 2 presents the search string used to retrieve the bibliographic dataset.

**Table 2:** Source and search string for bibliometric analysis

| Source | Search String                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scopus | ((("Enhancement" OR "Improvement") AND ("security" OR "cybersecurity" OR "cyber-security" OR "data security" OR "cloud computing security" OR "privacy" OR "data privacy" OR "data integrity" OR "data protection" OR "access control" OR "authentication" OR "authorization" OR "secure data sharing" OR "decentralised security" OR "tamper resistance" OR "transparency" OR "cryptography" OR "cryptographic algorithm") AND ("decentralization" OR "distributed management" OR "distributed technology" OR "distributed-ledger") AND ("blockchain" OR "blockchain-technology") AND ("scalability" OR "efficiency") AND ("cloud" OR "cloud computing" OR "cloud environment")) |

### 3.2 Inclusion and Exclusion Criteria

Predefined inclusion and exclusion criteria were applied to identify publications relevant to the objectives of the study. Publications were considered based on document type, relevance to blockchain-enabled cloud security,

publication period, language, and bibliographic completeness. Records that were duplicates, non-English, incomplete, or outside the scope of the study were excluded. Table 3 summarizes the criteria applied during the data refinement process.

**Table 3:** Inclusion and exclusion criteria

| S. No. | Inclusion Criteria                                                    | Exclusion Criteria                               |
|--------|-----------------------------------------------------------------------|--------------------------------------------------|
| 1      | Source type: Articles, conference papers, reviews, and book chapters. | Undefined author information                     |
| 2      | Documents related to blockchain-enabled cloud security.               | Undefined DOI                                    |
| 3      | Articles from 2019 to early 2025 were selected.                       | Duplicate records                                |
| 4      | English language articles were considered.                            | Non-English articles                             |
| 5      | Studies from all geographical regions were included.                  | Records marked as ineligible by automation tools |

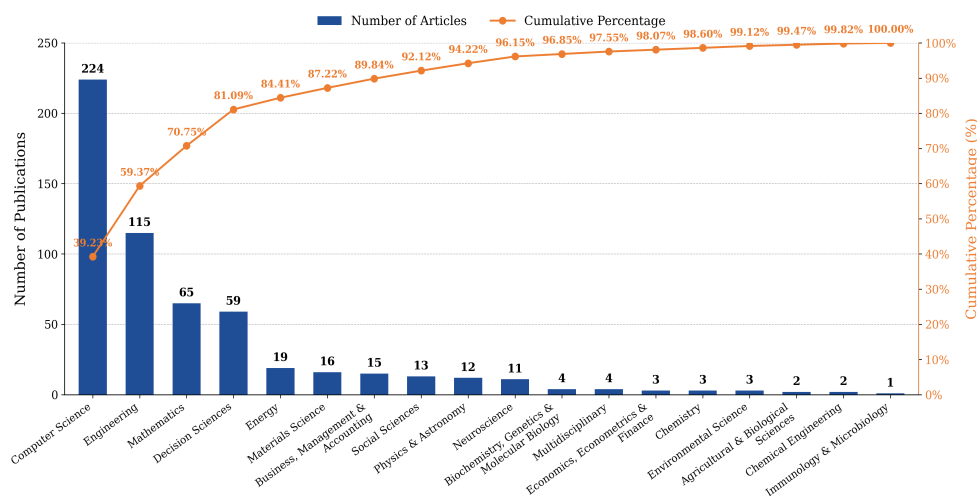
After dataset extraction and preprocessing, the bibliographic records were exported in CSV format and analysed using Biblioshiny and VOSviewer to generate bibliometric networks and scientific visualizations. The analysis focused on publication trends, source productivity, keyword co-occurrence, thematic evolution, collaboration networks, and research hotspots within blockchain-enabled cloud security.

## 4 RESULTS AND DISCUSSION

**4.1** What are the major research trends and thematic developments in the field of cloud security enhancement using blockchain technology?

### 4.1.1 Key Research Areas

Figure 2 illustrates the distribution of Scopus-indexed publications across the major subject areas represented in blockchain-enabled cloud security research. Computer Science constitutes the largest research domain, with 224 publications (39.23%), followed by Engineering (20.14%), Mathematics (11.38%), and Decision Sciences (10.33%).

**Distribution of Publications Across Subject Areas****Figure 2:** Key subject areas identified in blockchain-based cloud security research

Together, these four subject areas account for more than 81% of the reported distribution, indicating that research

in blockchain-enabled cloud security is primarily driven by computing, engineering, mathematical, and decision-

oriented disciplines. The remaining subject areas contribute comparatively smaller shares.

#### 4.1.2 Source Production Over Time

Figure 3 presents the publication trends of the leading sources in blockchain-enabled cloud security research between 2019 and 2025. IEEE Access shows the strongest growth, increasing from one publication in 2021 to nine publications by 2025. The ACM International Conference

Proceeding Series and the International Journal of Advanced Computer Science and Applications (IJACSA) also maintain publication activity, while LNEE, LNNS, and LNDECT show noticeable growth after 2022, each reaching five publications by 2025. The increasing activity across multiple sources indicates that research in blockchain-enabled cloud security has expanded across different publication venues.

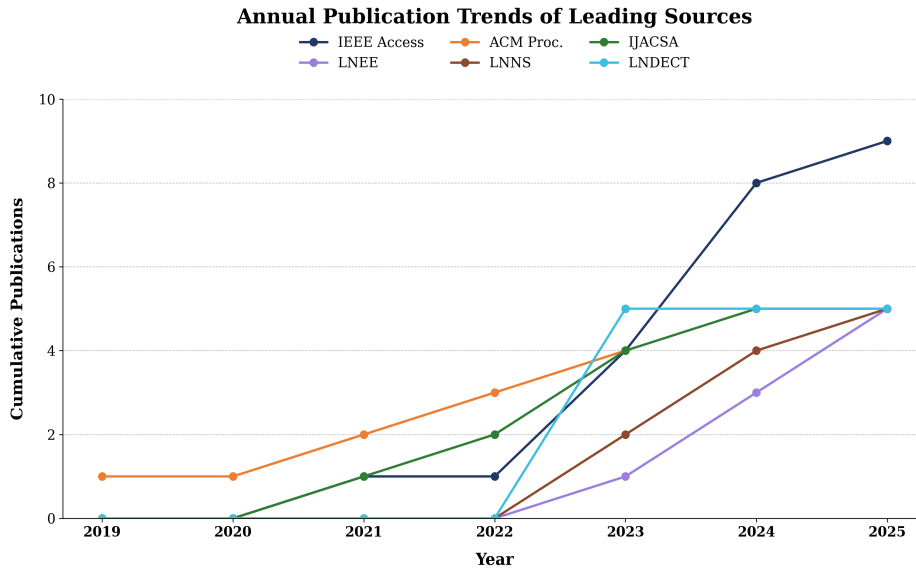


**Figure 3:** Annual publication trends of the leading publication sources in blockchain-based cloud security research

**Note:** IJACSA = International Journal of Advanced Computer Science and Applications; LNEE = Lecture Notes in Electrical Engineering; LNNS = Lecture Notes in Networks and Systems; LNDECT = Lecture Notes on Data Engineering and Communications Technologies

#### 4.1.3 Most Relevant Sources

Table 4 summarizes the leading publication sources according to publication output and bibliometric impact indicators. IEEE Access records the highest publication output with nine articles, followed by Cluster Computing

and the Journal of Supercomputing with four publications each. In contrast, IEEE Communications Surveys & Tutorials has the highest Impact Factor (19.8) and CiteScore (43.5), followed by ACM Computing Surveys and IEEE Transactions on Cloud Computing. This distinction shows that publication productivity and bibliometric impact do not necessarily correspond. The presence of several Q1 venues further indicates that blockchain-enabled cloud security research is represented across established computing, cloud, networking, and security journals.

**Table 4:** Top 15 most relevant publication sources

| Source                                                  | IF   | CS   | Quartile | Publisher | NA |
|---------------------------------------------------------|------|------|----------|-----------|----|
| IEEE Access                                             | 3.9  | 9    | Q1       | IEEE      | 9  |
| Cluster Computing                                       | 4.4  | 7    | Q1       | Springer  | 4  |
| Journal of Supercomputing                               | 3.3  | 6.3  | Q2       | Springer  | 4  |
| IEEE Internet of Things Journal                         | 10.6 | 17.6 | Q1       | IEEE      | 3  |
| ACM Computing Surveys                                   | 16.6 | 33.2 | Q1       | ACM       | 2  |
| IEEE Transactions on Cloud Computing                    | 9.2  | 18.7 | Q1       | IEEE      | 2  |
| Future Generation Computer Systems                      | 7.9  | 14.3 | Q1       | Elsevier  | 2  |
| Information Sciences                                    | 7.2  | 12.4 | Q1       | Elsevier  | 2  |
| Computer Networks                                       | 5.6  | 10.1 | Q1       | Elsevier  | 2  |
| Journal of Systems Architecture                         | 4.1  | 8    | Q2       | Elsevier  | 2  |
| Journal of Cloud Computing                              | 4    | 6.8  | Q1       | Springer  | 2  |
| Concurrency and Computation Practice and Experience     | 2    | 5    | Q2       | Wiley     | 2  |
| IEEE Communications Surveys and Tutorials               | 19.8 | 43.5 | Q1       | IEEE      | 1  |
| Journal of Network and Computer Applications            | 8.7  | 16.2 | Q1       | Elsevier  | 1  |
| IEEE Transactions on Information Forensics and Security | 7.6  | 15.3 | Q1       | IEEE      | 1  |

**Note:** IF = Impact Factor; CS = CiteScore; NA = Number of Articles.

#### 4.1.4 Leading Authors in Blockchain-Enabled Cloud Security

Table 5 presents the leading authors contributing to blockchain-enabled cloud security research during the study period (2019–2025), together with their affiliations, total citations, h-index, and first publication year within the selected dataset. The identified authors are affiliated

with institutions across different geographical regions, while their citation and h-index values show variation in scholarly impact. Most of the listed authors have their first publication in the selected dataset during 2023–2025, indicating the presence of several relatively recent contributors to the field.

**Table 5:** Top 10 leading authors in blockchain-enabled cloud security research

| Author      | Affiliation                           | TC  | h-index | PY-start |
|-------------|---------------------------------------|-----|---------|----------|
| A. Singh    | IIT Madras                            | 45  | 2       | 2025     |
| M. Alqudah  | Qatar University                      | 90  | 3       | 2025     |
| S. Ahmad    | University of Technology Sydney       | 80  | 3       | 2024     |
| V. Raja     | Chitkara University                   | 110 | 5       | 2024     |
| L. Ante     | University of Oldenburg               | 60  | 2       | 2024     |
| P. Khurana  | Indira Gandhi Institute of Technology | 130 | 4       | 2023     |
| K. Sharma   | Indira Gandhi Institute of Technology | 115 | 3       | 2023     |
| R. Kumar    | IIT Delhi                             | 90  | 4       | 2023     |
| G. K. Kaur  | Punjabi University                    | 120 | 5       | 2023     |
| Abhishek P. | KLE Technological University, India   | 5   | 2       | 2021     |

**Note:** TC = Total Citations; PY-start = First publication year in selected dataset.

#### 4.1.5 Corresponding Author Countries

Table 6 illustrates the geographical distribution of corresponding authors and international collaboration patterns. India is the leading contributor, accounting for 28.33% of the publications, followed by China with 16.31%. However, publication productivity and

international collaboration show different patterns: China has a higher MCP ratio than India (0.2632 vs. 0.1212), while Saudi Arabia records the highest MCP ratio (0.6667) despite its lower publication frequency. In contrast, the USA and United Kingdom show an MCP ratio of zero in the selected dataset.

**Table 6:** top 10 contributing countries by corresponding authors

| Country        | A  | SCP | MCP | Freq   | MCP Ratio |
|----------------|----|-----|-----|--------|-----------|
| India          | 66 | 58  | 8   | 0.2833 | 0.1212    |
| China          | 38 | 28  | 10  | 0.1631 | 0.2632    |
| Korea          | 3  | 2   | 1   | 0.0129 | 0.3333    |
| Morocco        | 3  | 2   | 1   | 0.0129 | 0.3333    |
| Saudi Arabia   | 3  | 1   | 2   | 0.0129 | 0.6667    |
| USA            | 3  | 3   | 0   | 0.0129 | 0.0000    |
| Egypt          | 2  | 1   | 1   | 0.0086 | 0.5000    |
| Germany        | 2  | 1   | 1   | 0.0086 | 0.5000    |
| Greece         | 2  | 1   | 1   | 0.0086 | 0.5000    |
| United Kingdom | 2  | 2   | 0   | 0.0086 | 0.0000    |

**Note:** A = Total Articles, SCP = Single Country Publications, MCP = Multiple Country Publications, Freq = Frequency of contribution, MCP Ratio = MCP/A.

#### 4.1.6 Keyword and Abstract Analysis

The keyword and abstract analyses provide complementary evidence of the dominant research themes in blockchain-enabled cloud security. Figure 4 presents the fifteen most frequently occurring author keywords. Blockchain is the most frequent keyword with 354

occurrences, followed by cloud security with 205 and cloud computing with 161. Other prominent terms include cloud storage, cryptography, data privacy, network security, authentication, data sharing, access control, and distributed ledger, indicating a strong focus on secure cloud data management and access control.

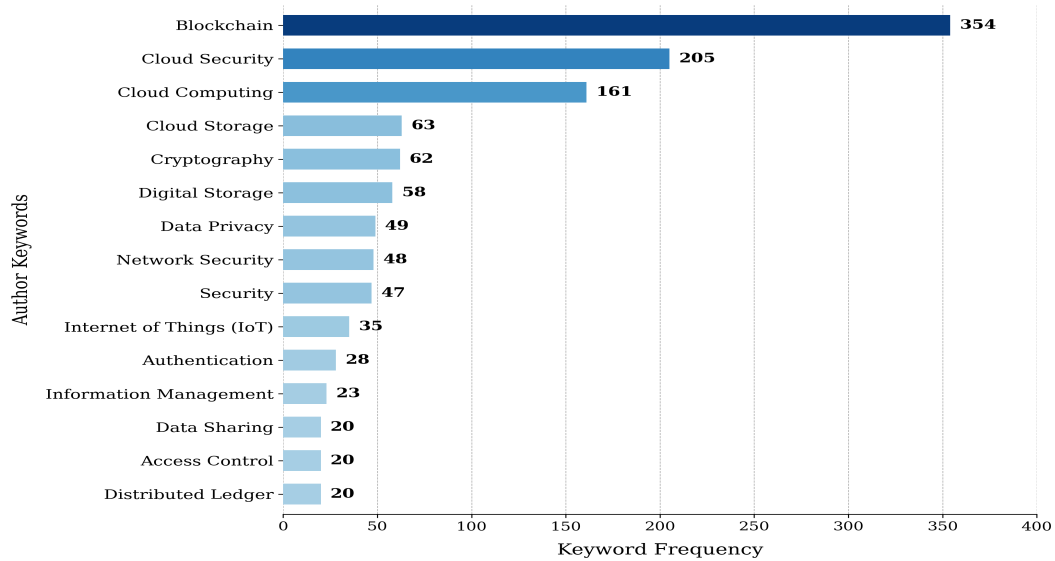


**Figure 4:** Frequently occurring keywords in blockchain-enabled cloud security research

The abstract-term analysis in Figure 5 provides a complementary view of the concepts occurring within the study descriptions. Frequently occurring terms include

cloud computing, cloud security, blockchain technology, cloud storage, data security, data sharing, access control, privacy protection, and encryption schemes.



**Figure 5:** Abstract terms co-occurrence analysis illustrating dominant research themes in blockchain-enabled cloud security

Terms such as fog computing, medical data, and decentralized cloud schemes further indicate application-specific research contexts. Together, the keyword and abstract analyses identify three closely related research emphases: blockchain–cloud integration, secure cloud data management, and privacy- and access-control-oriented security mechanisms.

#### 4.1.7 Co-occurrence Analysis Based on Keywords

The keyword co-occurrence network generated using VOSviewer identifies relationships among author keywords occurring at least ten times in the retrieved literature. As shown in Figure 6, the network forms four interconnected thematic clusters.

- 1. Cluster 1 (Green):** This cluster focuses on data management and privacy, including blockchain

technology, data privacy, data integrity, privacy protection, public key cryptography, and data sharing.

2. **Cluster 2 (Red):** This cluster represents blockchain–cloud integration, linking blockchain, cloud security, and cloud computing with cybersecurity, IoT, fog computing, and network architecture.
3. **Cluster 3 (Blue):** This cluster emphasizes privacy, authorization, distributed ledger, data sharing, information management, and privacy-preserving techniques, indicating a focus on controlled and secure information exchange.
4. **Cluster 4 (Yellow):** This cluster centers on security mechanisms, including cryptography, authentication, access control, cloud storage, trusted computing, smart contracts, and network security.

Collectively, the four clusters show that blockchain-enabled cloud security research is structured around interconnected themes covering blockchain–cloud

integration, data privacy and management, controlled information sharing, and security mechanisms.

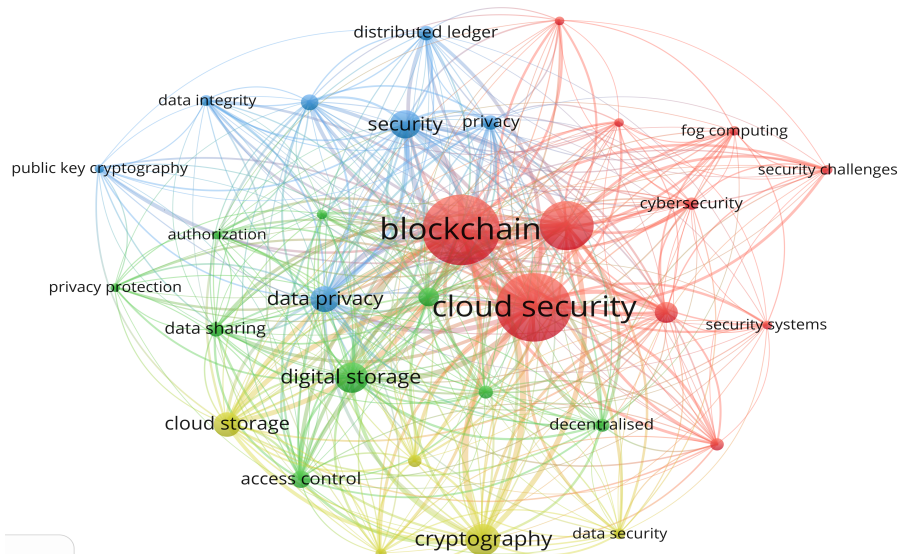


**Figure 6:** VOSviewer-based keyword co-occurrence network showing thematic clusters in blockchain-based cloud security research

#### 4.1.8 Thematic Map

Figure 7 presents the thematic map of blockchain-enabled cloud security research based on centrality and density.

Blockchain, cloud security, and cloud computing appear as Basic Themes, indicating their central position in the overall research structure.

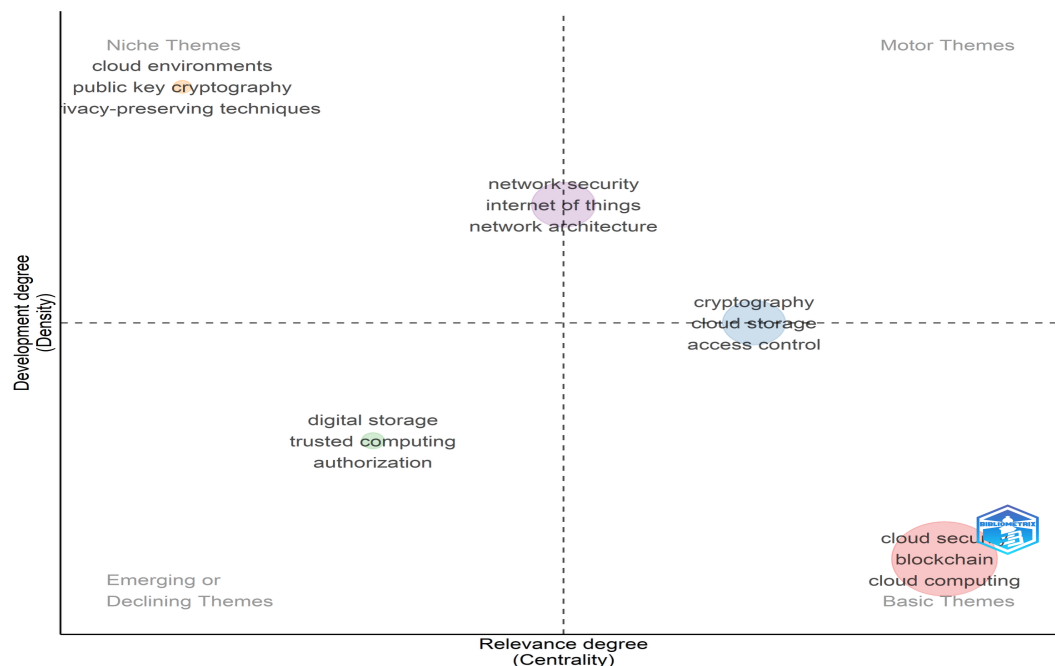


**Figure 7:** Thematic map illustrating the conceptual structure of blockchain-enabled cloud security research

**Note:** Centrality represents the relevance of a research theme within the overall research field, whereas density indicates its level of development. Larger bubbles denote themes with greater relative importance.

Network security, Internet of Things (IoT), and network architecture are positioned as Motor Themes, while cloud environments, public key cryptography, and privacy-preserving techniques appear as Niche Themes. Digital

storage, trusted computing, and authorization are positioned in the Emerging or Declining Themes quadrant. Since this quadrant may contain both newly emerging and declining topics, these themes should not be classified definitively without temporal analysis. Overall, the thematic map distinguishes foundational themes from active, specialized, and comparatively less-developed research areas. Digital storage, trusted computing, and authorization are positioned in the Emerging or Declining

quadrant. Since this quadrant may contain both emerging and declining themes, their position should not be interpreted as definitive evidence of either trend. Overall, the thematic map distinguishes the foundational themes from active, specialized, and comparatively less-developed research areas.

#### 4.1.9 Three-Field Plot Analysis

Figure 8 links the most productive authors (AU), dominant author keywords (DE), and leading publication sources (SO). Blockchain, cloud computing, and cloud security form the strongest thematic links, while IEEE Access, IJACSA, and LNDECT show prominent connections with the identified research themes. The plot therefore provides an integrated view of how major contributors, research

topics, and publication venues are connected. The RQ1 findings show that blockchain-enabled cloud security is primarily driven by Computer Science and Engineering, with substantial contributions from Mathematics and Decision Sciences. Publication activity is distributed across multiple established venues, while India and China represent the major contributing countries. At the conceptual level, blockchain, cloud security, and cloud computing form the core of the research landscape, with data privacy, secure data management, cryptography, authentication, access control, and data sharing forming closely related research dimensions. The co-occurrence, thematic-map, and three-field analyses further confirm the interconnected structure of these themes and their association with active researchers and publication venues.

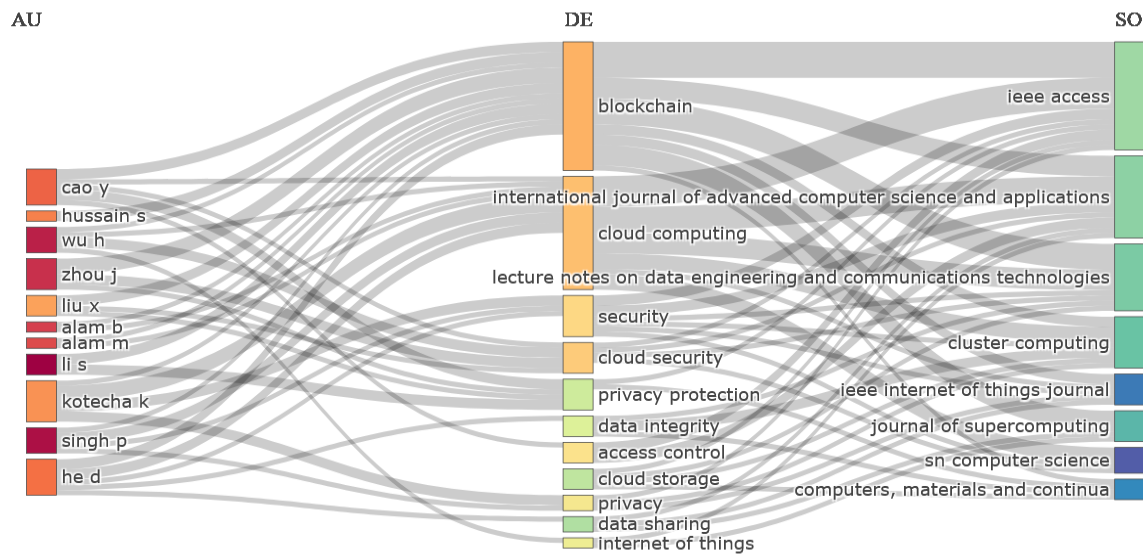


**Figure 8:** Three-field plot of authors, keywords, and publication sources

**4.2 RQ2:** Which bibliometric tools, blockchain-based security methods, and frameworks are predominantly discussed in the existing literature for enhancing cloud security?

To address RQ2, the retrieved literature was further examined to identify the bibliometric tools, blockchain-based security mechanisms, and blockchain frameworks most frequently employed in cloud security research. This analysis provides an overview of the analytical tools used for bibliometric investigations as well as the technological approaches adopted to enhance the security, privacy, and reliability of cloud environments.

##### 4.2.1 Bibliometric Analysis Tools

In this study, VOSviewer and Biblioshiny were mainly used to analyse the conceptual and structural framework in blockchain based cloud security.

1. **VOSviewer:** VOSviewer is a popular bibliometric visualization tool that can be used to construct and analyze scientific knowledge networks based on large-scale bibliographic data. In this study, it was employed to generate keyword co-occurrence networks, abstract term analysis, and keyword relationship visualizations.

These analyses facilitate the identification of research themes, conceptual relationships, and emerging trends within blockchain-enabled cloud security research (Eck and Waltman 2010; Aria and Cuccurullo 2017).

2. **Biblioshiny:** Biblioshiny provides a web-based interactive interface for conducting comprehensive bibliometric analyses without requiring programming expertise. In this study, it was used to examine publication trends, leading authors, influential journals, country-wise scientific production, thematic evolution, and collaboration patterns. Its integrated analytical capabilities support a systematic exploration of the intellectual structure and evolution of blockchain-enabled cloud security research (Aria and Cuccurullo 2017; Du 2024).

The combined use of VOSviewer and Biblioshiny facilitated comprehensive visualization and analysis of publication trends, collaboration networks, research themes, and the overall knowledge structure of blockchain-enabled cloud security research.

#### 4.2.2 Blockchain-Based Security Methods

Blockchain-enabled cloud security relies on multiple security mechanisms to address challenges related to data confidentiality, integrity, authentication, access control, and trust. The most frequently discussed mechanisms identified in the literature are summarized below.

1. **Smart Contracts:** Smart contracts automate the execution of predefined security policies, ensuring that data access permissions are enforced without manual intervention. They are widely employed for access control, compliance verification, automated auditing, and policy enforcement in blockchain-enabled cloud environments (Tolmach et al. 2021; Islam et al. 2021).
2. **Attribute-Based Encryption (ABE):** Attribute-Based Encryption is a cryptographic technique that provides encryption and access control through user attributes

such as role, organization, and department level. Access to encrypted data is granted only when a user's attributes satisfy the predefined access policies. (Li et al. 2021; Zuo et al. 2024; Yin et al. 2024).

3. **Homomorphic Encryption:** It enables computations to be performed directly on encrypted data without exposing the original information, making it particularly suitable for privacy-preserving cloud analytics and sensitive data processing (Yin et al. 2024; Kumar et al. 2022; Kumar et al. 2024).
4. **Consensus Mechanisms:** Consensus mechanisms enable participating nodes to reach agreement on the valid state of the distributed ledger, thereby ensuring data integrity, fault tolerance, and trust among network participants (Yousuf et al. 2021; Zaeem and Bardzell 2021).

**Table 7:** Comparison of security mechanisms for blockchain-enabled cloud security

| Security Mechanism                      | Primary Function                                           | Advantages                                                             | Limitations                                                     | Primary Applications                                                    |
|-----------------------------------------|------------------------------------------------------------|------------------------------------------------------------------------|-----------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Smart Contracts</b>                  | Automated policy enforcement and access control            | Automation, transparency, auditability, reduced human intervention     | Coding vulnerabilities, limited post-deployment flexibility     | Access control, identity management, compliance enforcement             |
| <b>Attribute-Based Encryption (ABE)</b> | Fine-grained encryption and attribute-based access control | Flexible access policies, strong confidentiality, secure data sharing  | High computational overhead, complex key management             | Secure cloud storage, healthcare data sharing, enterprise systems       |
| <b>Homomorphic Encryption</b>           | Computation on encrypted data                              | Privacy-preserving processing, data confidentiality during computation | High computational cost, increased processing latency           | Secure cloud analytics, healthcare, financial services                  |
| <b>Consensus Mechanisms</b>             | Distributed ledger validation and agreement                | Data integrity, fault tolerance, decentralised trust                   | Scalability limitations, high energy consumption (PoW), latency | Transaction validation, distributed cloud services, blockchain networks |
| <b>Data Provenance</b>                  | Data traceability and integrity verification               | Transparency, auditability, tamper detection, accountability           | Storage overhead, management complexity                         | Audit trails, regulatory compliance, forensic analysis                  |
| <b>Public Key Cryptography</b>          | Secure communication and authentication                    | Confidentiality, authentication, integrity, digital signatures         | Key management complexity, computational overhead               | Secure communication, digital signatures, user authentication           |

5. **Data Provenance:** Data provenance maintains traceability, integrity, and transparency by recording the history of data operations throughout the blockchain network. This enables effective auditing and helps detect unauthorized modifications or access (Tosh et al. 2019; Ruan et al. 2020).
6. **Public Key Cryptography:** Public key cryptography is an asymmetric cryptographic technique that employs a pair of keys (public and private) to provide secure communication, authentication, and digital signature verification. (Rivest et al. 1978; Khan 2023).

Table 7 outlines the major blockchain-based security

mechanisms, their main functions, benefits, drawbacks, and use cases. The comparison shows that each mechanism is focused on a specific aspect of cloud security, such as access control, privacy preservation, secure communication, data integrity, and decentralised trust. Smart Contracts and Consensus Mechanisms increase trust and validate transactions, whereas Attribute-Based Encryption and Homomorphic Encryption provide advanced cryptographic protection to ensure data confidentiality. Likewise, Data Provenance and Public Key Cryptography enhances the traceability, authentication and secure communication of data. Overall, these complementary mechanisms together create a multi-

layered security framework that boosts confidentiality, integrity, authentication, traceability, and trust within blockchain-empowered cloud systems.

#### 4.2.3 Popular Blockchain Frameworks

There are several blockchain frameworks that have been adopted for developing secure cloud-based applications,

each with different architectural features, consensus mechanisms, and privacy capabilities. Among the most widely discussed frameworks are Ethereum, Hyperledger Fabric, Hyperledger Besu, Quorum, and Corda.

**Table 8:** Comparison of blockchain frameworks for cloud security applications

| Blockchain Framework | Network Type          | Consensus Support                | Key Advantages                                                                    | Limitations                                                       | Primary Applications                                                                 |
|----------------------|-----------------------|----------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Ethereum             | Public                | PoS (formerly PoW)               | Large developer ecosystem, mature smart contract support, high decentralization   | Transaction fees, scalability challenges, limited privacy         | Public DApps, digital asset management, decentralised cloud services                 |
| Hyperledger Fabric   | Permissioned          | RAFT, PBFT (pluggable consensus) | High privacy, modular architecture, fine-grained access control, enterprise-ready | Complex deployment and network configuration                      | Enterprise cloud systems, healthcare, supply chain, permissioned business networks   |
| Hyperledger Besu     | Public / Permissioned | QBFT, IBFT, PoA                  | Ethereum compatibility, flexible deployment, enterprise integration               | Network configuration complexity, smaller ecosystem than Ethereum | Enterprise blockchain, secure cloud storage, consortium networks                     |
| Quorum               | Permissioned          | IBFT, RAFT                       | Enhanced privacy, high throughput, enterprise transaction management              | Limited community adoption, Ethereum dependency                   | Financial services, inter-organizational data sharing, enterprise cloud applications |
| Corda                | Permissioned          | Notary-based consensus           | High confidentiality, peer-to-peer transaction model, regulatory compliance       | Limited general-purpose smart contract ecosystem                  | Banking, finance, healthcare, business process automation                            |

While Ethereum is primarily designed for public decentralised applications, permissioned frameworks such as Hyperledger Fabric, Hyperledger Besu, Quorum, and Corda are widely preferred for enterprise cloud environments due to their enhanced privacy, controlled access, and regulatory compliance.

1. **Ethereum:** Ethereum is an open-source blockchain platform designed for developing decentralised applications (DApps). Its smart contract functionality enables automated policy enforcement, secure transactions, and access control management (Bistarelli et al. 2020; Wu et al. 2024).
2. **Hyperledger Fabric:** Hyperledger Fabric is a permissioned blockchain platform widely adopted for enterprise applications. Its modular architecture and permissioned consensus model enhance security, privacy, and scalability in cloud environments (Padmavathi et al. 2024; Nikolić et al. 2022).
3. **Hyperledger Besu:** Hyperledger Besu is an Ethereum-compatible blockchain platform developed under the Hyperledger Foundation that supports both public and permissioned blockchain networks. For cloud security applications, this framework is widely utilized to

ensure secure data transmission, fine-grained access control, and tamper-proof audit trails (Fan et al. 2022).

4. **Quorum:** Quorum is an enterprise-focused Ethereum-based blockchain platform developed by J.P. Morgan, utilized for enterprise-level applications. This framework aims to enhance privacy, security, performance, and smart contract management through its privacy manager, Tessera (Mazzoni et al. 2022; Stefanescu et al. 2022).
5. **Corda:** Corda is an enterprise blockchain platform based on a peer-to-peer transaction model, which ensures only parties involved in the transaction process will have access to the data. This framework is specifically designed to meet privacy, security, and regulatory compliance in enterprise environment (Stefanescu et al. 2022).

Table 8 compares the major blockchain frameworks based on their network type, consensus support, advantages, limitations, and application domains. The comparison shows that public frameworks such as Ethereum emphasize decentralization and transparency, whereas permissioned frameworks, including Hyperledger Fabric, Hyperledger Besu, Quorum, and Corda, prioritize privacy,

controlled access, and enterprise scalability. Consequently, permissioned blockchain platforms are more frequently adopted for cloud security applications that require regulatory compliance, secure collaboration, and efficient transaction processing. Overall, the reviewed literature indicates that VOSviewer and Biblioshiny are the predominant bibliometric tools for analyzing blockchain-enabled cloud security research. Smart contracts, Attribute-Based Encryption, Homomorphic Encryption, consensus mechanisms, data provenance, and public key cryptography represent the most frequently adopted security mechanisms, while Ethereum, Hyperledger Fabric, Hyperledger Besu, Quorum, and Corda constitute the principal blockchain frameworks for developing secure cloud-based applications. Collectively, these findings indicate that contemporary blockchain-enabled cloud security research increasingly favors permissioned blockchain frameworks integrated with advanced cryptographic and access control mechanisms to achieve secure, privacy-preserving, and scalable cloud environments.

**4.3 RQ3:** What are the key challenges, research gaps, and future research opportunities identified in this domain?

#### 4.3.1 Challenges Related to Existing Studies

Although blockchain technology has significantly improved cloud security through decentralization, transparency, and enhanced data integrity, the existing literature continues to report several technical and operational challenges that limit its large-scale adoption. The major challenges identified from the reviewed studies are summarized below.

1. **Scalability:** Scalability remains a major challenge in blockchain-enabled cloud systems, particularly when processing large transaction volumes. As the network grows, transaction throughput decreases while latency increases, limiting real-time cloud applications (Stefanescu et al. 2022; Sahraoui et al. 2025).
2. **High Resource Consumption:** Due to the high energy consumption of consensus mechanisms such as PoW, there is a growing need for energy-efficient alternatives suitable for cloud environments (Sahraoui et al. 2025; Ahmad et al. 2023).
3. **Regulatory and Legal Compliance:** In a decentralised environment, ensuring compliance related to data protection regulations is very challenging. It also creates uncertainty in adopting blockchain technology at the enterprise level (Ahmad et al. 2023).
4. **Transparency and Privacy Conflict:** Blockchain transparency can pose challenges when dealing with

sensitive data. To overcome this challenge, there is a need for a strong security mechanism to safeguard data while maintaining its integrity (Hejazi and Lashkari 2025; Guo et al. 2025).

5. **Security Risks in Smart Contracts:** Smart contracts automate the execution of security policies and access control to avoid unauthorized access. Any loophole can lead to vulnerability of sensitive information (Guo et al. 2025; Mitrea 2023).

Collectively, these challenges indicate that future blockchain-enabled cloud security solutions should balance scalability, privacy, regulatory compliance, and computational efficiency to support practical large-scale deployment.

#### 4.3.2 Research Gaps Identified Through Bibliometric Analysis

The bibliometric analysis identifies several research gaps that continue to limit the practical adoption of blockchain-enabled cloud security solutions. Although considerable progress has been made in developing decentralised security frameworks, most existing studies continue to emphasize conceptual models and simulation-based evaluations rather than large-scale real-world deployments (Tripathi et al. 2023; Dorsala et al. 2021; Ullah and Ullah 2024; Guo et al. 2022; Bhutta 2021). Challenges related to scalability, interoperability, computational overhead, and standardized integration across heterogeneous cloud environments remain insufficiently addressed, limiting the efficient deployment of blockchain-based cloud security solutions (Alghamdi et al. 2024; Xu et al. 2024; Li et al. 2024; Wahab et al. 2024).

Furthermore, limited attention has been given to regulatory compliance, privacy preservation, and the secure governance of sensitive healthcare, and enterprise data within decentralised cloud infrastructures (Li et al. 2024; Xu et al. 2024; Yang et al. 2022; Yin et al. 2024). Existing studies also provide limited discussion on secure and transparent data sharing among multiple organizational entities while ensuring privacy, fine-grained access control, traceability, and auditability (Ali 2025; Ullah and Ullah 2024; Tawfik 2025). Emerging research areas, including edge computing, AI integration, quantum-resistant cryptography, and cross-chain interoperability, remain relatively underexplored and warrant further investigation. Addressing these research gaps is essential for developing scalable, interoperable, privacy-preserving, and practically deployable blockchain-enabled cloud security solutions capable of meeting the evolving security requirements of modern cloud environments.

**Table 9:** Research challenges, identified gaps, and future directions in blockchain-enabled cloud security

| Challenge        | Identified Gap                        | Future Direction                   |
|------------------|---------------------------------------|------------------------------------|
| Scalability      | Limited real-world deployment         | Lightweight consensus and sharding |
| Privacy          | Limited privacy-preserving Mechanisms | ZKPs and Homomorphic Encryption    |
| Interoperability | Lack of standardized integration      | Cross-chain protocols              |
| Smart Contracts  | Security vulnerabilities              | Formal verification                |

|                       |                           |                            |
|-----------------------|---------------------------|----------------------------|
| Regulatory Compliance | Limited governance models | GDPR-compliant frameworks  |
| Resource Consumption  | High computational cost   | Energy-efficient consensus |

Table 9 summarizes the major challenges, research gaps, and future research directions identified from the reviewed literature. The comparison indicates that scalability, privacy, interoperability, and resource consumption remain the most persistent challenges, while practical deployment and standardized integration continue to be insufficiently explored.

#### 4.3.3 Future Research Directions

The bibliometric analysis and literature review highlight several research opportunities that can address the existing limitations of blockchain-enabled cloud security. Based on the identified research gaps and current technological challenges, the following future research directions are proposed.

1. **Lightweight Blockchain Architectures:** Cloud and distributed computing environments may operate under resource constraints, particularly in edge-assisted deployments. Future research should focus on developing lightweight blockchain architectures and optimized consensus mechanisms that provide strong security while minimizing computational and communication overhead.
2. **Privacy-Preserving Mechanisms:** With the rise in regulatory and privacy demands, incorporating an efficient privacy-preserving mechanisms with blockchain has become an emerging research area. To protect sensitive data, advanced cryptographic techniques, such as zero-knowledge proofs, homomorphic encryption, and efficient smart contracts, can be utilized along with the existing frameworks. Combining these techniques with blockchain frameworks can boost data confidentiality, fortify privacy protection, and ensure regulatory compliance in cloud environments.
3. **Smart Contract Verification & Automation:** The reliability of smart contracts is still crucial, as vulnerabilities in the logic of the contracts can result in data breaches and unauthorized access. Robustness of blockchain-enabled cloud applications can be enhanced through formal verification, secure contract design, flexible upgrades, and runtime monitoring.
4. **Real-World Deployment and Interoperability:** Despite the proliferation of blockchain-based cloud security solutions, large-scale deployment in the real world is still limited. Comparative evaluations and standardized interoperability frameworks can help bridge the gap between experimental implementations and practical cloud environments, particularly in multi-cloud and hybrid infrastructures.
5. **Scalability:** Scalability continues to be one of the most significant challenges in blockchain-enabled cloud systems. Sharding, sidechains, and off-chain storage are potential solutions that can enhance transaction latency and throughput.

6. **Compliance and Regulatory Alignment:** Compliance with evolving data protection regulations remains essential for enterprise blockchain adoption. Incorporating automated compliance verification into smart contracts can strengthen data governance, access control, and regulatory adherence.

Overall, the proposed research directions emphasize the importance of scalable, privacy-preserving, interoperable, and regulatory-compliant blockchain solutions that can operate securely in cloud environments. Solving these challenges will help to make blockchain technology more widely adopted into various Cloud Based applications.

#### 4.4 Comparative Analysis of This Study to Existing Reviews

Several prior surveys and bibliometric studies have examined blockchain technology in the context of cloud computing, cloud security, and adjacent domains. To clarify the specific contribution of the present work, Table 10 compares this study with representative prior reviews across five dimensions: methodological approach, domain focus, use of bibliometric tools, structured comparison of security mechanisms, and blockchain frameworks.

Bao et al. (Bao et al. 2024) conducted a bibliometric analysis of blockchain research broadly, applying quantitative bibliometric methods similar to those used in the present study; however, their scope encompasses blockchain research in general rather than cloud security specifically. Elhadari et al. (Elhadari et al. 2025) presented a narrative survey of blockchain adoption in Internet of Things environments, which focuses primarily on IoT applications rather than cloud security. Similarly, Alghamdi et al. (Alghamdi et al. 2024) surveyed blockchain scalability challenges across general blockchain systems, with scalability representing the primary technical focus rather than cloud security or bibliometric analysis. Ahmed (Ahmed 2025b) and Dorsala et al. (Dorsala et al. 2021) surveyed blockchain integration with cloud computing; however, both rely primarily on narrative synthesis rather than the bibliometric methodology adopted in the present study. Ullah and Ullah (Ullah and Ullah 2024) provided a comprehensive review focused specifically on blockchain for cloud security, representing the closest thematic overlap with the present study; however, their review does not employ bibliometric tools such as VOSviewer and Biblioshiny or report a systematically screened publication dataset comparable to the present analysis. Han et al. (H. Han et al. 2022), Boughdiri et al. (Boughdiri et al. 2025), and Jain et al. (Jain et al. 2025) address narrower technical sub-domains, including cloud data integrity auditing, blockchain storage scalability, and consensus algorithm scalability, respectively, rather than providing a comprehensive treatment of blockchain-based security mechanisms and framework options (Kumari P, et al 2024) (Lee SY et al. 2024).

**Table 10:** Comparative analysis of this study with existing reviews

| Reference                                | Year | Methodology                                    | Domain Focus                                           | 1 | 2 | 3 | 4 | 5 |
|------------------------------------------|------|------------------------------------------------|--------------------------------------------------------|---|---|---|---|---|
| Bao et al. (Bao et al. 2024)             | 2024 | Bibliometric analysis                          | Blockchain research (general)                          | ✓ | × | × | × | × |
| Elhadari et al. (Elhadari et al. 2025)   | 2025 | Narrative survey                               | Blockchain adoption in IoT                             | × | × | ✓ | × | × |
| Ahmed (Ahmed 2025b)                      | 2025 | Narrative survey                               | Blockchain-cloud integration (security and efficiency) | × | ✓ | P | × | × |
| Alghamdi et al. (Alghamdi et al. 2024)   | 2024 | Narrative survey                               | Blockchain scalability (general)                       | × | × | × | × | ✓ |
| Dorsala et al. (Dorsala et al. 2021)     | 2021 | Narrative survey                               | Blockchain solutions for cloud computing (general)     | × | P | P | P | × |
| Ullah and Ullah (Ullah and Ullah 2024)   | 2024 | Comprehensive review                           | Blockchain for cloud security                          | × | ✓ | ✓ | P | × |
| Han et al. (H. Han et al. 2022)          | 2022 | Narrative survey                               | Cloud data integrity auditing (narrow)                 | × | P | P | × | × |
| Boughdiri et al. (Boughdiri et al. 2025) | 2025 | Systematic literature review (SLR)             | Blockchain storage scalability (narrow)                | × | × | × | ✓ | ✓ |
| Jain et al. (Jain et al. 2025)           | 2025 | Narrative survey                               | Consensus algorithm scalability (narrow)               | × | × | P | × | × |
| This Study                               | 2026 | PRISMA-guided bibliometric + structured review | Blockchain-enabled cloud security (comprehensive)      | ✓ | ✓ | ✓ | ✓ | ✓ |

**Note:** (1) Bibliometric/Quantitative Analysis Tools (e.g., VOSviewer, Biblioshiny); (2) Cloud-Security-Specific Domain Focus; (3) Comprehensive Comparison of Security Mechanisms; (4) Structured Comparison of Blockchain Frameworks; (5) PRISMA or Equivalent Systematic Screening Protocol; ✓ = Addressed; P = Partially Addressed; × = Not addressed.

Among the representative reviews examined in Table X, no study combines (i) a PRISMA-guided systematic screening process, (ii) the combined use of Biblioshiny and VOSviewer, (iii) a structured comparison of different blockchain-based security mechanisms, and (iv) a structured comparison of various blockchain frameworks within a cloud-security-specific domain scope. This combination distinguishes the present work methodologically from narrative reviews such as (Ahmed 2025b), (Dorsala et al. 2021), and (Ullah and Ullah 2024), and in terms of scope and analytical coverage from broader or narrower studies such as (Bao et al. 2024), (Elhadari et al. 2025), (Alghamdi et al. 2024), (H. Han et al. 2022), (Boughdiri et al. 2025), and (Jain et al. 2025).

## 5 CONCLUSION

This study presents a comprehensive bibliometric and technical analysis of blockchain-enabled cloud security research based on Scopus-indexed publications. The findings reveal sustained growth in research activity and identify blockchain, cloud security, cloud computing, data privacy, cryptography, access control, and smart contracts as dominant research themes. The review further shows

that Smart Contracts, Attribute-Based Encryption, Homomorphic Encryption, Consensus Mechanisms, Data Provenance, and Public Key Cryptography provide complementary approaches to strengthening cloud security. Among the major blockchain frameworks discussed in the reviewed literature, Hyperledger Fabric, Hyperledger Besu, Ethereum, Quorum, and Corda demonstrate diverse capabilities, with permissioned architectures being particularly relevant to enterprise environments requiring controlled access and enhanced privacy. Despite these developments, scalability, interoperability, computational overhead, regulatory compliance, and practical deployment remain important challenges. Emerging opportunities include lightweight blockchain architectures, privacy-preserving computation, cross-chain interoperability, AI integration, and secure smart contract verification. Overall, this study provides an integrated view of the research landscape, technical approaches, major challenges, and emerging directions in blockchain-enabled cloud security, thereby supporting the development of scalable, privacy-preserving, and practically deployable solutions.

## REFERENCES

Agbeyangi, A. O., O. A. Oki, and A. Mgidi. 2024. "Blockchain in Healthcare: Implementing Hyperledger Fabric for Electronic Health Records at Frere Provincial Hospital." *Proceedings of the 45th Conference of the South African Institute of Computer Scientists and Information Technologists (SAICSIT)*, July, 93–106.

- Ahmad, H., L. Campanile, M. Iacono, F. Marulli, and M. Mastroianni. 2023. "GDPR Compliance Verification Through a User-Centric Blockchain Approach in a Multi-Cloud Environment." *Computers & Electrical Engineering* 110: 108905.
- Ahmed, W. 2025a. "Blockchain Integration in Modern Cloud Computing." *Engineering and Technology Journal* 25 (7): 711–28. <https://doi.org/10.1016/j.etj.2025.09.001>.
- Ahmed, W. 2025b. "Blockchain Integration in Modern Cloud Computing: A Comprehensive Survey of Security and Efficiency." *Premier Journal of Data Science* 2 (September): 711–28. <https://doi.org/10.70389/PJDS.100003>.
- Alghamdi, T. A., A. A. Sheikh, M. Alsaed, and K. Alsubhi. 2024. "A Survey of Blockchain Based Systems: Scalability Issues and Solutions." *IEEE Access* 12 (June): 78920–52. <https://doi.org/10.1109/ACCESS.2024.3409876>.
- Ali, A. A. 2025. "Securing Electronic Health Records Using Blockchain-Enabled Federated Learning for IoT-Based Smart Healthcare." *Smart Health* 25 (May): 100321. <https://doi.org/10.1016/j.smhl.2025.100321>.
- Ali, M., S. U. Khan, and A. V. Vasilakos. 2015. "Security in Cloud Computing: Opportunities and Challenges." *Information Sciences* 305 (June): 357–83. <https://doi.org/10.1016/j.ins.2015.01.025>.
- Aria, M., and C. Cuccurullo. 2017. "Bibliometrix: An r-Tool for Comprehensive Science Mapping Analysis." *Journal of Informetrics* 11 (4): 959–75. <https://doi.org/10.1016/j.joi.2017.08.007>.
- Bao, L., J. Yang, X. Yang, and C. Rong. 2024. "Bibliometric Analysis of Scientific Publications on Blockchain Research and Applications." *IEEE Access* 12: 15432–51.
- Bhutta, M. N. M. 2021. "A Survey on Blockchain Technology." *IEEE Access* 9: 61072–97.
- Bistarelli, S., M. Falcone, and E. Ranieri. 2020. "Ethereum Smart Contracts: Analysis and Statistics of Their Source Code." *Blockchain: Research and Applications* 1 (2): 100011.
- Boughdiri, M., I. Amous, and A. Seba. 2025. "A Systematic Literature Review on Blockchain Storage Scalability: Issues and Solutions." *IEEE Access* 13 (January): 12450–75. <https://doi.org/10.1109/ACCESS.2025.3351234>.
- Chakraverti, A. K. 2025. "Enhancing Healthcare System for Patient Data with HEO-PRAFT Consensus Mechanism Using SPS Authentication Based EPRSS Encryption." *Biomedical Signal Processing and Control* 102 (March): 106746. <https://doi.org/10.1016/j.bspc.2025.106746>.
- Dorsala, M. R., V. K. Gudavalli, D. S. Dhabale, and S. S. Kumar. 2021. "Blockchain-Based Solutions for Cloud Computing: A Survey." *Journal of Network and Computer Applications* 194 (November): 103227. <https://doi.org/10.1016/j.jnca.2021.103227>.
- Dou, M., Q. Zhang, and X. Wang. 2025. "A Secure Medical Information Framework Integrating Attribute-Based Signcryption with Blockchain Mechanisms." *Scientific Reports* 15 (April): 11082. <https://doi.org/10.1038/s41598-025-01082-x>.
- Du, Q. 2024. "Protocol for Conducting Bibliometric Analysis in Biomedicine and Related Research Using CiteSpace and VOSviewer Software." *STAR Protocols* 5 (2): 104349.
- Dubovitskaya, A. 2020. "ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care." *Journal of Medical Internet Research* 22 (8): e13598. <https://doi.org/10.2196/13598>.
- Eck, N. J. van, and L. Waltman. 2010. "Visualizing Bibliometric Networks." *Studies in the History and Philosophy of Science* 45 (4): 1–12.
- Elhadari, Zouhair, Hicham Zougagh, Nouredine Idboufker, and Mohamed Ech-chebaby. 2025. "Survey on the Adoption of Blockchain Technology in Internet of Things Environments: Techniques, Challenges and Future Research Directions." *IAENG International Journal of Computer Science* 52 (1).
- Fan, C., C.-Y. Lin, H. Khazaei, and P. Musilek. 2022. "Performance Analysis of Hyperledger Besu in Private Blockchain." *Proceedings of the IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)*, 64–73.
- Guo, H., J. Yu, and P. Liu. 2022. "A Survey on Blockchain Technology and Its Security." *Journal of Information Security and Applications* 67: 103144.
- Guo, Z., C. Yang, Y. Guo, and R. Wang. 2025. "Blockchain-Enhanced Smart Contracts for Formal Verification of IoT Access Control Mechanisms." *Applied Intelligence* 55 (2): 1234–52.
- Han, H., M. Huang, Y. Zhang, and W. Yang. 2022. "A Survey on Blockchain-Based Integrity Auditing for Cloud Data." *Digital Communications and Networks* 8 (5): 618–32. <https://doi.org/10.1016/j.dcan.2022.05.014>.
- Han, Y., Y. Zhang, and S. H. Vermund. 2022. "Blockchain Technology for Electronic Health Records." *International Journal of Environmental Research and Public Health* 19 (23): 15577. <https://doi.org/10.3390/ijerph192315577>.
- Hejazi, N., and A. Habibi Lashkari. 2025. "A Comprehensive Survey of Smart Contract Vulnerability Detection Tools: Techniques and Methodologies." *Journal of Network and Computer Applications* 231: 104087.
- Islam, S. S., M. S. Hossain, and M. M. Islam. 2021. "Smart Contract Development and Security Challenges in

- Blockchain: A Review." *IEEE Transactions on Knowledge and Data Engineering* 33 (5): 1992–2005.
- Jain, A. K., A. Sahoo, and P. K. Jena. 2025. "A Survey on Scalable Consensus Algorithms for Blockchain Networks." *Blockchain: Research and Applications* 6 (1): 100179. <https://doi.org/10.1016/j.bcra.2024.100179>.
- Khan, M. A., A. S. Salah, and F. Ahmed. 2024. "Blockchain for Secure and Decentralized Artificial Intelligence in Cybersecurity." *Internet of Things and Cyber-Physical Systems* 4: 170–79. <https://doi.org/10.1016/j.iotcps.2024.01.003>.
- Khan, M. R. 2023. "Analysis of Elliptic Curve Cryptography and RSA." *IEEE Access* 11: 116271–86.
- Kumar, G. S., K. Premalatha, G. U. Maheshwari, and P. R. Kanna. 2024. "No More Privacy Concern: A Privacy-Chain Based Homomorphic Encryption Scheme for Sensitive Data Protection." *Expert Systems with Applications* 240: 122532.
- Kumari P, Singh M. Blockchain-Based Distributed Data Security and Trust Management System for Cloud Computing. Library Progress International. 2024;44(3).
- Kumar, R., S. Kumar, A. Gandomi, and P. Mishra. 2022. "Blockchain and Homomorphic Encryption-Based Privacy-Preserving Federated Learning for COVID-19 Detection in Chest x-Ray Images." *Internet of Things* 20: 100607.
- Li, L., Y. Su, X. Zhang, and H. Li. 2024. "Blockchain-Enabled Decentralized Storage with Reliable Deduplication and Storage Equilibrium." *IEEE Transactions on Network Science and Engineering* 11 (3): 1456–72. <https://doi.org/10.1109/TNSE.2024.3401234>.
- Lee SY. Blockchain-Based Cloud Security Management System for Hospital. Library Progress International. 2024;44(2):180–190.
- Li, Y., G. Zhang, X. Wang, and H. Yu. 2021. "Attribute-Based Encryption with Flexible Access Policy for Cloud Storage." *IEEE Transactions on Cloud Computing* 9 (4): 1198–210. <https://doi.org/10.1109/TCC.2019.2929197>.
- Mazzoni, M., S. Ranise, and M. Pradella. 2022. "Performance Evaluation of Permissioned Blockchains for Financial Applications: The ConsenSys Quorum Case Study." *Blockchain: Research and Applications* 3 (1): 100026.
- Mitrea, D. 2023. "Smart Contracts and Homomorphic Encryption for Private P2P Electricity Trading and Demand Response." *Energies* 16 (24): 8031.
- Muneshwara, M., P. Kaur, A. Pandey, and R. Singh. 2023. "A Novel Consensus Algorithm for Blockchain IoT Prototype in Health Care System." *International Journal of Intelligent Systems and Applications in Engineering* 12 (2): 236–49.
- Nikolić, S., N. Zdravković, I. Franc, and N. Arivazhagan. 2022. "A Comparison of Hyperledger Consensus Mechanisms and Their Security Properties." *Proceedings of the International Conference on Business Information Security (BISEC)*.
- Padmavathi, U., K. Sharma, R. Singh, and A. Kumar. 2024. "Examining Architectural Aspects of Hyperledger Fabric." *IEEE Transactions on Cloud Computing* 12 (4): 2156–70.
- Pham, Xuan-Lam, and Thi Thu Le. 2024. "Bibliometric Analysis and Systematic Review of Research on Expert Finding: A PRISMA-Guided Approach." *International Arab Journal of Information Technology* 21 (6): 663–75.
- Rahman, N. T. 2024. "Enhancing Health-Care Security: The Role of Blockchain and Consensus Mechanisms." *Advances in Internet of Healthcare* 1 (2): 29–47. <https://doi.org/10.36922/aih.2580>.
- Rivest, R. L., A. Shamir, and L. Adleman. 1978. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." *Communications of the ACM* 21 (2): 120–26. <https://doi.org/10.1145/359340.359342>.
- Ruan, P., G. Loghin, M. Saxena, E. Ooi, and B. Tan. 2020. "Fine-Grained, Secure and Efficient Data Provenance on Blockchain." *Proceedings of the VLDB Conference*, 975–88.
- Sahraoui, S., M. Dabbagh, and A. Sharma. 2025. "Lightweight Consensus Mechanisms in the Internet of Blockchain Things: Analysis and Research Directions." *Digital Communications and Networks* 11 (2): 1–18.
- Sharma, P., R. Jindal, and M. D. Borah. 2021. "Blockchain-Based Decentralized Architecture for Cloud Storage System." *Journal of Information Security and Applications* 62 (November): 102970. <https://doi.org/10.1016/j.jisa.2021.102970>.
- Shi, S., D. He, L. Wang, and M. K. Khan. 2020. "Applications of Blockchain in Ensuring the Security and Privacy of Electronic Health Record Systems: A Survey." *Computers & Security* 97 (October): 101966. <https://doi.org/10.1016/j.cose.2020.101966>.
- Singh, A., and K. Chatterjee. 2017. "Cloud Security Issues and Challenges: A Survey." *Journal of Network and Computer Applications* 79 (February): 88–115. <https://doi.org/10.1016/j.jnca.2016.11.027>.
- Stefanescu, A., M. Rughinis, and A. Deaconu. 2022. "A Systematic Literature Review of Lightweight Blockchain for Internet of Things." *IEEE Access* 10: 61234–56.
- Subramanian, N., and A. Jeyaraj. 2018. "Recent Security Challenges in Cloud Computing." *Computers & Electrical Engineering* 71 (October): 28–42. <https://doi.org/10.1016/j.compeleceng.2018.06.006>.
- Tanwar, S., K. Parekh, and R. Evans. 2020. "Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications." *Journal of Information*

- Security and Applications* 50 (February): 102407. <https://doi.org/10.1016/j.jisa.2019.11.001>.
- Tawfik, A. M. 2025. "ACHealthChain Blockchain Framework for Access Control and Privacy Preservation in Healthcare." *Scientific Reports* 15 (May): 10757. <https://doi.org/10.1038/s41598-025-00757-1>.
- Tolmach, P., Y. Li, S. W. Lin, Y. Liu, and Z. Li. 2021. "A Survey of Smart Contract Formal Specification and Verification." *ACM Computing Surveys* 54 (7): 133.
- Tosh, D., S. Shetty, X. Liang, C. Kamhoua, and L. Njilla. 2019. "Towards Assured Data Provenance in Blockchain Integrated Cloud." *IEEE Consumer Electronics Magazine* 8 (2): 40–47.
- Tripathi, G., M. A. Ahad, and S. Paiva. 2023. "A Comprehensive Review of Blockchain Technology: Underlying Principles and Historical Background with Future Challenges." *Decision Analytics Journal* 9 (December): 100344. <https://doi.org/10.1016/j.dajour.2023.100344>.
- Ullah, F., M. A. Rahim, M. Khan, A. Naeem, and S. Y. Amjad. 2024. "Blockchain-Enabled EHR Access Auditing: Immutable Audit Trails for Data Security." *Heliyon* 10 (15): e35122. <https://doi.org/10.1016/j.heliyon.2024.e35122>.
- Ullah, L., and F. Ullah. 2024. "Blockchain Technology for Cloud Security: A Comprehensive Review." *Journal of Computer Fraud & Security* 2024 (3): 1–15.
- Verma, A., P. Kumar, and R. Singh. 2025. "A Framework for Secured Access Control of Cloud Data Using Blockchain Technology." *Journal of Information Systems and Emerging Markets* 18 (2): 115–32. <https://doi.org/10.1016/j.jisem.2025.03.001>.
- Vinayasree, P., S. Chakraborty, and V. Kumar. 2024. "A Scalable and Secure Blockchain-Based Healthcare Data Management with Practical Byzantine Fault Tolerance." *Journal of Applied Information Technology* 102 (22): 1–15. <https://doi.org/10.18280/jait.102022>.
- Wahab, N. H. A., Z. Dayong, J. N. Fadila, and K. Y. Wong. 2024. "Advances in Consortium Chain Scalability: A Review of the Practical Byzantine Fault Tolerance Consensus Algorithm." *International Journal of Advanced Computer Science and Applications* 15 (7): 977–88.
- Wu, G., H. Wang, X. Lai, M. Wang, D. He, and S. Chan. 2024. "A Comprehensive Survey of Smart Contract Security: State of the Art and Research Directions." *Journal of Network and Computer Applications* 230: 103754.
- Xu, C., J. Wang, and Z. Liu. 2024. "A Privacy-Preserving and Redactable Healthcare Blockchain System." *IEEE Transactions on Services Computing* 17 (2): 456–71. <https://doi.org/10.1109/TSC.2024.3401234>.
- Yang, Y., L. Wang, J. Zhang, and Z. Liu. 2022. "A Revocable Attribute-Based Encryption EHR Sharing Scheme with Blockchain for Multiple Authorities." *Nano Biomedicine and Engineering* 14 (3): 242–59. <https://doi.org/10.5101/nbe.v14i3.p242-259>.
- Yang, Y., J. Zhang, L. Wang, and Z. Liu. 2021. "Protecting Personal Sensitive Data Security in the Cloud with Blockchain." *Computers & Security* 97 (October): 101946. <https://doi.org/10.1016/j.cose.2020.101946>.
- Yin, H., Y. Zhao, L. Zhang, and W. Lu. 2024. "Attribute-Based Searchable Encryption with Decentralized Access Control for Blockchain-Based Healthcare." *Information Systems* 126: 102324.
- Yousuf, H., H. N. Siddiqui, A. Ashraf, and U. Rajput. 2021. "Systematic Review on Fully Homomorphic Encryption Scheme and Its Applications." *Information Systems Frontiers* 23 (5): 1121–40.
- Zaeem, R. Nokhbeh, and J. Bardzell. 2021. "Blockchain-Based Self-Sovereign Identity: A Survey." *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*.
- Zuo, Y., H. Xu, X. Liu, and J. Zhang. 2024. "Secure and Efficient Blockchain-Based Access Control Scheme with Attribute Update." *IEEE Transactions on Dependable and Secure Computing* 21 (6): 2945–60.