Majestic International Journal of AI Innovations
Volume 1, 2026, **pp.** 1-17, **Article ID:** CM2601105003
DOI: 10.65080/inprocess

CONTENT MAJESTIC PUBLISHER

OPEN ACCESS

Systematic Review Article

Enhancing Data Security in Cloud-Based Information Systems: A Systematic Literature Review

Yazeed Alsuhaibany[1, *]

[1]*College of Business-Al Khobar, Al Yamamah University, Saudi Arabia*

Article History

Received: 03 September, 2025 Revised: 21 October, 2025 Accepted: 07 November, 2025 Published: 15 January, 2026

Abstract:

Objective: The rapid growth of cloud computing has changed how businesses handle, store, and access information. Nevertheless, this shift has raised complex security issues, particularly regarding security, integrity, and data availability. Traditional security strategies are inadequate because they cannot respond to the evolving threat landscape in an increasingly distributed, heterogeneous cloud infrastructure.

Aims: The proposed Systematic Literature Review (SLR) aims to synthesise existing knowledge on data security strategies in cloud-based information systems.

Methodology: Following the PRISMA approach, we searched peer-reviewed articles in the most prominent databases, namely IEEE, Scopus, SpringerLink, and ACM Digital Library, published between 2013 and 2024.

Results: The results indicated that data breaches, unauthorised access, insider threats, and multi-tenancy vulnerabilities are the most notable threats. The scientists propose different solutions to these risks, *e.g.,* homomorphic encryption, zero-trust architectures, AI-based threat detection, blockchain auditing, and federated identity management. Despite these developments, scalability, legal compliance, real-time detection, and energy-efficient security measures are still missing.

Conclusion: This review highlights the need for hybrid, multi-layered defence models to ensure cloud resilience. It also calls for greater focus on privacy-preserving technologies and streamlining global policies. In general, the review highlights the adaptation, security, and sustainability of architectures that are essential to safeguard sensitive data within cloud ecosystems.

Keywords: Cloud computing; data security; privacy protection; zero-trust architecture; AI-based security, homomorphic encryption, blockchain, federated identity.

1. INTRODUCTION

Cloud computing has become one of the fundamental pillars of digital infrastructure, enabling scalable, on-demand delivery of computing resources, storage, and services [1, 2]. Multinational corporations, smaller healthcare enterprises, and government offices are increasingly reliant on cloud-based information systems to streamline operations, improve speed, and enhance cost-effectiveness [3-5]. Nevertheless, technological change has raised serious concerns about data safety, especially as confidential data is outsourced to offshore servers operated by third-party providers [6, 7].

The main principles of security, which are confidentiality, integrity, and availability, cannot be easily ensured in cloud settings since they are distributed and multi-tenant [8-10]. The cloud frequently stores data in geographically separated data centres, exposing it to more cyberattacks [11-13]. The most urgent security threats are unauthorised hashing [14], insider abuse [15], incompetent use of application programming interfaces (APIs) [16], and improperly set services [15, 17-19].

Organisations that surrender all forms of direct management of infrastructure must trust cloud service providers (CSPs) to deploy high levels of security [20-22]. Nevertheless, instances involving data breaches, ransomware attacks, and service outages indicate that such trust is not necessarily valid [23, 24]. Even more sophisticated aspects of virtualisation and container orchestration tools have introduced additional security compromise vectors [25-27].

*Address correspondence to this author at College of Business-Al Khobar, Al Yamamah University, Saudi Arabia; E-mail: y_alsuhaibany@yu.edu.sa

Most of these concerns have inspired several scholarly and commercial initiatives to address the situation by developing effective systems and technologies to enhance cloud data security. Some encryption use cases (symmetric [28], asymmetric, and homomorphic encryption [29]), secure multi-party computation [28], and blockchain-based auditing [30]. AI used to detect anomalies has shown promising potential. The zero-trust security model, which invalidates any implicit trust not only within but also beyond the network perimeter, is also gaining traction in cloud-native environments.

Nevertheless, the researchers still face many challenges. Most proposed solutions lack scalability, exhibit excessive computational overhead, or are incompatible with large-scale applications [31-33]. Compliance with laws and regulations also poses a challenge to cloud security, as regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) govern data sovereignty and privacy [34-36]. Additionally, developing a transparent way for users to manage cryptographic key administration [37] and auditability across Federated cloud ecosystems [38] remains an area of research [39, 40].

Despite the growing volume of research on cloud security, existing studies remain fragmented across domains and often lack holistic or comparative synthesis. Prior works typically focus on isolated techniques, such as encryption, access control, or blockchain, but fail to comprehensively evaluate their effectiveness across different cloud service layers (IaaS, PaaS, SaaS) or application contexts (*e.g.,* healthcare, IoT, finance). Additionally, as emerging threats evolve alongside technologies such as AI and edge computing, the existing literature does not adequately address how these changes affect the robustness of current security models. Furthermore, few reviews systematically evaluate both technical performance and contextual applicability while highlighting limitations, interoperability challenges, or the user-centric design of proposed solutions. This creates a critical knowledge gap that limits informed decision-making for practitioners and leaves future researchers without a clear roadmap.

To address this, the present Systematic Literature Review (SLR) synthesises and critically examines the state of research on data security in cloud-based systems from 2013 to 2024. It consolidates fragmented insights across disciplines and presents a comparative evaluation of techniques, threats, and their alignment with key security goals, *i.e.,* confidentiality, integrity, and availability. The following focused research questions guide this review:

1. What are the primary data security threats in modern cloud environments across sectors and service layers?
2. What security techniques and frameworks have been proposed, and how effective are they contextually and technically?
3. What research gaps and limitations persist in current solutions, and what targeted directions should future studies pursue?

This review follows a transparent and replicable process based on PRISMA 2020 guidelines and includes peer-reviewed studies from multiple domains, including computer science, cybersecurity, data science, and cloud engineering. By addressing the identified gap, this study aims to inform both theoretical advancement and practical implementation. It provides structured insights for researchers, practitioners, and policymakers working to develop secure, adaptive, and scalable cloud infrastructures in alignment with open science, interdisciplinary collaboration, and global innovation agendas.

2. REVIEW PROTOCOL

The current Systematic Literature Review has followed PRISMA 2020 guidelines, making it transparent, reproducible, and methodologically robust. The PRISMA framework will help carry out an objective, systematic process for identifying, screening, and selecting relevant literature, thereby increasing the reliability of the review [41]. This process commenced with developing research questions to address, which were formulated to explore primary data security threats in cloud computing, available technology solutions, research gaps, and future research directions. A prespecified review protocol was also developed, which included defining inclusion and exclusion criteria for the studies, specifying search strings, and outlining a specific method for data extraction. This process was repeated to ensure the protocol aligned with the review's objectives, and each step of the literature selection process was summarised in a detailed structure to make it applicable.

2.1. Data Sources and Search Strategy

Multiple reputable academic databases were selected to ensure comprehensive coverage of the existing research. These are IEEE Xplore, ACM Digital Library, Scopus, and SpringerLink. These databases have been selected for their comprehensive coverage of computer science, cybersecurity, and cloud computing, ensuring access to many relevant peer-reviewed publications. The search strategy used Boolean operators to combine keywords and narrow the search scope to cloud security. The searches were conducted between May and June 2025. The primary search phrase that was implemented in all databases was*:*

- **IEEE Xplore:** ("Cloud Computing") AND ("Data Security") AND ("Encryption" OR "Access Control" OR "Privacy")
- **Scopus:** ("Cloud Computing") AND ("Data Security") AND ("Encryption" OR "Access Control" OR "Privacy")
- **ACM Digital Library:** ("Cloud Computing") AND ("Data Security") AND ("Encryption" OR "Access Control" OR "Privacy")
- **Springer Nature Link:** ("Cloud Computing") AND ("Data Security") AND ("Encryption" OR "Access Control" OR "Privacy")

When required, the search requests have been tailored according to the database's syntax, and filters have been used to restrict the results to journal articles and conference proceedings published in English. The initial search strings brought 59,329 articles. After the relative identification, 200 articles were selected. These outputs were exported into reference management software (*e.g.,* EndNote) to enable de-duplication and monitoring of the outputs through the succeeding screening stages. Table **1** depicts the selected databases and studies listed that are considered for this paper.

2.2. Inclusion and Exclusion Criteria

As depicted in Table **2**, strict inclusion and exclusion criteria were applied during the screening process to ensure relevance and quality.

2.3. Study Selection Process

The study selection process followed the standard PRISMA flow diagram, which involves four main stages: identification, screening, eligibility, and inclusion [42]. In the identification phase, 200 records were downloaded from each database. The search identified 26 duplicate records, 45 ineligible, and 23 other irrelevant studies, leaving 106 titles and abstracts to be viewed in detail. This screening step entailed an assessment of the relevance of every study compared to the inclusion criteria.

2.4. Data Extraction Strategy

Among the screened studies, 59 were considered potentially relevant and underwent full-text review at the eligibility phase. Based on such considerations, 19 of the studies were omitted due to their non-peer-reviewed nature or lack of relevance to the research questions. Finally, 40 articles appeared in the final synthesis. Such selection was checked by two reviewers independently without any agreements that were not resolved by discussion or that referred to a third reviewer. The selection flow is illustrated in the PRISMA diagram displayed in Fig. (**1**).

A structured data extraction form was developed to collect relevant information from each selected study systematically. The form was piloted on a random sample of ten articles and adjusted to improve clarity and comprehensiveness of selected data. The key data fields extracted included:

- **Author(s) and Year of Publication**
- **Methodology Employed** (*e.g.,* simulation, case study, prototype implementation)
- **Specific Data Security Threat(s) Addressed**
- **Proposed or Evaluated Security Approach**
- **Evaluation Type** (*e.g.,* empirical testing, comparative analysis, formal proof)
- **Dataset or Use Case** (*e.g.,* public cloud, healthcare application, IoT integration)

2.5. Key Findings and Limitations

The synthesis of information was conducted using a narrative thematic approach. Each study was coded based on recurring patterns and clustered under key thematic dimensions such as the type of security technique, the nature of threats addressed, and the layer of the cloud stack (IaaS, PaaS, SaaS) targeted. The extracted data were also used to populate comparative matrices to identify overlaps, gaps, and methodological trends. Descriptive synthesis allowed the categorisation of methods and results to answer the predefined research questions.

Table 1. List of studies retrieved from the selected databases.

Databases	No. of Returned Studies after search strings	Identification Phase	Removal of Duplicates and Ineligible Studies	Final Sample for Screening Phase
ACM Digital Library	242	16	8	8
Springer Nature Link	2,324	42	22	20
Scopus	986	68	33	35
IEEE Explore	55,777	74	31	43
Total	**59,329**	**200**	**94**	**106**

Table 2. Inclusion and exclusion criteria based on PRISMA checklist 2020 [41].

Criteria Type	Included	Excluded
Publication Type	Peer-reviewed journal articles and conference papers	Preprints, theses, white papers, editorials, book chapters
Language	English	Non-English
Publication Year	From 2013 to 2024	Outside the range of 2013–2024
Topic Relevance	Focused on data security in cloud computing	General cloud topics without a security focus or unrelated to cloud-based systems
Technical Contribution	Proposes or evaluates technical approaches, frameworks, or models for cloud data security	Descriptive papers lacking technical, empirical, or evaluative components
Security Focus	Addressed at least one of: confidentiality, integrity, availability, access control, threat detection	Did not address any specific security aspects or focused only on on-premise or non-cloud infrastructure

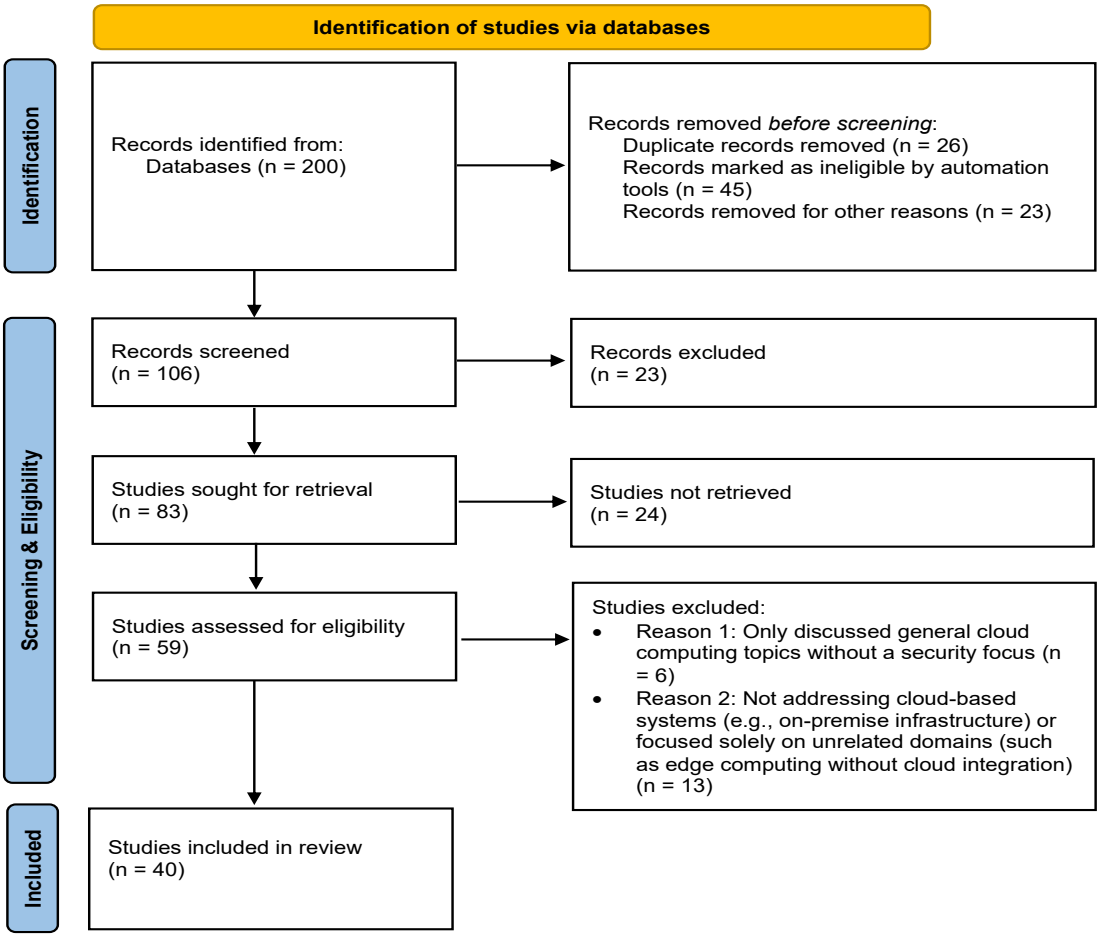

Fig. (1). PRISMA diagram.

When specific data fields (such as dataset descriptions or evaluation methods) were ambiguous or missing, interpretations were agreed upon through discussion among the reviewers to minimise extraction bias. All extracted data were entered and managed in spreadsheet software to facilitate efficient sorting, filtering, cross-tabulation, and meta-level thematic analysis. This structured approach enabled the consistent and transparent comparison of studies, ultimately supporting the identification of prevalent challenges, effective techniques, and areas needing further investigation. The extracted data is shown in Table **3** [43-82].

2.6. Risk of Bias and Reporting Bias Assessment

In accordance with PRISMA 2020 guidelines, this review incorporated a multi-layered risk of bias assessment to ensure the credibility and validity of included studies. Each paper was evaluated using a structured rubric covering four key dimensions: (i) methodological rigor, (ii) transparency of results, (iii) relevance to cloud data security, and (iv) robustness of validation methods. Studies that provided empirical evidence, clearly documented experimental setups, and articulated limitations were marked as high quality. Conversely, papers lacking these elements were rated as having a moderate or high risk of bias.

Two independent reviewers conducted the risk assessment process to reduce subjective judgment, and disagreements were resolved through discussion. Additionally, publication-related biases were considered. Reporting bias was assessed by examining whether included studies presented balanced outcomes or selectively reported only favourable results. Any discrepancies in the scope of findings and the claims made were noted. To counteract possible publication bias, the search strategy was designed to include multiple databases across technical and interdisciplinary domains. However, only peer-reviewed articles were included, which may inherently limit grey literature and increase susceptibility to publication bias.

2.7. Certainty of Evidence Assessment

The evidence derived upon this SLR was quantitatively evaluated through a triangulated approach. To begin with, consistency of results in a variety of high-quality studies was taken as a proxy of confidence. An example of this is that encryption-based confidentiality and blockchain-based integrity methods were repeatedly and reliably verified in various environments and data, which strengthens the reliability of their observations.

Second, some degree of certainty was supported by the availability of empirical reviews like the experimentation on real-life or simulated validation and comparative analysis. The weight of the certainty assessment was lower on studies based on theoretical constructs or unverifiable models.

Third, the judgment of the confidence also took into consideration the quality rating based on the risk of bias assessment. Key conclusions and recommendations were made using only findings of the studies with low or moderate bias. Weaknesses were explicitly recognised where there was diminished certainty because of small sample sizes, absence of assessment or unreported fields.

Consequently, the review gives high-certainty information on major trends (*e.g.,* access control models in healthcare data), and indicates low-certainty gaps that require additional empirical validation (*e.g.,* multimedia cloud content steganography).

3. THEMATIC ANALYSIS OF CLOUD SECURITY CHALLENGES

To bridge the fragmented understanding of evolving data security challenges in cloud-based information systems, this Systematic Literature Review (SLR) was focused on research questions guided by this review:

1. What are the primary data security threats across sectors and service layers in modern cloud environments?
2. What security techniques and frameworks have been proposed, and how effective are they contextually and technically?
3. What research gaps and limitations persist in current solutions, and what targeted directions should future studies pursue?

Through the thematic synthesis procedure (open coding → axial coding → selective coding), three **assertive themes** were derived from the literature. These themes are not new questions but structured outcomes that map directly to the guiding RQs:

Theme 1: Persistent and Emerging Threats: Identity theft, credential leakage, latency in MFA, scalability weaknesses, and privacy vulnerabilities.

Theme 2: Effectiveness of Security Techniques and Frameworks: Encryption models (AES, ECC), IAM/RBAC/ZKP, blockchain-based identity, and ML-driven anomaly detection, assessed for their contextual strengths and limitations.

Theme 3: Research Gaps and Future Directions: Limited scalability in multi-cloud settings, lack of standardised ZKP protocols, insufficient real-world validation of ML methods, and interoperability gaps across IaaS/PaaS/SaaS layers.

By aligning the derived themes with the original research questions, this review ensures consistency, maintains focus, and demonstrates how the coding-based synthesis contributes directly to answering the RQs. While several past reviews have discussed general trends in cloud security, none have integrated domain-specific and layer-specific evidence with technique-oriented classifications in a meta-synthesised manner. This review fills that gap using a structured coding framework to consolidate and contrast research contributions from 2013 to 2024.

3.1. Coding Strategy and Thematic Construction

The data extracted from 40 selected studies were coded through a three-phase process:

- **Open Coding**: Initial labels were assigned to text fragments representing security threats, approaches, or outcomes.
- **Axial Coding**: Similar codes were grouped into categories like "access control," "encryption," "data sharing," or "application specificity."
- **Selective Coding**: These categories were distilled into six major themes that comprehensively reflect cloud security challenges.

The Table **4** below summarises the frequency of these themes across the reviewed literature:

3.2. Unauthorised Access and Identity Management

One of the most frequent and noticeable topics of the reviewed studies is the problem of unauthorised access to cloud resources, especially in multi-tenant or multi-system environments. Several articles noted that traditional identity and access management (IAM) systems are inefficient in the cloud due to their dynamics and decentralised nature. As an illustration, [73] designed the decentralised access control model of industrial control systems to help eliminate the possibility of an unauthorised device access to the critical infrastructures. In a similar manner, the research by [79] paired identity spoofing in hybrid clouds and proposed a role-based IAM model to mitigate this threat.

In addition, identity and attribute-based access control (ABAC) models have also been examined in cloud-specific situations. [76] designed a version of the ABAC model to work in the context of Hadoop and complicate access to information, but did not impose any restrictions on big data processing, whereas [75] based their ABAC on blockchain through Hyperledger to reduce the risks of data leakage. Although these innovations exist, many implementations do not test the ability of their designs to scale, the latencies, and performance at large workloads.

3.3. Data Confidentiality and Encryption Limitations

Confidentiality of data has continued to be a significant issue of concern, when data is outsourced to third party infrastructures. Most papers have been examining lightweight encryption, homomorphic encryption, and hybrid cryptography as leading solutions. As an example, [63, 67] have suggested new lightweight cryptosystems aiming at lowering the computational burden without the loss of encryption capabilities. Still, their methods need to be brought to real-life tests on a much greater scale to establish the resilience and compatibility.

Table 3. Data extraction and analysis for the selected studies.

Ref.	Author(s) and Year of Publication	Methodology Employed	Specific Data Security Threat(s) Addressed	Proposed or Evaluated Security Approach	Evaluation Type	Dataset or Use Case	Key Findings and Limitations
[43]	Victor Chang & Muthu Ramachandran (2016)	Conceptual framework development	Lack of standardised practices; trust in cloud adoption	Cloud Computing Adoption Framework (CCAF)	Theoretical analysis	Generic cloud environment	Proposes an adoption framework integrating security with business readiness.
[44]	Ye Tao, Peng Xu, Hai Jin (2019)	Prototype implementation	Secure data sharing and search in cloud-edge systems	Encrypted keyword search + attribute-based encryption	Prototype and benchmark tests	Cloud-edge collaborative storage	Enhances efficiency and privacy in edge-cloud models; lacks scalability testing.
[45]	Kwangsu Lee *et al.* (2019)	Cryptographic construction and formal proof	Data confidentiality during dynamic read/write	Self-updatable encryption with CCA security	Formal cryptographic proof	Generic cloud storage	Enhances forward/backward secrecy for cloud storage; not implemented in real systems.
[46]	Jianghong Wei, Wenfen Liu, Xuexian Hu (2018)	Scheme design and simulation	Unauthorised access; revocation challenges	Revocable-storage identity-based encryption (RS-IBE)	Simulated performance and security analysis	General cloud data access	Allows revocation and fine-grained control; lacks deployment case studies.
[47]	Jiadi Yu *et al.* (2013)	Algorithm development and testing	Secure keyword search over encrypted data	Ranked searchable symmetric encryption (RSSE)	Prototype evaluation	Encrypted cloud documents	Improves search accuracy with privacy preservation; performance optimisation remains unaddressed.
[48]	Mohammed Y. Shakor *et al.* (2024)	Prototype with simulation	Data security and key management	Dynamic AES with blockchain-based key management	Simulation-based performance evaluation	Generic cloud platform	It combines AES and blockchain for stronger key control but requires more real-world testing.
[49]	Nelson Santos *et al.* (2024)	Experimental system with biometric testing	Healthcare data security in public cloud	Biometric authentication + encryption	Experimental validation	Public healthcare cloud systems	Biometric methods improve access control; integration with legacy systems remains challenging.
[50]	Hongwei Li *et al.* (2020)	Scheme design and security proof	Search efficiency and confidentiality	Dynamic Searchable Symmetric Encryption (DSSE)	Theoretical and practical analysis	Encrypted medical cloud data	Enables dynamic search with privacy; efficiency trade-offs exist.
[51]	Wei Li *et al.* (2019)	Framework implementation and simulation	Access control for personal health records	Fine-grained access control (CP-ABE variant)	Implementation with performance tests	Personal health records in cloud	Enhances access flexibility; increased overhead for large-scale systems.
[52]	Qinlong Huang *et al.* (2021)	Scheme design and implementation	Genomic data privacy and access control	Privacy-preserving testing + fine-grained access	Prototype with evaluation	Genomic cloud data	Balances privacy and usability in genomic data; scalability remains open.

(Table 3) contd....

[53]	Saja J. Mohammed & Zeena N. Al-Kateeb (2024)	Encryption model design and evaluation	Audio file confidentiality in cloud	Chao_SIFT encryption for media data	Experimental results on audio files	Cloud-based audio storage	Secures cloud-stored audio using feature-based encryption; lacks cross-media validation.
[54]	Revati R. Dewangan, Sunita Soni & Ashish Mishal (2024)	Algorithm development and testing	Image privacy in cloud storage	Optimised Homomorphic Encryption (OHE)	Simulation and visual analysis	Cloud image repositories	Protects image confidentiality with reduced processing cost; not tested at cloud scale.
[55]	Pranav Shrivastava, Bashir Alam & Mansaf Alam (2023)	Architecture design and testing	Data security and auditability	Hybrid lightweight blockchain encryption	Performance benchmarking	Generic cloud environment	Enhances traceability and integrity using blockchain; needs lighter alternatives for IoT settings.
[56]	Pranav Shrivastava, Bashir Alam & Mansaf Alam (2024)	Cryptographic framework design	Anonymous access and encryption	Ring-based homomorphic encryption + blockchain	Prototype with privacy analysis	Cloud storage systems	Combines blockchain and encryption for anonymous authentication; computational load is significant.
[57]	Miao Tian *et al.* (2024)	Scheme design with searchable encryption	Secure image retrieval and access control	Searchable encryption + access control policy	Experimental simulation	Media cloud storage	Provides secure image access and search; limited to media-type datasets.
[58]	Chandra Sekhar Tiwari & Vijay Kumar Jha (2024)	Smart contract framework implementation	Secure contract creation for cloud data	THC-DFECC-based privacy-preserving contracts	Framework evaluation *via* case simulation	Smart contract cloud services	Secures data exchange in contracts; practical application requires cloud-platform integration.
[59]	Rui Jia *et al.* (2023)	Educational model design and pilot testing	Lack of awareness and misconfiguration	Security education system for cloud platforms	Pilot testing with learners	Cloud education systems	Improves data protection awareness; limited by small participant base.
[60]	Binjie Hua *et al.* (2023)	Algorithmic design and testing	Big data privacy and visual security	Image encryption algorithm for privacy protection	Simulation and image reconstruction	Big data processing in cloud	Combines big data with image-layer security; lacks interoperability with analytics tools.
[61]	Wenjin Jin (2024)	Blockchain system design and simulation	Digital risk and privacy in finance	Blockchain + cloud for risk assessment	Simulation of digital economy models	Asset trading and finance clouds	Improves auditability and reduces fraud; privacy–latency trade-off noted.
[62]	Jing Cai *et al.* (2024)	Framework development and implementation	Privacy and access control in asset trading	Blockchain-based access control with multichannel security	Implementation and load testing	Asset trading in cloud systems	Manages secure access to cloud assets; blockchain latency is a concern in high-frequency trades.
[63]	Fursan Thabit *et al.* (2022)	Simulation and experimental testing	Data integrity and unauthorised access	Lightweight homomorphic cryptographic algorithm with dual-layer encryption	Empirical performance testing (encryption	Generic cloud environment	High encryption efficiency and security; lacks real-world deployment proof.

(Table 3) contd....

[64]	D. Shivaramakrishna & M. Nagaratna (2023)	Cryptographic model design and evaluation	Key exposure and access control	Hybrid AES-OTP & RSA with adaptive key mgmt + time-limited access control	Comparative analysis and simulation	Cloud storage environments	Enhances access granularity and key management; needs scalability validation.
[65]	S. Navin Prasad & C. Rekha (2023)	Blockchain protocol design	Identity spoofing and unauthorised access	Blockchain-based IAS protocol	Experimental framework and prototype	Cloud access control systems	Improves authentication security; complexity of integration with legacy systems remains.
[66]	Sathish Chander Krishnan (2024)	AI-based access control model with simulations	Identity theft and access violations	DRL-based access control + picturised authentication + revocation	Simulation and security analysis	Multi-user cloud systems	Novel revocation and authentication mechanism; AI decision consistency remains a challenge.
[67]	Fursan Thabit *et al.* (2021)	Lightweight cipher algorithm testing	Cloud data breach risk	128-bit block cipher using substitution-permutation + logical operations	Experimental testing and statistical analysis	Generic cloud platforms	Offers fast processing and high confusion/diffusion; lacks interoperability benchmarks.
[68]	Umi Salma Basha *et al.* (2024)	Protocol analysis and implementation	Healthcare data vulnerability	EPM-KEA Encryption Protocol	Simulation and application testing	Healthcare data cloud systems	Strong healthcare data encryption; model complexity may impact real-time performance.
[69]	Shaopeng Guan *et al.* (2024)	Hadoop-based model implementation	Secure big data storage and integrity	Secure storage *via* Hadoop + HDFS with crypto layers	Empirical testing on Hadoop	Big data in cloud	Resilient against attack types; not designed for real-time querying.
[70]	Sourav Bera *et al.* (2023)	Cryptographic scheme with verification layer	Data authenticity and retrieval validation	Attribute-Based Verifiable Storage and Retrieval (AB-VSR)	Formal proof and prototype validation	Cloud storage systems	Combines access control with proof of integrity; needs performance under load validation.
[71]	Xin Dong *et al.* (2014)	Cryptographic framework development	Privacy-preserving data sharing	Privacy-preserving, scalable data-sharing framework	Simulated evaluation and framework analysis	General cloud applications	Enhances scalability and privacy; lacks deployment in commercial systems.
[72]	Neha Agrawal & Shashikala Tapaswi (2019)	Agent-based system design	Mobile cloud access vulnerabilities	Encrypted agent-based access control framework	Security evaluation and theoretical analysis	Mobile cloud computing	Improves secure access control in mobile scenarios; real-time constraint adaptation is missing.
[73]	Kasturi Routray, Padmalochan Bera (2024)	Prototype Implementation	Unauthorised Access in Industrial Cloud Systems	Decentralised Access Control Model	Prototype Validation	Cloud-Assisted Industrial Control Systems	Improved access management and decentralisation; large-scale integration validation needed.
[74]	Yubing Duan, Xiaolei Deng, Haosen Yang (2021)	Model Implementation and Testing	Multi-Tenant Data Isolation	Environmental Attributes and Security Labels	Empirical Testing	Cloud Multi-Tenant Systems	Flexible access control; lacks full-scale real-world validation.

(Table 3) contd....

[75]	Afnan Alniamy, Bradley D. Taylor (2020)	Blockchain Integration with Access Control	Data Leakage during Sharing	Attribute-Based Access Control using Hyperledger	Prototype Demonstration	Permissioned Blockchain Systems	Achieves fine-grained access; high-load performance remains untested.
[76]	Maanak Gupta, Farhan Patwa, Ravi Sandhu (2018)	Access Control Policy Design in Hadoop	Unauthorised Big Data Access	Attribute-Based Access Control Model	Policy Evaluation in Hadoop	Big Data Processing on Hadoop	Enables secure and granular access; cross-platform performance not fully assessed.
[77]	Sahar Ebadinezhad, Halmat Ayub Abdulmajed (2024)	Protocol Design and Simulation	Data Encryption Weakness	DKE Encryption Protocol	Simulated Testing	General Cloud Data Encryption	Flexible encryption solution; real-world feasibility needs validation.
[78]	Zizhong Wei *et al.* (2024)	System Design and Testing	Agricultural Data Vulnerability	Privacy Computing System (PCS-ADS)	Experimental Testing	Agricultural Data	Protects farm data; limited test on scalability across regions.
[79]	Saurabh Deochake, Vrushali Channapattan (2022)	IAM Framework Development	Identity Spoofing in Hybrid Clouds	Role-based IAM for Hybrid Clouds	Prototype Evaluation	Multi-tenant Hybrid Cloud	Strong tenant separation and security; performance under multi-domain setup unverified.
[80]	Reynaldo R. Corpuz *et al.* (2018)	Encryption Algorithm Modification	Data Confidentiality Risks	Modified Blowfish Algorithm	Algorithm Performance Testing	General Cloud Storage	Improved speed; full cryptographic strength assessment lacking.
[81]	Suyel Namasudra *et al.* (2020)	Encryption Design using DNA Algorithms	Multimedia Data Leakage	DNA-Based Encryption	Simulation and Security Testing	Multimedia Cloud Storage	Secure for image and video files; computational demands may limit use.
[82]	Arpan Bhattacharya *et al.* (2023)	Steganography-based Security Model	Unauthorised Data Access	Cloud Steganography	Model Demonstration	General Cloud Data	Effective data hiding; needs scaling tests for diverse cloud platforms.

Table 4. Thematic summary of cloud security challenges.

Security Challenge	Studies Addressing Challenge
Unauthorised Access & Identity Management	[73, 76, 75, 79]
Data Confidentiality & Encryption	[54, 63, 67, 81]
Access Control in Multi-Tenant Environments	[46, 74, 83-87]
Secure Data Sharing & Search	[44, 47, 50]
Emerging Solutions (Blockchain & Steganography)	[55-56, 61, 82, 88-89]
Application-Specific Security	[68, 78]

DNA-based encryption and homomorphic encryption were also claimed to be promising methods, but computationally expensive. Although, [81] reported the high level of protection of multimedia files using DNA-based approaches, they mentioned the high processing requirements as a limitation. [54] emphasised the prevalent capability of optimised homomorphic encryption in image data security, but the bottleneck was scalability. Generally, existing research admitted that though encryption secures data in motion and at rest, performance trade-offs tend to result in low applicability in large-scale or latency-sensitive workloads.

3.4. Access Control in Multi-Tenant and Dynamic Environments

As the multi-cloud and hybrid designs have emerged, access control in dynamic and multi-tenant environments has grown to be very complex [83, 84]. Some research tried to incorporate the contextual or environmental determinants in the access policy [85, 86]. The approach to the environmental characteristics and label-based access control model proposed by [74] increases the adaptability of the deployed access control model, but remains to be checked in real-world loads.

In addition, attribute-based encryption (ABE) and revocable identity-based encryption (IBE) had been commonly discussed on the fine-grained access to data [87]. For instance, [46] created an identity-based encryption scheme with revocable storage, in which revocation of a user does not affect system efficiency. These solutions have flexibility providing access control capabilities but the major complexity of key management is often high and lack interoperability between cloud platforms.

3.5. Secure Data Sharing and Search

The other main theme was safe data sharing and searchable encryption. One can often discover cloud users who need to exchange or access encrypted data without compromising privacy. This problem was addressed by some studies such as [47, 50] by taking into consideration the advancement of a dynamic searchable and symmetric scheme of encryption in the medical and multipurpose clouds. These programs can improve searches without causing information of value to leak out. However, not all of them have been widely empirically tested in a multi-user or high-volume search environment.

In edge-cloud collaborative systems, such as the one presented by [44], it was additional complicated to make sure that keyword searching was secure and efficient. To realise greater granularity, they combined encrypted search and attribute-based encryption, but observed that scalability is a challenge that restrains general deployment.

3.6. Emerging Solutions: Blockchain and Steganography

Blockchain security is also being investigated more. It is a tool to guarantee data's immutability, transparency, and decentralisation. [55, 56, 61] have presented papers with frameworks that use blockchain to secure access control, asset trading, and anonymous authentication. When homomorphic or ring-based encryption is used with blockchain, the result is both audibility and trust, but with significantly expensive overhead processing and possible latency, particularly in resource constraints.

Cloud steganography is another innovative solution that is increasingly used and is studied by [82]. Steganography provides an additional level of privacy by utilising hidden content within the most benign of data [88, 89]. Although this is more effective in improving concealment, it is not widely validated and might not hold against advanced intrusion detection methodologies.

3.7. Application-Specific Security and Sectoral Needs

Several articles discussed security requirements relevant in specific areas like healthcare, agriculture, and genomic information. In a recent case, [68] proposed EPM-KEA encryption in healthcare systems focusing on compliance and real-time security. Similarly, [78] developed PCS-ADS, a privacy computing system for agricultural data. Such studies highlight that security adaptations in various sectors must be considered, where solutions developed with the idea of being widespread may be unsuitable for sensitive or regulatory environments.

4. TECHNIQUES FOR ENHANCING DATA SECURITY IN THE CLOUD

Development of cloud computing has changed the manner in which organisations access, store and manage data. However, these have many advantages linked with massive dangers in safeguarding confidential information. An analysis of literature has revealed that a variety of methods have been developed to address threats against confidentiality, integrity, and availability. This section will involve a deep discussion of the major techniques that are actively pursued or are gaining momentum in order to enhance the degree of data security within cloud settings.

4.1. Encryption Techniques: Symmetric, Asymmetric, and Hybrid Models

Encryption remains the backbone of data confidentiality in cloud systems. Non-cryptographic symmetric encryption algorithms, commonly known as traditional symmetric encryption algorithms, are highly used because of their speed and simplicity. One of the prominent examples is the Advanced Encryption Standard (AES) [90]. Nevertheless, symmetric encryption may not be adequate for cloud applications due to the difficulties in distributing and managing keys [91].

Although they are more computationally intensive, more efficient key management is provided by asymmetric encryption algorithms such as RSA. Consequently, numerous studies suggest a hybrid system of encryption that assimilates the most effective attributes of both systems. As an example, [64] proposed a hybrid cryptographic framework that combined AES-OTP and RSA, adaptive key management, and time-limited access control. Such practice improves the security and flexibility of access and meets the real-time control requirements in dynamically scaled-up environments and clouds.

Furthermore, lightweight cryptography has become popular, including IoT and mobile cloud computing [92]. The proposed efficient homomorphic and symmetric encryption schemes were created by [63, 67] and optimised depending on low-power conditions, featuring not only efficient execution but also high-security standards.

4.2. Attribute-Based and Identity-Based Encryption

Fine-grain access control has also been repeatedly implemented using attribute-based encryption (ABE) and identity-based encryption (IBE). The attributes of these encryption paradigms are that there is a data access mechanism that entails user attributes or roles that can be very helpful in multi-user and collaborative cloud environments [93].

The scheme of revocable storage identity-based encryption (RS-IBE) was proposed by [46] that secures data sharing and allows revoking users without re-encryption. It is an economical method of administration where user turnover is high.

In the same context, [51] used ABE to restrict user access to their health records stored in the cloud. Their structure guarantees decryption *via* qualified medical staff only by using specific characteristics such as department, level of clearance, and specialization. These models have been useful in upgrading data privacy and flexibility in operations, but they are always associated with advanced computational and key management complexity.

4.3. Homomorphic and Searchable Encryption

A major challenge in cloud data security is performing operations or searches on encrypted data without decrypting it. This is where searchable encryption (SE) and homomorphic encryption (HE) come into play.

Homomorphic encryption enables the computations to be made over encrypted data, generating encrypted outputs; the data need not be decrypted, nor intermediate values be revealed [94]. Despite being resource-intensive, it offers unmatched confidentiality on applications such as cloud-based analytics and financial modelling.

The case of the secure image processing in clouds optimised by HE was studied by [54]. They are built privately with light computation, and partly address mass scale. Searchable encryption has been subjected to rigorous research where the encryption is required when one has to search a database that has been encrypted. [47, 50] reported dynamic searchable symmetric encryption (DSSE) schemes which possess a keyword search and can provide data privacy. These techniques have been practically applied in the legal or medical field, where it would be important to preserve the privacy of the documents under search.

4.4. Blockchain for Secure Data Integrity and Access Control

Cloud data security has been very alluring by using blockchain technology, primarily because it ensures integrity of data, traceable record mechanisms and decentralised access control. Its consensus algorithms and tamper-resistant ledger add the dimension of graph to sharing and storage of clouds [55, 56] augmented encryption models using blockchain that implemented smart contracts and homomorphic encryption to control entry and the recording of every exchange. [75] also used blockchain to offer Hyperledger-based access to attribute control that facilitated a decentralised user verification and implemented policies.

Such situations are the best fit with blockchain since its immutability and transparency ensure data auditing and non-repudiation. It is thus appropriate in financial systems, healthcare and the trade of digital assets [95, 96]. However, the greatest limitation is that blockchain has large computation and storage overheads, which hamper its implementation in high-frequency access systems.

4.5. Advanced Access Control Mechanisms

The initial aspect of cloud security is the application of controls to ensure that only authorised users can access the cloud data. Sophisticated systems such as Context-Aware Access Control (CAAC), Role-Based Access Control (RBAC), and Environmental Attribute-based Control were employed to respond to the ever-changing live contexts of cloud environments [97].

In one such case, [74] proposed an environmental attribute-based model, the parameter of which is context-dependent (location, time, and system state) and is applied to access decisions. The model glues it more to the real-life situations and improves security and usability.

In addition, [76] implemented an ABAC model to products of the Hadoop ecosystem to regulate access to big data. These are policy based and granular models and hence can be useful in hybrid, federated clouds.

They are capable of complex rule engines and proper decision-making mechanisms to prevent the delays that will be a bottleneck in real time systems in undertaking access evaluation.

4.6. Data Hiding and Obfuscation Techniques

Data hiding techniques such as steganography have also been considered as lightweight security layers of multimedia data to complement encryption in the cloud environment. The cloud steganography model introduced by [82] allows essential data to be stored in media files that the intruder will not notice.

Such methods are particularly effective when the data must be hidden in plain view, *e.g.,* in secretive communications or in a region with extensive surveillance. Nevertheless, steganography is not enough to offer fully-fledged data security; it is usually incorporated with encryption to offer multi-layered protection.

4.7. Biometric and Multi-Factor Authentication

While encryption protects data in storage and transit, authentication techniques secure access points. The conventional password-based solutions are becoming less adequate as they are prone to phishing attacks and brute forces [98].

Some studies implemented the use of biometric authentication to access the cloud. As an example, the article by [49] employed facial biometrics and fingerprint scanning to verify access to cloud computing in healthcare related to the general population. Such an approach enhances identity authentication and increases user accountability.

Multifactor authentication (MFA) (the combination of something the user knows (password), something they have (device), and something they are (biometric)) is increasingly becoming important as well [99]. Such solutions are much more likely not to be breached, and they might need extra measures of infrastructure or user compliance.

4.8. Privacy-Preserving Data Sharing and Revocation

With the introduction of collaboration characteristics in cloud systems, there is a need to share information and data in a privacy-preserving and secure way. Providing temporary and traceable access to a third party is increasingly offered over schemes like proxy re-encryption, revocable keys, and zero-knowledge proofs [100].

The data sharing schemes provided by [46, 52] allow sharing data to be used medically and in genomics, respectively. They can be cancelled, dynamically altered, and added. These models take note of confidentiality, compliance, and adaptability, but the usage of keys and identity of users across organisations continues to pose integration issues.

5. COMPARATIVE ANALYSIS OF FINDINGS

5.1. Trends Across Techniques

The security of cloud computing evolves rapidly and it is apparent that it is skewed towards hybrid and fine-grained access control processes. Even though the traditional encryption remains the heart of the matter, researchers are adding such technologies as blockchain, attribute-based encryption (ABE), searchable encryption, and the context-aware access models to make the security mechanism more dynamic and scalable.

A number of frameworks have been established that can address the constraint on resources in both IoT and mobile by implementing lightweight cryptography. To illustrate this, [63] developed a lightweight homomorphic encryption algorithm, which can enhance security without causing much load on computational resources. Other authors, such as [64], also suggested some complementary models including AES, RSA, and OTP mechanisms to establish a more secure encryption and better key management process.

The other trend is the use of blockchain to guarantee decentralised access control and auditability. Such works as [55, 56] employed blockchain in situations where it was required that data is visible and that logs are tamper-proof, particularly in multi-tenant and financial applications.

5.2. Solution Effectiveness by Cloud Layer

The security responses achieved different levels of performance at distinct cloud service layers: infrastructure-as-a-service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

At the IaaS layer, encryption methods and key management are prevalent. There are fast, hardware-compatible cryptographic systems, like lightweight cryptography [67, 80].

In the case of the PaaS layer, the solutions can work regarding role, identity, and attribute control. The customised ABAC model based on Hadoop environments [76], and access control based on the Hyperledger platform was developed to perform the same operation securely [75].

Researchers concentrated on searchable encryption, biometric authentication, and context-based access control in SaaS environments where sharing data and user interaction plays a crucial role. As an example, [50] created searchable symmetric encryption of healthcare data, whereas [49] used biometrics to allow secure access to the work of healthcare systems.

5.3. Evaluation Methods

The most prevalent assessment methods used in all the studies were simulation, prototype implementation, and empirical testing. Cryptographic models were the most used in simulations, with [64, 77] calculating new procedures in controlled conditions.

It was employed to test the real-time behaviour and scalability, especially on blockchain systems like [66, 73]. Very few studies operated on publicly available data or users' real-world environments, these researchers need to standardise more benchmarks.

5.4. Best-Suited Techniques by Security Objective

- **Confidentiality**: Solutions such as homomorphic encryption [54], searchable encryption [47], and a hybrid model of AES-RSA [64] provided high confidentiality in the sharing of data and in computation.
- **Integrity**: The model of blockchain was most helpful in retaining data immutable and transaction transparency, especially in financial systems or healthcare settings [55, 61].
- **Availability**: Availability was covered by redundant encryption and encrypted storage, access recovery through smart contracts, and systems such as PCS-ADS for agricultural information [78]. Table **5** shows a comparative analysis of the methods employed, along with the threats, strengths, and limitations.

Table 5. Comparative analysis.

Method	Threat Addressed	Strengths	Limitations
AES + RSA Hybrid Encryption	Unauthorised data access	Strong key management, fast processing	Key distribution complexity
Homomorphic Encryption	Privacy during computation	Allows encrypted processing	High computational cost
Attribute-Based Encryption (ABE)	Unauthorised data access, revocation	Fine-grained access control	Key management and scalability issues
Blockchain-Based Access Control	Tampering, Identity spoofing	Transparency, decentralised control	High latency, energy usage
DNA-Based Encryption	Multimedia confidentiality	High-level data hiding	Resource intensive
Searchable Encryption	Secure data retrieval	Preserves data privacy during query	Limited keyword matching
Steganography	Concealment of sensitive info	Lightweight, hard to detect	Vulnerable to steganalysis
Biometric Authentication	Identity spoofing	Strong user verification	Hardware dependency, privacy concerns
Context-Aware Access Control	Unauthorised context-based access	Adaptive security based on the environment	Complex rule configuration
Verifiable Storage & Retrieval	Tampering, integrity attacks	Proof of data possession	Implementation complexity

CONCLUSION

The systematic literature review analysed 40 peer-reviewed articles on data security in information systems based on clouds and discussed the primary techniques, methods of assessment and challenges. The outcomes create active research setting through developing confidentiality, integrity and availability through encryption, access control, blockchain and biometric techniques. Though traditional encryption is still the foundation of cloud data security, other newer approaches, such as homomorphic encryption, searchable encryption, and blockchain-based offerings are gaining pace due to their ability to offer finer-grained, transparent, and scalable security.

The effectiveness of these approaches often determines the choice of the cloud layer to apply to them, *i.e.,* IaaS, PaaS, or SaaS, and the environment, *i.e.,* healthcare, IoT, or enterprise collaboration. Methods like identity-based models and ABE provide finer control, but blockchain ensures integrity and traceability. However, the various approaches have trade-offs where they are characterised by computational costs, practicality, and difficult implementation.

LIMITATION

Nonetheless, despite the improvements, there are some research gaps. Such drawbacks are the absence of practical verification, issues with scaling, and the inability to be user-oriented and industry-specific. The future of cloud security is based on integrated, adaptive, and intelligent solutions that combine efficient encryption with behavioural analytics, cloud-hosted monitoring, and compliance-enhancing solutions.

Researchers and practitioners must cooperate to develop balanced, effective, sustainable security solutions as cloud services extend into more environments and devices. These systems should not only protect against current threats but also cope with upcoming complexities in digital environments of the future.

LIST OF ABBREVIATIONS

AES	=	Advanced Encryption Standard
ABAC	=	Attribute-Based Access Control
ABE	=	Attribute-Based Encryption
CAAC	=	Context-Aware Access Control
DSSE	=	Dynamic Searchable Symmetric Encryption
EPM-KEA	=	Enhanced Parallel Multi-Key Encryption Algorithm
GDPR	=	General Data Protection Regulation
IaaS	=	Infrastructure-as-a-Service
MFA	=	Multi-Factor Authentication
PaaS	=	Platform-as-a-Service
SaaS	=	Software-as-a-Service

AUTHOR'S CONTRIBUTION

Yazeed Alsuhaibany has contributed to conceptualization, idea generation, problem statement, methodology, results analysis, results interpretation.

REPORTING STANDARDS

PRISMA guidelines has been followed.

CONSENT FOR PUBLICATION

Not applicable.

AVAILABILITY OF DATA AND MATERIALS

The data will be made available on reasonable request by contacting the corresponding author [A.A.A].

FUNDING

None.

CONFLICT OF INTEREST

The author declares that there is no conflict of interest regarding the publication of this manuscript. No financial, personal, or professional relationships have influenced the content or outcomes of this study.

ACKNOWLEDGEMENTS

The author would like to express their sincere gratitude to all the researchers whose work was reviewed and cited in this study. Their contributions have been instrumental in shaping the insights and findings of this systematic literature review. We also thank the academic community and institutions providing access to high-quality digital libraries and databases, which enabled a comprehensive and rigorous analysis.

DECLARATION OF AI

During the preparation of this work the author used ChatGPT for editing purposes. After using this tool, the author reviewed and edited the content as needed and take full responsibility for the content of the published article.

REFERENCES

[1] Surianarayanan C, Chelliah PR. Essentials of Cloud Computing: A Holistic, Cloud-Native Perspective. 2nd ed. Cham: Springer; 2023. https://link.springer.com/book/10.1007/978-3-031-32044-6

[2] Voorsluys W, Broberg J, Buyya R. Introduction to cloud computing. In: Buyya R, Broberg J, Goscinski A, editors. Cloud computing: Principles and paradigms. Hoboken: Wiley Online Library; 2011. p. 1-41. https://onlinelibrary.wiley.com/doi/book/10.1002/9780470940105

[3] Ashrafuzzaman M. The impact of cloud-based management information systems on hrm efficiency: An analysis of small and medium-sized enterprises (SMES). Acad J Artif Intell Mach Learn Data Sci Manag Inf Syst. 2024;1(01):40-56. Available from: https://www.researchgate.net/publication/391810829_The_Impact_Of_Cloud_Based_Management_Information_Systems_On_HRM_Efficiency_An_Analysis_Of_Small_And_Medium-Sized_Enterprises_SMEs

[4] Singh S, Kaur J. Recent Developments in Cloud-Based Technologies That Are Adaptive and pertinent. In: Kishor K, editor. Advancements in Cloud-Based Intelligent Informative Engineering. Hershey: IGI Global; 2025. p. 95-114. https://www.igi-global.com/chapter/recent-developments-in-cloud-based-technologies-that-are-adaptive-and-pertinent/375861

[5] Chava K. The Role of Cloud Computing in Accelerating AI-Driven Innovations in Healthcare Systems. Eur Adv J Emerg Technol. 2024;2(1). https://doi.org/10.5281/zenodo.15876802

[6] Gozman D, Willcocks L. The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. J Bus Res. 2019; 97:235-56. https://doi.org/10.1016/j.jbusres.2018.06.006

[7] Benaroch M. Cybersecurity risk in IT outsourcing—Challenges and emerging realities. In: Information systems outsourcing: The era of digital transformation. Cham: Springer; 2020. p. 313-34. https://link.springer.com/chapter/10.1007/978-3-030-45819-5_13

[8] Chippagiri S. A Study of Cloud Security Frameworks for Safeguarding Multi-Tenant Cloud Architectures. Int J Comput Appl. 2025; 975:8887. Available from: https://www.ijcaonline.org/archives/volume186/number60/chippagiri-2025-ijca-924369.pdf

[9] Hayat MA, Islam S, Hossain MF. Securing the Cloud Infrastructure: Investigating Multi-tenancy Challenges, Modern Solutions and Future Research Opportunities. Int J Inf Technol Comput Sci. 2024;16(4):1-28. Available from: https://www.mecs-press.org/ijitcs/ijitcs-v16-n4/v16n4-1.html

[10] Mushtaq MF, Akram U, Khan I, Khan SN, Shahzad A, Ullah A. Cloud computing environment and security challenges: A review. Int J Adv Comput Sci Appl. 2017;8(10):183-95. Available from: https://thesai.org/Publications/ViewPaper?Volume=8&Issue=10&Code=IJACSA&SerialNo=25

[11] Onyigwang OJ, Shestak Y, Oksiuk A. Information protection of data processing center against cyber-attacks. In: 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP). IEEE; 2016. https://doi.org/10.1109/DSMP.2016.7583586

[12] Ahmad W, Rasool A, Javed AR, Baker T, Jalil Z. Cyber security in iot-based cloud computing: A comprehensive survey. Electronics. 2021;11(1):16. https://doi.org/10.3390/electronics11010016

[13] Okonofua H, Rahman SS. Cybersecurity: An analysis of the protection mechanisms in a cloud-centered environment. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom/BigDataSE). IEEE; 2018. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00299

[14] Razaque A, Shaldanbayeva N, Alotaibi B, Alotaibi M, Murat A, Alotaibi A. Big data handling approach for unauthorised cloud computing access. Electronics. 2022;11(1):137. https://doi.org/10.3390/electronics11010137

[15] Phaphoom N, Wang X, Abrahamsson P. Foundations and technological landscape of cloud computing. Int Sch Res Notices. 2013; 2013:782174. https://doi.org/10.1155/2013/782174

[16] Mousavi Z, Islam C, Babar MA, Abuadbba A, Moore K. Detecting misuse of security APIs: A systematic review. ACM Comput Surv. 2025;57(12):1-39. https://doi.org/10.1145/3735968

[17] Soofi AA, Khan MI, Amin F. A review on data security in cloud computing. Int J Comput Appl. 2017;96(2):95-6. http://dx.doi.org/10.5120/16338-5625

[18] Alghofaili Y, Albattah A, Alrajeh N, Rassam MA, Al-Rimy BAS. Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. Appl Sci. 2021;11(19):9005. https://doi.org/10.3390/app11199005

[19] Dawood M, Tu S, Xiao C, Alasmary H, Waqas M, Rehman SU. Cyberattacks and security of cloud computing: A complete guideline. Symmetry. 2023;15(11):1981. https://doi.org/10.3390/sym15111981

[20] Tang C, Liu J. Selecting a trusted cloud service provider for your SaaS program. Comput Secur. 2015; 50:60-73. https://doi.org/10.1016/j.cose.2015.02.001

[21] Lata M, Kumar V. Cyber security techniques in cloud environment: Comparative analysis of public, private and hybrid cloud. EDPACS. 2025;70(3):1-21. https://doi.org/10.1080/07366981.2025.2449743

[22] Maeser R. Analysing CSP trustworthiness and predicting cloud service performance. IEEE Open J Comput Soc. 2020;1:73-85. https://doi.org/10.1109/OJCS.2020.2994095

[23] Reshmi T. Information security breaches due to ransomware attacks-a systematic literature review. Int J Inf Manage Data Insights. 2021;1(2):100013. https://doi.org/10.1016/j.jjimei.2021.100013

[24] Brewczyńska M, Dunn S, Elijahu A. Data privacy laws response to ransomware attacks: A multi-jurisdictional analysis. In: Regulating new technologies in uncertain times. Cham: Springer; 2019. p. 281-305. https://link.springer.com/chapter/10.1007/978-94-6265-279-8_15

[25] Albugmi A, Alassafi MO, Walters R, Wills G. Data security in cloud computing. In: 2016 Fifth international conference on future generation communication technologies (FGCT). IEEE; 2016. Available from: https://ieeexplore.ieee.org/document/7605062

[26] Casalicchio E, Iannucci S. The state-of-the-art in container technologies: Application, orchestration and security. Concurr Comput Pract Exp. 2020;32(17):e5668. http): e/doi.org/10.1002/cpe.5668

[27] Wong AY, Chekole EG, Ochoa M, Zhou J. Threat modeling and security analysis of containers: A survey. arXiv. 2021. https://arxiv.org/abs/2111.11475

[28] Liu T. Research on privacy techniques based on multi-party secure computation. In: 2024 3rd International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS). IEEE; 2024. https://doi.org/10.1109/AIARS63200.2024.00171

[29] Jiang Y, Zhou Y, Feng T. A blockchain-based secure multi-party computation scheme with multi-key fully homomorphic proxy re-encryption. Information. 2022;13(10):481. https://doi.org/10.3390/info13100481

[30] Bounceur A, Berkani AS, Moumen H, Benharzallah S. The Transparency Challenge in Blockchain-Enabled Sustainable Development Goals Applications: Exploring Privacy-Preserving Techniques and Emerging Platforms. IEEE Access. 2025. https://doi.org/10.1109/ACCESS.2025.3567341

[31] Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: Issues, threats, and solutions. J Supercomput. 2020;76(12):9493-532. https://doi.org/10.1007/s11227-020-03213-1

[32] Sun PJ. Privacy protection and data security in cloud computing: A survey, challenges, and solutions. IEEE Access. 2019; 7:147420-52. https://doi.org/10.1109/ACCESS.2019.2946185

[33] El Kafhali S, El Mir I, Hanini M. Security threats, defense mechanisms, challenges, and future directions in cloud computing. Arch Comput Methods Eng. 2022;29(1):223-46. https://doi.org/10.1007/s11831-021-09573-y

[34] Kommidi VR, Padakanti S, Pendyala V. Securing the Cloud: A Comprehensive Analysis of Data Protection and Regulatory Compliance in Rule-Based Eligibility Systems. Int J Res Comput Appl Inf Technol. 2024;7(2). https://doi.org/10.5281/zenodo.13991239

[35] Naik S. Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy. Eastasouth J Inf Syst Comput Sci. 2023;1(01):69-87. https://doi.org/10.58812/esiscs.v1i01.452

[36] Singh A, Kolluri S, Modi TB. Security and Privacy Challenges in Cloud-Based Database Management: Strategies and Solutions. TECHNO REVIEW J Technol Manage. 2021;1(1):32-40. https://doi.org/10.31305/trjtm2021.v01.n01.006

[37] Salako AO, Fabuyi JA, Aideyan NT, Selesi-Aina O, Dapo-Oyewole DL, Olaniyi OO. Advancing information governance in AI-driven cloud ecosystem: Strategies for enhancing data security and meeting regulatory compliance. Asian J Res Comput Sci. 2024;17(12):66-88. Available from: https://journalajrcos.com/index.php/AJRCOS/article/view/530

[38] Sundar K, Vishwak GK, Eswaran SG. Enhancing Cloud Security: Secure and Auditable Data Sharing and its Implementation. In: 2024 2nd International Conference on Networking and Communications (ICNWC). IEEE; 2024. https://doi.org/10.1109/ICNWC60771.2024.10537314

[39] Sun Y, Zhang J, Xiong Y, Zhu G. Data security and privacy in cloud computing. Int J Distrib Sens Netw. 2014;10(7):190903. Available from: https://journals.sagepub.com/doi/10.1155/2014/190903

[40] Karamchand G. Secure and Privacy-Preserving Data Migration Techniques in Cloud Ecosystems. J Data Anal Crit Manage. 2025;1(02):67-78. Available from: https://jdacm.com/index.php/jdacm/article/view/36

[41] Sarkis-Onofre R, Catalá-López F, Aromataris E, Lockwood C. How to properly use the PRISMA Statement. Syst Rev. 2021;10(1):117. https://doi.org/10.1186/s13643-021-01671-z

[42] McCrae N, Blackstock M, Purssell E. Eligibility criteria in systematic reviews: A methodological review. Int J Nurs Stud. 2015;52(7):1269-76. https://doi.org/10.1016/j.ijnurstu.2015.02.002

[43] Chang V, Ramachandran M. Towards achieving data security with the cloud computing adoption framework. IEEE Trans Serv Comput. 2015;9(1):138-51. https://doi.org/10.1109/TSC.2015.2491281

[44] Tao Y, Xu P, Jin H. Secure data sharing and search for cloud-edge-collaborative storage. IEEE Access. 2019; 8:15963-72. https://doi.org/10.1109/ACCESS.2019.2962600

[45] Lee K, Lee DH, Park JH, Yung M, Mu Y. CCA security for self-updatable encryption: Protecting cloud data when clients read/write ciphertexts. Comput J. 2019;62(4):545-62. https://doi.org/10.1093/comjnl/bxy122

[46] Wei J, Liu W, Hu X. Secure data sharing in cloud computing using revocable-storage identity-based encryption. IEEE Trans Cloud Comput. 2016;6(4):1136-48. https://doi.org/10.1109/TCC.2016.2545668

[47] Yu J, Lu P, Zhu Y, Xue G, Li M. Toward secure multikeyword top-k retrieval over encrypted cloud data. IEEE Trans Dependable Secur Comput. 2013;10(4):239-50. https://doi.org/10.1109/TDSC.2013.9

[48] Shakor MY, Khaleel MI, Safran M, Alfarhood S, Zhu M. Dynamic AES encryption and blockchain key management: A novel solution for cloud data security. IEEE Access. 2024;12:26334-43. https://doi.org/10.1109/ACCESS.2024.3351119

[49] Santos N, Ghita B, Masala GL. Medical systems data security and biometric authentication in public cloud servers. IEEE Trans Emerg Top Comput. 2023;12(2):572-82. https://doi.org/10.1109/TETC.2023.3271957

[50] Li H, Yang Y, Dai Y, Yu S, Xiang Y. Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data. IEEE Trans Cloud Comput. 2017;8(2):484-94. https://doi.org/10.1109/TCC.2017.2769645

[51] Li W, Liu BM, Liu D, Liu RP, Wang P, Luo S, et al. Unified fine-grained access control for personal health records in cloud computing. IEEE J Biomed Health Inform. 2018;23(3):1278-89. https://doi.org/10.1109/JBHI.2018.2850304

[52] Huang Q, Yue W, Yang Y, Chen L. P2GT: Fine-grained genomic data access control with privacy-preserving testing in cloud computing. IEEE/ACM Trans Comput Biol Bioinform. 2021;19(4):2385-98. https://doi.org/10.1109/TCBB.2021.3063388

[53] Mohammed SJ, Al-Kateeb ZN. Chao_SIFT based encryption approach to secure audio files in cloud computing. Multimed Tools Appl. 2024:1-15. https://doi.org/10.1007/s11042-024-19424-0

[54] Dewangan RR, Soni S, Mishal A. Optimized Homomorphic Encryption (OHE) algorithms for protecting sensitive image data in the cloud computing environment. Int J Inf Technol. 2024;16(7):4143-53. https://doi.org/10.1007/s41870-024-01921-y

[55] Shrivastava P, Alam B, Alam M. A hybrid lightweight blockchain based encryption scheme for security enhancement in cloud computing. Multimed Tools Appl. 2024;83(1):2683-702. https://doi.org/10.1007/s11042-023-17040-y

[56] Shrivastava P, Alam B, Alam M. An anonymous authentication with blockchain assisted ring-based homomorphic encryption for enhancing security in cloud computing. Cluster Comput. 2024;27(10):13675-91. https://doi.org/10.1007/s10586-024-04617-x

[57] Tian M, Zhang Y, Zhang Y, Xiao X, Wen W. A privacy-preserving image retrieval scheme with access control based on searchable encryption in media cloud. Cybersecurity. 2024;7(1):22. https://doi.org/10.1186/s42400-024-00213-z

[58] Tiwari CS, Jha VK. THC-DFECC-based privacy preserved smart contract creation for cloud data security. Int J Inf Technol. 2024;16(7):4191-207. https://doi.org/10.1007/s41870-024-02040-4

[59] Jia R, Ni X, Shao X, Zhang T, Qi Q. Development of a security education model system for cloud computing and data security and privacy protection. Wirel Pers Commun. 2023:1-17. https://doi.org/10.1007/s11277-023-10570-6

[60] Hua B, Wang Z, Meng J, Xi H, Qi R. Big data security and privacy protection model based on image encryption algorithm. Soft Comput. 2023:1-13. https://doi.org/10.1007/s00500-023-08548-4

[61] Jin W. Security and privacy of digital economic risk assessment system based on cloud computing and blockchain. Soft Comput. 2024;28(3):2753-68. https://doi.org/10.1007/s00500-023-09586-8

[62] Cai J, Huang H, Ma C, Liu J. A blockchain-based privacy protecting framework with multi-channel access control model for asset trading. Peer-to-Peer Netw Appl. 2024;17(5):2810-29. https://doi.org/10.1007/s12083-024-01732-9

[63] Thabit F, Can O, Alhomdy S, Al-Gaphari GH, Jagtap S. A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing. Int J Intell Netw. 2022; 3:16-30. https://doi.org/10.1016/j.ijin.2022.04.001

[64] Shivaramakrishna D, Nagaratna M. A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control. Alexandria Eng J. 2023; 84:275-84. https://doi.org/10.1016/j.aej.2023.10.054

[65] Prasad SN, Rekha C. Block chain based IAS protocol to enhance security and privacy in cloud computing. Meas Sens. 2023; 28:100813. https://doi.org/10.1016/j.measen.2023.100813

[66] Krishnan SC. AI-HybridChain: Picturised authentication and DRL based access control method with secure two-fold revocation for ensuring cloud computing security. Future Gener Comput Syst. 2024; 160:389-405. https://doi.org/10.1016/j.future.2024.04.054

[67] Thabit F, Alhomdy S, Al-Ahdal AH, Jagtap S. A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transit Proc. 2021;2(1):91-9. https://doi.org/10.1016/j.gltp.2021.01.013

[68] Basha US, Gupta SK, Alawad W, Kim S, Bharany S. Fortifying healthcare data security in the cloud: A comprehensive examination of the EPM-KEA encryption protocol. Comput Mater Contin. 2024;79(2):1234-56. https://doi.org/10.32604/cmc.2024.046265

[69] Guan S, Zhang C, Wang Y, Liu W. Hadoop-based secure storage solution for big data in cloud computing environment. Digit Commun Netw. 2024;10(1):227-36. https://doi.org/10.1016/j.dcan.2023.01.014

[70] Bera S, Prasad S, Rao YS, Das AK, Park Y. Designing attribute-based verifiable data storage and retrieval scheme in cloud computing environment. J Inf Secur Appl. 2023; 75:103482. https://doi.org/10.1016/j.jisa.2023.103482

[71] Dong X, Yu J, Luo Y, Chen Y, Xue G, Li M. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. Comput Secur. 2014; 42:151-64. https://doi.org/10.1016/j.cose.2013.12.002

[72] Agrawal N, Tapaswi S. A trustworthy agent-based encrypted access control method for mobile cloud computing environment. Pervasive Mob Comput. 2019; 52:13-28. https://doi.org/10.1016/j.pmcj.2018.11.003

[73] Routray K, Bera P. Lightweight and Decentralised Access Control for Cloud-Assisted Industrial Control Systems. In: Proceedings of the 2024 Workshop on Re-design Industrial Control Systems with Security. ACM; 2023. Available from: https://dl.acm.org/doi/10.1145/3689930.3695207

[74] Duan Y, Deng X, Yang H. A multi-tenant access control method based on environmental attributes and security labels. In: Proceedings of the 2021 3rd International Conference on Information Technology and Computer Communications. ACM; 2021. Available from: https://dl.acm.org/doi/10.1145/3473465.3473473

[75] Alniamy A, Taylor BD. Attribute-based access control of data sharing based on hyperledger blockchain. In: Proceedings of the 2020 2nd International Conference on Blockchain Technology. ACM; 2020. Available from: https://dl.acm.org/doi/10.1145/3390566.3391688

[76] Gupta M, Patwa F, Sandhu R. An attribute-based access control model for secure big data processing in hadoop ecosystem. In: Proceedings of the Third ACM Workshop on Attribute-Based Access Control. ACM; 2018. https://dl.acm.org/doi/10.1145/3180457.3180463

[77] Ebadinezhad S, Abdulmajed HA. Data Security Enhancement in Cloud Computing by Proposing A DKE Encryption Protocol. In: International Conference on Advances in Artificial Intelligence and Applications. ACM; 2024. Available from: https://dl.acm.org/doi/10.1145/3603273.3634712

[78] Wei Z, Li R, Jiang K, Luo Q, Sun Z, Han T, et al. PCS-ADS: Privacy Computing System for Agricultural Data Security. In: Proceedings of the 2024 8th International Conference on Control Engineering and Artificial Intelligence. ACM; 2024. Available from: https://dl.acm.org/doi/10.1145/3640824.3640868

[79] Deochake S, Channapattan V. Identity and access management framework for multi-tenant resources in hybrid cloud computing. In: Proceedings of the 17th International Conference on Availability, Reliability and Security. ACM; 2022. https://dl.acm.org/doi/10.1145/3538969.3544896

[80] Corpuz RR, Gerardo BD, Medina RP. Using a modified approach of blowfish algorithm for data security in cloud computing. In: Proceedings of the 6th International Conference on Information Technology: IoT and Smart City. ACM; 2018. Availablr from: https://dl.acm.org/doi/10.1145/3301551.3301597

[81] Namasudra S, Chakraborty R, Majumder A, Moparthi NR. Securing multimedia by using DNA-based encryption in the cloud computing environment. ACM Trans Multimed Comput Commun Appl. 2020;16(3s):1-19. Available from: https://dl.acm.org/doi/10.1145/3392665

[82] Bhattacharya A, Seth A, Malhotra D, Verma N. Cloud Steganography: An Intelligent Approach to Improve Data Security in the Cloud Environment. In: Proceedings of the 4th International Conference on Information Management & Machine Intelligence. ACM; 2022. Available from: https://dl.acm.org/doi/10.1145/3590837.3590902

[83] Baldin I, Ruth P, Wang C, Chase JS. The future of multi-clouds: A survey of essential architectural elements. In: 2018 international scientific and technical conference modern computer network technologies (MoNeTeC). IEEE; 2018. https://doi.org/10.1109/MoNeTeC.2018.8572139

[84] Dilworth R. Advancements and Challenges in Cloud Computing: Multi-Cloud Management, Security, and AI-Driven Threat Mitigation. In: Proceedings of the 2024 7th Artificial Intelligence and Cloud Computing Conference. ACM; 2024. Available from: https://dl.acm.org/doi/10.1145/3719384.3719476

[85] Al Hadwer A, Tavana M, Gillis D, Rezania D. A systematic review of organisational factors impacting cloud-based technology adoption using technology-organisation-environment framework. Internet Things. 2021; 15:100407. https://doi.org/10.1016/j.iot.2021.100407

[86] Rahman S, Hossain MZ. Cloud-based management information systems opportunities and challenges for small and medium enterprises (SMEs). Pac J Bus Innov Strategy. 2024;1(1):28-37. https://doi.org/10.70818/pjbis.2024.v01i01.014

[87] Xu S, Yang G, Mu Y, Deng RH. Secure fine-grained access control and data sharing for dynamic groups in the cloud. IEEE Trans Inf Forensics Secur. 2018;13(8):2101-13. https://ieeexplore.ieee.org/document/8310065

[88] Adee R, Mouratidis H. A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors. 2022;22(3):1109. https://doi.org/10.3390/s22031109

[89] AlKhamese AY, Shabana WR, Hanafy IM. Data security in cloud computing using steganography: A review. In: 2019 International conference on innovative trends in computer engineering (ITCE). IEEE; 2019. https://doi.org/10.1109/ITCE.2019.8646434

[90] Tiwari A, Padmavati M, Arya M. AES (Advanced Encryption Standard) Based Cryptography for Data Security in Cloud Environment. Int J Res Appl Sci Eng Technol. 2019;7(6):1608-18. http://doi.org/10.22214/ijraset.2019.6272

[91] Fakhar F, Shibli MA. Management of symmetric cryptographic keys in cloud-based environment. In: 2013 15th International Conference on Advanced Communications Technology (ICACT). IEEE; 2013. Available from: https://www.icact.org/upload/2013/0343/20130343_finalpaper.pdf

[92] Thabit F, Can O, Wani RUZ, Qasem MA, Thorat S, Alkhzaimi HA. Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms. Concurr Comput Pract Exp. 2023;35(21):e7691. https://doi.org/10.1002/cpe.7691

[93] Zhu Y, Ma D, Hu CJ, Huang D. How to use attribute-based encryption to implement role-based access control in the cloud. In: Proceedings of the 2013 international workshop on Security in cloud computing. ACM; 2013. https://dl.acm.org/doi/10.1145/2484402.2484411

[94] Alloghani M, Alani MM, Al-Jumeily D, Baker T, Mustafina J, Hussain A, et al. A systematic review on the status and progress of homomorphic encryption technologies. J Inf Secur Appl. 2019;48:102362. https://doi.org/10.1016/j.jisa.2019.102362

[95] Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet. 2022;14(11):341. https://doi.org/10.3390/fi14110341

[96] Sarwar MI, Iqbal MW, Alyas T, Namoun A, Alrehaili A, Tufail A, et al. Data vaults for blockchain-empowered accounting information systems. IEEE Access. 2021; 9:117306-24. https://doi.org/10.1109/ACCESS.2021.3107484

[97] Farhadighalati N, Estrada-Jimenez LA, Nikghadam-Hojjati S, Barata J. A systematic review of access control models: Background, existing research, and challenges. IEEE Access. 2025. https://doi.org/10.1109/ACCESS.2025.3533145

[98] AlQahtani A, Taher F. AI implementations in cloud-based sign-in logs to detect brute force attack attempts. In: 4th International Conference on Distributed Sensing and Intelligent Systems (ICDSIS 2023). IET; 2023. https://doi.org/10.1049/icp.2024.0494

[99] Mali S. Assessing the Effectiveness of Multi-Factor Authentication in Cloud-Based Big Data Environments. Internet Things Cloud Comput. 2024;12(2):17-27. https://doi.org/10.11648/j.iotcc.20241202.11

[100] Bernabe JB, Canovas JL, Hernandez-Ramos JL, Moreno RT, Skarmeta A. Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access. 2019; 7:164908-40. https://doi.org/10.1109/ACCESS.2019.2950872

Cite as: Alsuhaibany Y. Enhancing data security in cloud-based information systems: A systematic literature review. Majestic International Journal of AI Innovations, 2026; 1:1–17, Article ID: CM2601105003.