https://doi.org/10.58086/py0e-1y49

INTEGRATION OF AES AND BLOCKCHAIN FOR SENSITIVE DATA PROTECTION: A BIBLIOMETRIC ANALYSIS

Filipe Gomes[1]✉, **Mário Dias Lousã**[1,2], **José Carlos Morais**[1,3]

[1] Instituto Superior Politécnico Gaya (ISPGAYA), Portugal.
[2] Insight - Piaget Research Center for Ecological Human Developement, Portugal.
[3] CEOS.PP, ISCAP, Polytechnic of Porto, Portugal.
✉ Corresponding authors**:** ispg2021103030@ispgaya.pt

Abstract

The protection of sensitive data is becoming increasingly complex as digital services expand, connected devices multiply, and distributed systems become the norm. Encryption methods such as the Advanced Encryption Standard (AES) remain fundamental to ensuring the confidentiality of information, but they do not meet all security requirements. At the same time, blockchain technology has been adopted in various contexts for its ability to ensure integrity, traceability, and non-repudiation. Despite the complementary nature of these technologies, studies analyzing their combined use remain relatively scarce and fragmented. This article analyses existing research on the combined use of blockchain and encryption through a bibliometric analysis of scientific publications indexed in The Lens database between 2016 and 2026. The study is based on descriptive indicators and keyword co-occurrence analysis, using the VOSviewer tool to identify thematic relationships and research trends. Results show significant growth from 2020, with major contributions from Asia and increasing interest across multiple disciplinary areas. Most publications are situated within computer science and cybersecurity, while applied research is primarily focused on domains such as healthcare and Internet of Things (IoT) systems. Despite this expansion, the literature remains largely fragmented, with relatively few studies proposing or experimentally evaluating integrated architectures that effectively combine encryption and blockchain mechanisms to simultaneously ensure data confidentiality, integrity, and auditability.

Keywords: Data Security; Encryption; Confidentiality; Bibliometric Analysis.

1. Introduction

The protection of sensitive data has become a major information security challenge in an era marked by the digitization of services, the proliferation of connected devices, and the growing reliance on cloud infrastructures. Organizations across different sectors store and process ever-increasing volumes of sensitive information, ranging from personal and clinical data to financial records, thereby amplifying the impact of potential information leaks, data tampering, and unauthorized access (Mubeena & Jawahar, 2025).

In this context, classical cryptographic mechanisms, particularly symmetric encryption based on the Advanced Encryption Standard (AES), continue to play a central role in ensuring data confidentiality, both at rest and in transit (Stallings, 2017). In parallel, blockchain technology has emerged as a promising paradigm for guaranteeing integrity, traceability, and non-repudiation in distributed environments (Li et al., 2020). Originally associated with cryptocurrencies, blockchain has evolved into a generalized mechanism for immutable record-keeping, supporting smart contracts, operational auditing, and event logging across multiple domains, including healthcare, supply chains, the Internet of Things (IoT), and industrial environments (Taylor et al., 2020; Wylde, 2022).

The ability of blockchain to maintain a verifiable and tamper-resistant history naturally complements the confidentiality properties provided by encryption, paving the way for hybrid architectures that combine AES and blockchain technologies for comprehensive sensitive data protection (Casino et al., 2019). Despite this potential, scientific production in this area remains fragmented, with studies focusing on encryption or blockchain in isolation, rather than their integration (Hidayat & Mahardiko, 2024).

Research addressing IoT systems, smart contracts, or healthcare applications often employs both symmetric encryption and blockchain registries. However, such studies do not always explicitly discuss threat models, architectural design choices, or trade-offs between performance, scalability, and security (Yeboah-Ofori et al., 2023). This dispersion hinders the development of a consolidated view of the state of the art concerning the integration of encryption and blockchain for data protection.

Within this scenario, a bibliometric review provides a suitable tool for mapping and understanding the evolution of research in this field. By analyzing scientific output published between 2016 and 2026, it becomes possible to identify temporal trends, influential authors and institutions, predominant scientific areas, and the conceptual clusters that structure the

literature, such as combinations of blockchain, data security, confidentiality, integrity, IoT, and cloud computing. At the same time, bibliometric analysis enables the identification of structural gaps, including the limited number of studies explicitly addressing AES–blockchain hybrid architectures, the lack of systematic empirical evaluations, and the predominance of theoretical approaches over practical validation (Katoon & Turukmane, 2025).

Accordingly, this article aims to characterize the scientific landscape surrounding the joint use of blockchain and encryption mechanisms for sensitive data protection, using bibliometric techniques to analyze the evolution of research output, major contributions, and emerging thematic relationships within the literature (van Eck & Waltman, 2010). In doing so, it seeks to summarize the state of the art, identify opportunities for future research, and support the development of technical solutions that coherently exploit the complementary confidentiality and integrity properties offered by AES and blockchain technologies.

2. Research Questions

This bibliometric review seeks to map and analyze the scientific landscape regarding the combined use of encryption technologies, in particular AES, and immutable blockchain-based registration mechanisms for the protection of sensitive data. In this regard, five research questions were defined to guide the entire study:

RQ1: How did scientific output on blockchain and encryption applied to data security evolve between 2016 and 2026?

RQ2: Which authors, institutions, and countries have the greatest influence in the field of blockchain, encryption, and data protection integration?

RQ3: What themes, concepts, and areas of application structure exist in literature, according to the analysis of keywords and thematic clusters?

RQ4: What structural gaps exist in current research on data security that combines confidentiality (AES) and integrity (blockchain)?

RQ5: How do the findings identify gaps in hybrid AES-blockchain architectures?

3. Bibliometric Methodology

3.1. Databases Used

This bibliometric review was conducted using The Lens platform, one of the largest open access scientific databases, which integrates content from sources such as CrossRef, PubMed, Microsoft Academic Graph, and institutional repositories. This database was chosen due to its comprehensiveness, continuous updating of its portfolio, and structured metadata export capability, which are essential for creating reliable bibliometric analyses.

In addition, The Lens allows filtering by document type, scientific area, publication dates, and keywords, ensuring a transparent and replicable data collection process. These features are in line with the best practices recommended in literature for open science and applied bibliometrics studies.

3.2. Research Strategy

The search strategy was designed systematically, ensuring the collection of publications directly related to the topics of blockchain, encryption, confidentiality, integrity, and protection of sensitive data. To this end, Boolean operators and specific terms representing the core concepts of the study were combined. After several exploratory iterations, the final query adopted on The Lens platform was:

("data security" OR "confidentiality" OR "encryption" OR "AES")
AND
("blockchain" OR "smart contract" OR "immutable ledger")

This query allowed for a balanced coverage of scientific production discussing cryptographic mechanisms, immutable records, and hybrid security approaches. The use of combinations with OR ensured the inclusion of terminological variants, while the AND operator ensured that only articles dealing with both dimensions of the study were considered.

- Time period: 2016–2026.
- Document types: journal articles, conference papers, and book chapters.
- Language: no restrictions.
- Subject areas: Technology, Computer Science, Security, Cryptography.

The formulation of the query and the iterative refinement process followed good methodological practices recommended in the bibliometrics literature, which emphasize the need to test different semantic combinations and evaluate the consistency of the results before consolidating the final version of the research (Aria & Cuccurullo, 2017).

3.3 Data collection and study selection (PRISMA-informed)

A PRISMA-informed workflow was adopted to ensure transparency and replicability in the data collection and study selection process for this bibliometric review. The initial search was conducted in the "The Lens" database using the predefined query, resulting in a total of 3,812 records. After the removal of 55 duplicate records, 3,757 publications remained and were screened based on titles and abstracts.

During the screening phase, 3,397 publications were excluded for not meeting the predefined inclusion criteria. As all remaining records were accessible and aligned with the scope of the study, a final dataset of 360 publications was included in the bibliometric analysis.

This dataset constituted the basis for all subsequent descriptive and network-based analyses, including publication trends, authorship patterns, geographical distribution, and keyword co-occurrence mapping. The complete study selection process is summarized in Figure 1.

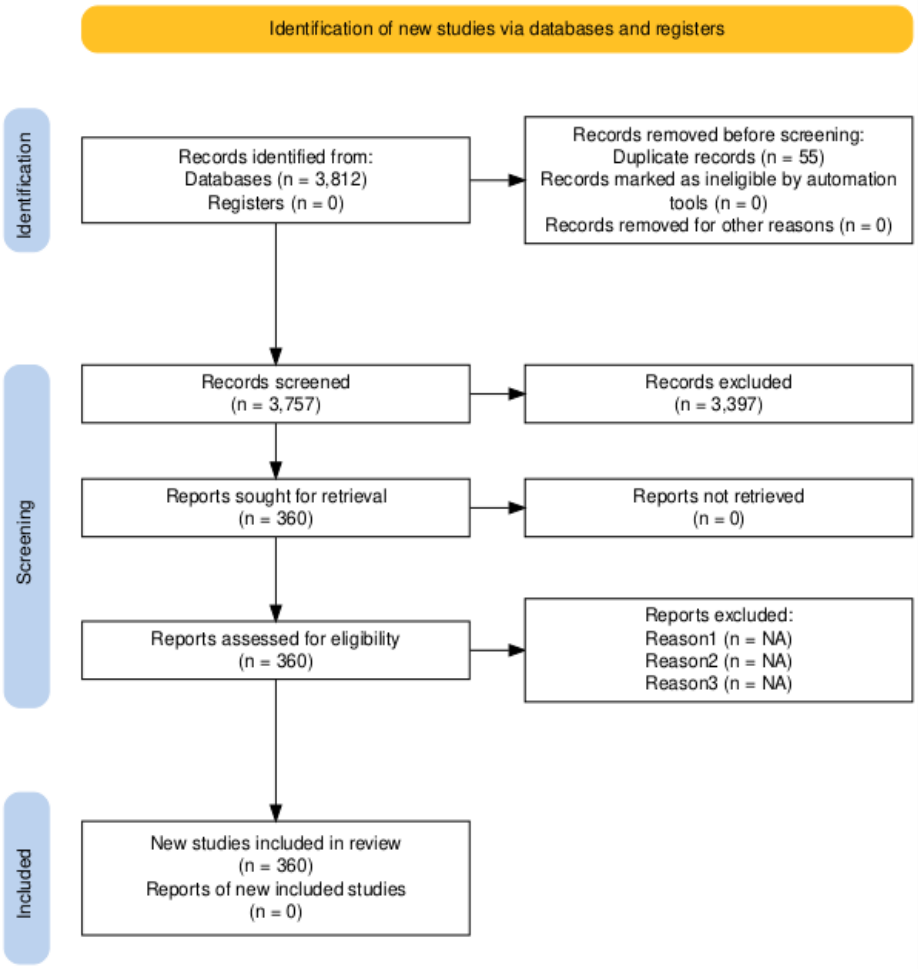

Fig 1. PRISMA-informed workflow of the bibliometric study selection process
Source: Authors' elaboration based on PRISMA statement (no date).

3.4. Inclusion and Exclusion Criteria

The selection of publications followed criteria defined to ensure that the corpus analyzed was consistent with the objective of the review, focusing on the intersection between blockchain, encryption, and sensitive data security. Thus, all studies that explicitly addressed information protection mechanisms, hybrid architecture models, practical applications in distributed environments, or analyses of technologies that combine confidentiality (e.g., through AES) with integrity mechanisms based on immutable records were included.

Work applied in areas such as IoT, cloud computing, or digital health was also considered, provided that the use of blockchain and encryption was clearly related to data security requirements. Only peer-reviewed publications, journal articles, conference papers, and book chapters, were included, ensuring a minimum level of scientific rigor. The period was limited

to 2016–2026, corresponding to the phase of greatest expansion and maturation of approaches that integrate blockchain into information security contexts.

On the other hand, publications whose focus was not directly related to data protection were excluded. These include studies devoted exclusively to cryptocurrencies or financial aspects of blockchain, purely mathematical works on cryptographic algorithms with no practical application, and research focused solely on communication networks or protocols with no connection to the integrity or confidentiality of stored data. Documents that were not peer-reviewed, duplicates, or lacking methodological rigor were also excluded.

The adoption of these criteria ensured a consistent, transparent selection process aligned with international best practices for systematic and bibliometric reviews, which recommend explicit and replicable procedures for filtering literature.

3.5. Analysis Procedures

The bibliometric analysis was carried out in several complementary stages to comprehensively characterize the scientific landscape corresponding to the intersection between blockchain, encryption, and data security. After extracting the records from The Lens platform, the metadata was organized and processed using counting, mapping, and network visualization techniques.

Initially, a descriptive analysis was carried out, including the annual count of publications, the identification of the most productive authors, the institutions with the highest volume of contributions, and the geographical distribution of research. These metrics provided an understanding of the temporal evolution of the domain and mapped the main centers of scientific production.

Next, keyword co-occurrence analysis was performed using VOSviewer software, widely recognized in the literature for its ability to generate network maps and thematic clusters from relevant terms. This tool made it possible to identify the central topics, the relationships between concepts such as blockchain, data security, encryption, integrity, and IoT, and the main thematic nuclei that structure the area of study.

Conceptual proximity relationships were also examined through clusters automatically generated by VOSviewer. This analysis made it possible to identify emerging themes, consolidated areas, and possible links between subdomains.

This set of procedures follows established practices in bibliometric studies, which recommend combining descriptive analyses and network mapping to provide an integrated and in-depth reading of scientific output.

4. Results

4.1. RQ1 — Evolution of Scientific Production

Analysis of scientific output over the period considered reveals a clear upward trend in research relating to blockchain, encryption, and data security. In the early years of the time series, the relatively low volume of publications indicates that the topic was still in an emerging phase, often associated with exploratory studies or narrowly focused applications. From around 2020 onwards, a sharp increase in the number of publications per year is observed, accompanying the maturation of blockchain technology, its adoption beyond cryptocurrency-related contexts, and the strengthening of data protection requirements in sectors such as healthcare, industry, and cloud computing. This growth peaks between approximately 2021 and 2023, suggesting a shift toward studies that explicitly consider the combined use of encryption - particularly AES - and blockchain-supported integrity and auditability mechanisms. In recent years, a slight stabilization in publication volume can be observed. Rather than indicating a decline in relevance, this pattern suggests a consolidation phase, in which research diversifies into more specialized application domains, such as IoT, e-health, and Industry 4.0.

Figure 2 illustrates the annual evolution of scientific production on blockchain, encryption, and data security (2016–2026).

Overall, these results confirm that this is a relatively recent field that has expanded rapidly over the last decade.

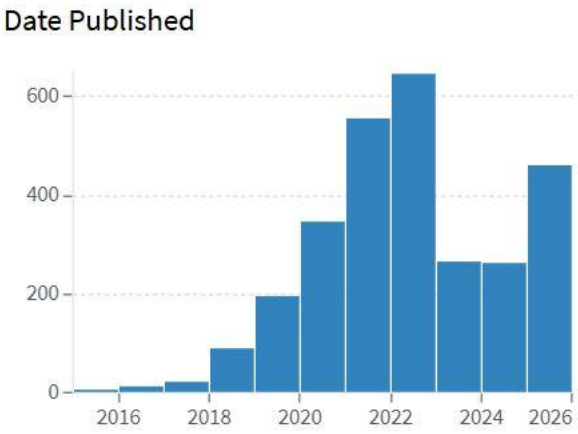

Fig 2. Annual evolution of scientific production on blockchain, encryption, and data security (2016–2026)
Source: The Lens.

4.2. RQ2 — Influential Authors, Institutions, and Countries

The analysis of authorship metrics identifies the researchers who have contributed most consistently to scientific output in the field of data security supported by blockchain and encryption. Authors such as Abdullah M. Almuhaideb, Madhusanka Liyanage, Abdelwahed Motwakel, Abdul Razzaq, and Abdullah Lakhan stand out in terms of publication volume, with contributions focusing on distributed security, blockchain-based IoT systems, authentication mechanisms, data auditing, and sensitive information protection (Figure 3).

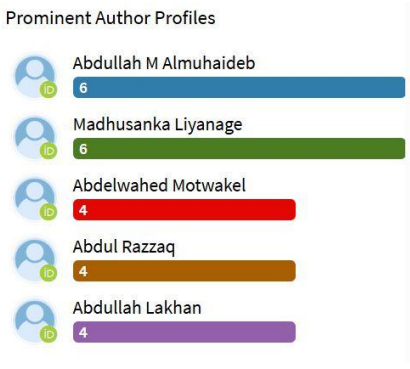

Fig 3. Authors with the highest number of publications in the analyzed field
Source: The Lens database (2025).

Scientific production is distributed across universities, research centers, and technological institutes with strong backgrounds in information security and distributed systems. Asian countries, particularly China, India, and Pakistan, account for a substantial share of

publications (figure 4), reflecting broader trends in blockchain and cybersecurity research driven by rapid digitalization and applied technological development.

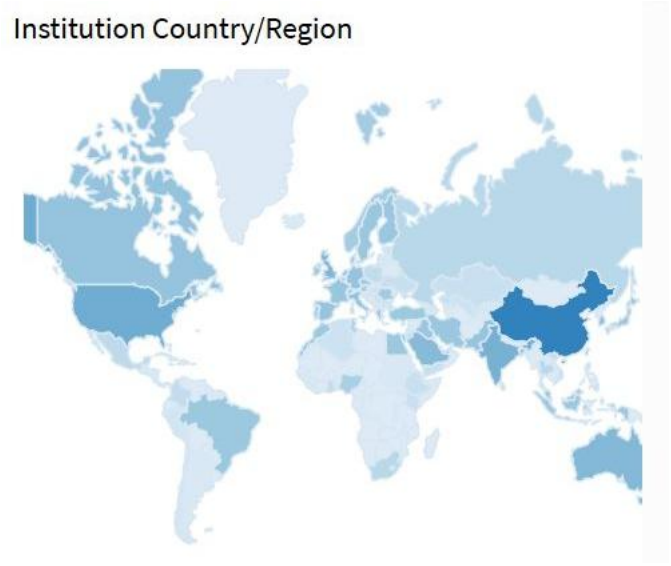

Fig 4. Geographical distribution of scientific output (2016–2026)
Source: The Lens database (2025).

Other countries, including the United States, the United Kingdom, and several European nations, contribute at a lower but consistent level, indicating that research on blockchain-based data security is globally distributed rather than regionally concentrated.

4.3. RQ3 — Scientific Areas and Document Types

Analysis of the scientific areas associated with the publications shows that research on blockchain and encryption applied to data security is highly multidisciplinary, although predominantly focused on computer science and technology. The data reveals that most articles fall within the fields of Computer Science, Cybersecurity, Cryptography, and Information Systems, reflecting the technical nature of the domain studied (Figure 5). These fields cover topics such as cryptographic mechanisms, distributed ledgers, secure architecture, authentication, data integrity, and intelligent systems.

In addition, complementary areas such as Electronic Engineering, Telecommunications, Artificial Intelligence, and IoT Systems are emerging, highlighting the breadth of practical applications in which blockchain and encryption are used to mitigate risks associated with the storage, transmission, and processing of sensitive data. The presence of these areas

indicates that the technology has been applied in network infrastructures as well as distributed devices, industrial environments, and emerging computing platforms.

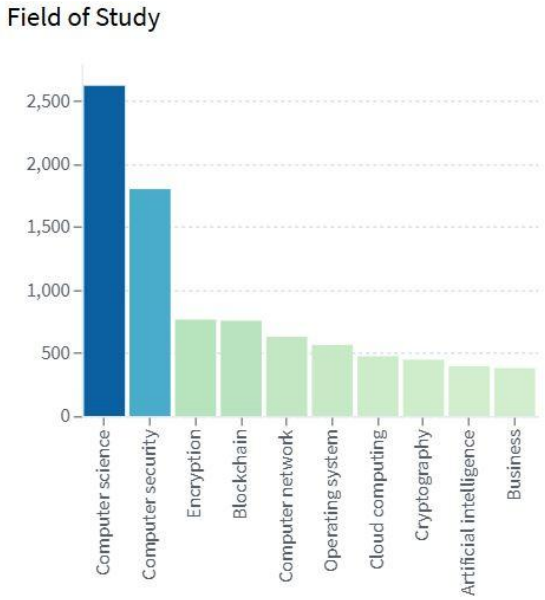

Fig 5. Scientific areas associated with the publications analyzed
Source: The Lens database (2025).

Regarding the type of document (Figure 6), most publications are articles in scientific journals, which highlight the high academic rigor and maturity of scientific production in this field. These are followed by conference papers, which continue to play an important role in technological areas due to the rapid pace of innovation and the need for rapid dissemination of results. Book chapters represent a smaller proportion but contribute to theoretical consolidation and in-depth discussion of specific topics.

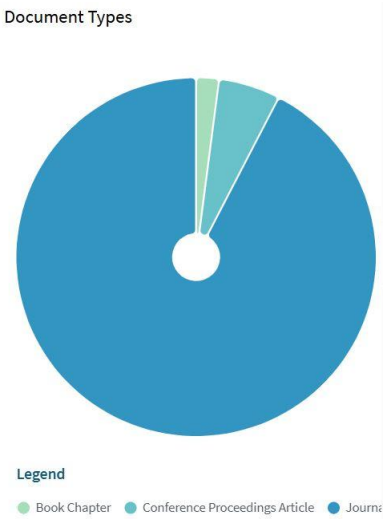

Fig 6. Distribution by document type (2016–2026)
Source: The Lens database (2025).

This diversity reflects the evolving and application-driven nature of the field. This variety reinforces the relevance of a bibliometric approach that allows for an integrated understanding of the different dimensions and contexts in which blockchain, and encryption are explored to enhance the security of sensitive data.

4.4. RQ4 — Conceptual Clusters (VOSviewer)

The co-occurrence analysis of keywords (Figure 7), performed using VOSviewer software, enabled the identification of the conceptual structure of the literature and the main themes that organize research in the field of data security supported by blockchain and encryption. This analysis resulted in three well-defined thematic clusters, reflecting distinct research orientations.

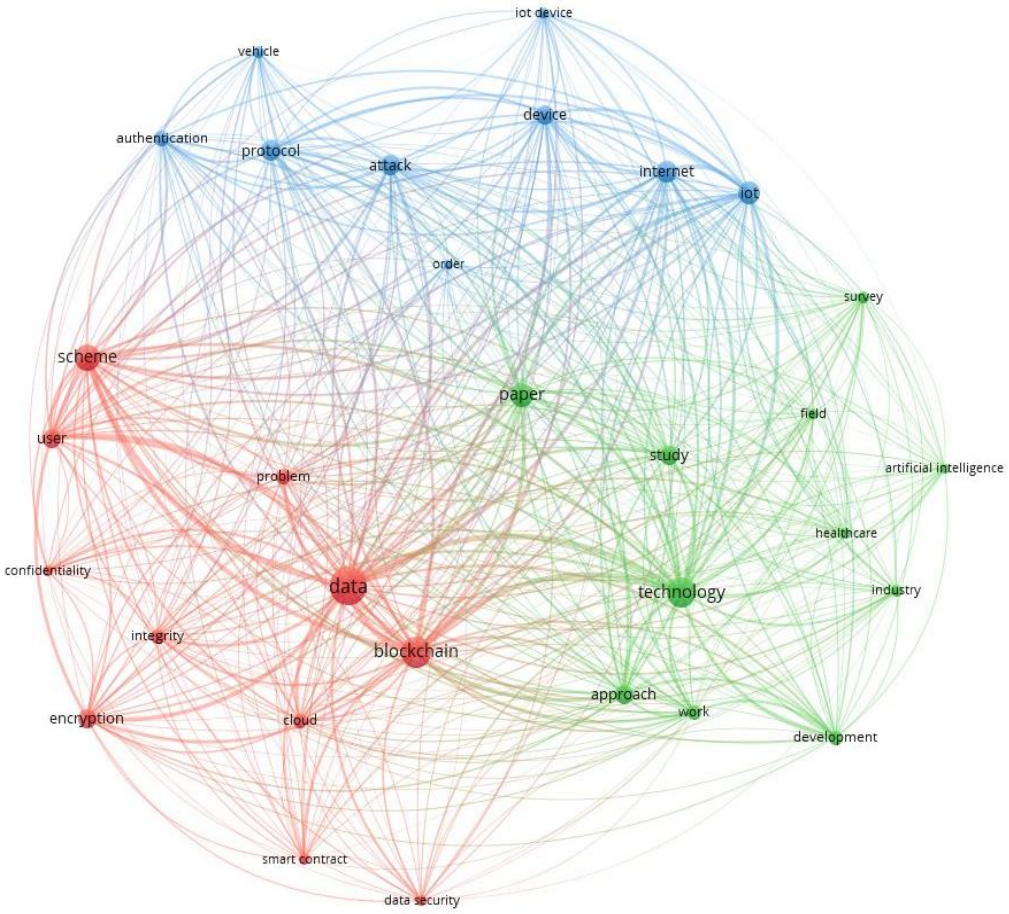

Fig 7. Keyword co-occurrence map (VOSviewer).
Source: VOSviewer (2025).

Cluster 1, the most central and dense, groups terms such as *blockchain*, *encryption*, *data security*, *confidentiality*, *integrity*, and *smart contract*. This cluster represents the conceptual core of the field and highlights the frequent association between encryption mechanisms, including symmetric encryption approaches such as AES and immutable registration systems aimed at ensuring comprehensive data protection. The prominence of these keywords indicates that the literature recurrently addresses the articulation between confidentiality and integrity, pointing to an increasingly structured, albeit still fragmented, research direction focused on hybrid cryptographic and blockchain-based approaches.

Cluster 2 brings together topics related to technological applications and industrial contexts, including *technology*, *development*, *healthcare*, *industry*, and *artificial intelligence*. This cluster reflects the growing adoption of blockchain and encryption in applied domains, particularly in medical systems, smart industrial environments, and AI-driven solutions. It also suggests an increasing concern with adapting data protection mechanisms to scenarios that require high reliability, traceability, and auditing capabilities.

Cluster 3 focuses on distributed infrastructures and interconnected devices, grouping terms such as *IoT*, *device*, *protocol*, *authentication*, and *attack*. This cluster highlights the relevance of security in networked environments, where the combination of encryption and blockchain mechanisms is frequently explored to mitigate risks associated with cyberattacks, device compromise, and data manipulation, both in transit and at rest.

The overall analysis of these clusters indicates that the literature is both cohesive due to the centrality of data protection concerns and diverse, reflecting the wide range of application contexts in which blockchain and encryption coexist as complementary security mechanisms. These results provide a solid basis for identifying prevailing trends, emerging themes, and potential research gaps.

Overall, the bibliometric findings reveal a consistent thematic association between encryption mechanisms and blockchain-based solutions across multiple application domains. However, the relatively limited number of studies that explicitly propose or evaluate integrated security architectures suggests the presence of a structural research gap. The implications of these findings, particularly regarding the development of hybrid encryption–blockchain architectures, are further discussed in the following section.

5. Discussion

The bibliometric results indicate that research on blockchain, encryption, and sensitive data security has increased significantly since around 2020, coinciding with the technological maturation of blockchain platforms and with growing regulatory and operational pressures to ensure confidentiality, integrity, and auditability in distributed digital environments. Research activity is global in scope, although it is strongly concentrated in Asian academic and research institutions, particularly in China and India. This concentration reflects sustained investment in distributed technologies, large-scale digital infrastructures, and application-driven security solutions. At the same time, consistent contributions from European and North American institutions contribute to a diverse and internationally connected research landscape.

The thematic analysis shows that the literature is structured around a central cluster integrating blockchain, encryption, and data security, indicating an increasing awareness of the complementary role of cryptographic mechanisms and blockchain-based integrity guarantees. However, application-oriented clusters related to healthcare, industrial systems, and the Internet of Things (IoT) remain weakly connected to this conceptual core. This separation suggests that, although hybrid security models are widely acknowledged at a theoretical level, their translation into practical and integrated architectural solutions remains limited.

Several technical and practical factors help explain this fragmentation. Blockchain scalability limitations, combined with the computational and storage overhead associated with encrypting large volumes of data, represent significant challenges, particularly in resource-constrained environments such as IoT and edge computing. As a result, many studies continue to address confidentiality and integrity as largely independent concerns, rather than proposing unified architectures that integrate encryption mechanisms with blockchain technologies and validate them through experimental evaluation.

Overall, these findings highlight a research field that is expanding, multidisciplinary, and increasingly application-oriented, yet still characterized by notable structural gaps. While research output has grown substantially, much of the existing literature remains conceptual or focused on isolated use cases. By synthesizing current knowledge and identifying these limitations, this study clarifies directions for future research, particularly the need for practical, scalable, and experimentally validated hybrid security architectures capable of effectively combining confidentiality, integrity, and auditability.

6. Conclusion

This bibliometric review analyzes the evolution of research on blockchain and encryption for the protection of sensitive data, showing a field that has expanded markedly since 2020 in response to increasing demands for confidentiality, integrity, and auditability in distributed digital environments. The results reveal a global research ecosystem, with strong participation from Asian institutions and significant contributions from European and North American research centers.

The co-occurrence analysis indicates that the literature is organized around three main thematic axes: (i) core data security mechanisms and hybrid approaches combining encryption and blockchain technologies; (ii) application-driven research in critical domains such as healthcare, industrial systems, and artificial intelligence; and (iii) security challenges related to IoT devices and networks. Despite this thematic diversity and sustained growth, the analysis highlights notable gaps in the literature, particularly the limited number of approaches that effectively integrate confidentiality provided by symmetric encryption with integrity guarantees offered by distributed ledgers.

Current research remains largely fragmented, with many studies focusing either on encryption-based solutions or on blockchain-centric models, and relatively few works addressing unified hybrid architectures or providing rigorous experimental validation in real-world contexts. In this context, the findings of this review underscore the need for future research focused on systematic integration models between AES and blockchain, supported by comprehensive experimental evaluations of performance, scalability, and robustness. By consolidating the state of the art and identifying key trends and limitations, this work contributes to guiding future research efforts and supporting the development of advanced data protection mechanisms capable of addressing emerging challenges in the digital era.

References

Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics, 11*(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Hidayat, T., & Mahardiko, R. (2021). Data encryption algorithm AES by using blockchain technology: A review. *BACA: Jurnal Dokumentasi Dan Informasi, 42*(1), 19–30. https://doi.org/10.14203/j.baca.v42i1.643

Katoon, P. M., & Turukmane, A. V. (2025). Interoperable blockchain network for healthcare data using Fabric, Ethereum and IPFS. *Discover Artificial Intelligence, 5*(1), 308. https://doi.org/10.1007/s44163-025-00564-7

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020

Mubeena, S., & Jawahar, P. K. (2025). Lightweight compression and chaos-based encryption for secure IoT healthcare data storage on blockchain. *Engineering, Technology & Applied Science Research, 15*(6), 29759–29769. https://doi.org/10.48084/etasr.12888

PRISMA statement. (no date). PRISMA Statement. Retrieved December 3, 2025, from https://www.prisma-statement.org/

Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson.

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics, 84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Yeboah-Ofori, A., Sadat, S. K., & Darvishi, I. (2023). Blockchain security encryption to preserve data privacy and integrity in cloud environment. *Proceedings of the 10th International Conference on Future Internet of Things and Cloud (FiCloud)*, 344–351. https://doi.org/10.1109/FiCloud58648.2023.00057