STM JOURNALS

Journal of
Web Engineering & Technology
https://journals.stmjournals.com/jowet

ISSN: 2455-1880
Volume 13, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoWET

Review JoWET

Advancements in Privacy-Preserving Techniques for Cloud Database Management Systems: A Review Analysis

Abid Hussain*

Abstract

Cloud computing is a technology that provides a lot of configurable resources, enabling decentralized data execution and space. Cloud technologies have transformed the ideas of internal data storage and access to provide businesses with flexibility and efficiency. Thanks to cloud services like DBaaS, users may make use of advanced database features without having to worry about the burden of traditional databases. With more organizations moving to the usage of Cloud Database Management Systems (CDBMS) to administer as well as scale their data infrastructures, the issue of data privacy and security has gained different magnitudes. This study examines the topography of changing privacy threats in cloud settings, such as information breaches, internal assaults, illegal provider entrance, query deduction, metadata disclosures, and duty management concerns. Some privacy-preserving solutions, including cryptography solutions, access control, anonymization techniques, secure multi-party computing, and secure execution environments, have been established to protect against such risks. The study classifies the solutions and analyzes their strengths, weaknesses, and areas in the context of cloud databases. Even when great progress has been made, there has been little real-world implementation because of such issues as performance-security trade-offs, insufficient standardization, inability to support complex queries, and key management problems.

Keywords: Cloud database management systems (CDBMS), privacy preservation, data breaches, cryptographic techniques, homomorphic encryption, access control, secure multi-party computation, trusted execution environments, anonymization, regulatory compliance, data security

INTRODUCTION

The escalating frequency of data security breaches and cyberattacks, combined with their higher level of sophistication, means that conventional security systems are commonly ineffective in protecting contemporary database management systems (DBMS). There is even further complexity in the cloud-based framework, whereas data storage and processing have been outsourced [1, 2]. Cloud computing has developed as a cornerstone of contemporary IT infrastructure, through which it is possible to store data and perform calculations at a scale and at a cost that are suitable. Yet, this change of paradigm opens the door to a lot of security and privacy issues, given the fact that data owners will have to spill direct control of their sensitive data to third-party service providers.

There is thus a need to secure cloud DBMSs using privacy-preserving methods. In order to ensure that private information, such as financial transactions, health records, and personal identifying numbers, will not be disclosed to unauthorized parties while being calculated or analyzed, these techniques employ mathematical and cryptographic concepts [3, 4]. Such methods as

***Author for Correspondence**
Abid Hussain
E-mail: abid.hussain@cpur.edu.in

Professor, School of Computer Application & Technology, Career Point University, Kota, Rajasthan, India

Received Date: July 11, 2025
Accepted Date: September 30, 2025
Published Date: October 15, 2025

Citation: Abid Hussain. Advancements in Privacy-Preserving Techniques for Cloud Database Management Systems: A Review Analysis. Journal of Web Engineering & Technology. 2026; 13(1): 11–22p.

strong encryption, secure authentication procedures, and active anomaly checks are paramount in this objective. Also, such techniques should adhere to international regulatory policies such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which apply high levels of data protection and transparency provisions [5].

There is one important aspect in utilizing a cloud-based database that should be of concern, and that is data privacy and security. One thing that needs to be put into consideration and is highly regarded is data privacy and security [6]. Even though cloud computing has been an invention that has helped us in one way or another, it cannot be certain that the privacy and security of data are well secured. There are a lot of factors that may influence data privacy and data security, including the inability to control the data, issues of data exchange, ethics and trust concerns, and external attacks.

The data-mining-as-a-service (DMaaS) model is an advantage to users who get the outsourced analytics of large datasets, with the resulting data being a risk of new forms of privacy concerns. The servers that carry out data mining can read sensitive patterns and trends of client information, thus violating the so-called corporate privacy [7, 8]. Unlike personal privacy, which protects individual-level data, corporate privacy involves safeguarding both individual data objects and the mined behavioral patterns that are strategic assets of businesses.

The rise of big data analytics further compounds these challenges. In sectors such as healthcare, finance, smart cities, and e-commerce, massive amounts of distributed data are shared and processed to extract actionable insights [9, 10]. Nevertheless, in such distributed computing environments, ensuring privacy while enabling data sharing becomes a critical concern. Data must be analyzed without revealing it to unauthorized parties, necessitating advanced privacy-preserving mechanisms.

Moreover, privacy attacks on cloud storage systems can lead to significant financial and reputational damages for both users and service providers [11, 12]. These attacks highlight the need for resilient privacy-preserving architectures capable of securing data in transit and at rest. As a result, creating novel and trustworthy privacy-preserving frameworks specifically for cloud-based DBMSs is becoming more and more important. These frameworks guarantee the confidentiality and integrity of data across various cloud services in addition to reducing the dangers of illegal access and data leakage.

Structure of the study

The study is structured as follows: The next Section reviews privacy threats in cloud database environments. The Section after that outlines categories of privacy-preserving techniques. Then the Section after that discusses key challenges and research gaps, followed by the Section which presents the literature review, and lastly, the conclusions in the last Section.

OVERVIEW: PRIVACY THREATS IN CLOUD DATABASE ENVIRONMENTS

Cloud Database Management Systems (CDBMS) have revolutionized how organizations manage and access data (Figure 1). However, this shift to the cloud introduces several critical privacy threats that must be addressed proactively to ensure data confidentiality, integrity, and compliance [13, 14]. The most significant risks are query inference, metadata leakage, insider threats, cloud providers' unauthorized access, data breaches, and difficulties with regulatory compliance.

Data Breaches and Insider Threats

As seen in Figure 2, data breaches continue to be one of the most concerning risks in cloud systems. Vulnerabilities in system architecture, unsafe APIs, or inadequate access restrictions might expose sensitive data kept in cloud databases [15]. While external attacks often gain attention, insider threats, where employees or contractors misuse their access privileges, can be even more damaging. These threats are particularly dangerous because insiders often bypass traditional security measures and exploit trusted access.

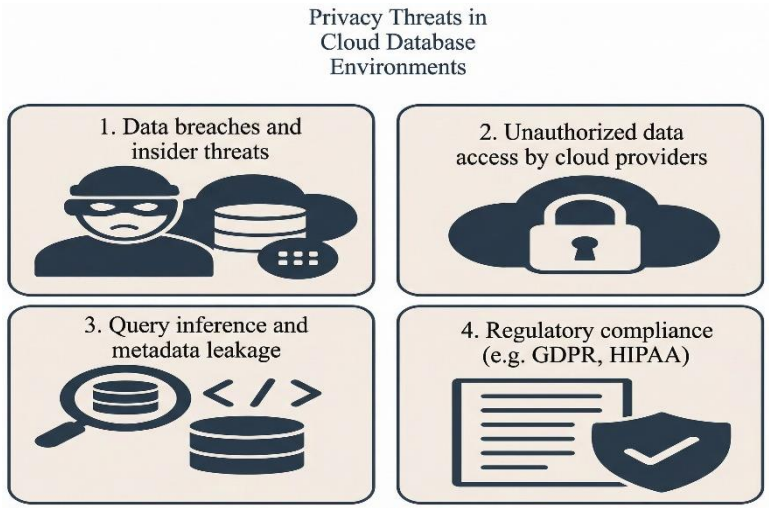

Figure 1. Privacy threats in cloud database environments [13].

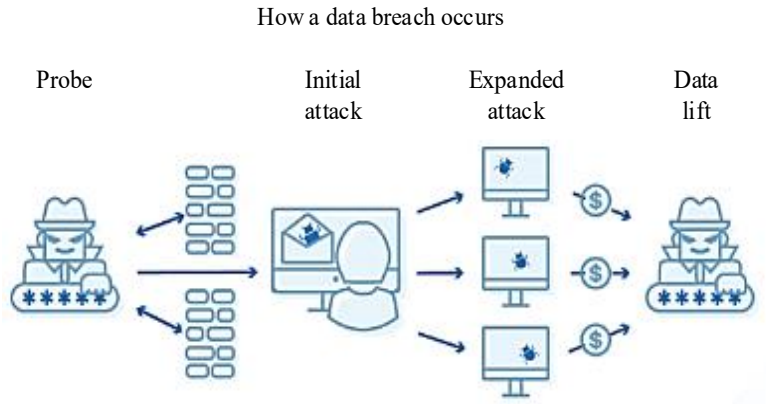

Figure 2. Data breach occurs and insider threats [15].

Unauthorized Data Access by Cloud Providers

The cloud providers are responsible for maintaining infrastructure security, and their administrative access can pose privacy risks. There is a potential for intentional or accidental data exposure, especially when clear boundaries between tenant data are not enforced [16]. Multi-tenancy, where resources are shared among multiple clients, increases the attack surface and raises concerns about whether cloud administrators might access or manipulate user data, intentionally or otherwise.

Query Inference and Metadata Leakage

Even if data is encrypted, attackers can gain insights through query inference by analyzing query patterns, access frequencies, or response times. Such indirect leakages allow adversaries to deduce sensitive information without ever decrypting the actual data [17]. Equally, schema names, table structures, and column types metadata leakages can give important context that allows the reconstruction of privacy data models, resulting in violations of privacy.

Regulatory Compliance

Organizations handling sensitive user data must comply with data protection laws like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) [18]. These regulations impose strict requirements on how personal data is stored, processed, and transferred across borders. Ensuring compliance in a cloud environment is complex, particularly when data is replicated across multiple regions and controlled by third-party providers. Non-compliance can lead to legal penalties, reputational damage, and loss of customer trust.

CATEGORIES OF PRIVACY-PRESERVING TECHNIQUES

Cloud database environments, preserving data privacy requires a multi-layered defense that integrates cryptographic, access control, anonymization, and secure computation methods. These categories of privacy-preserving techniques form the foundation of secure data management and regulatory compliance in cloud computing.

Cryptographic Techniques

Cryptographic techniques form the backbone of privacy preservation in cloud systems, as shown in Figure 3, allowing sensitive data to be secured even when processed or queried in potentially untrusted environments [19]. Below are four essential cryptographic approaches used in cloud database privacy.

Homomorphic Encryption (HE)

One effective method that allows computation on encrypted material without first decrypting it is homomorphic encryption [20]. This implies that a cloud server can add or multiply ciphertexts, and the result, after decryption, is identical to the outcome of the same operations on the plaintext, as shown in Figure 4.

- *Use Case:* Privacy-preserving analytics, secure machine learning, and encrypted data aggregation in healthcare or finance.
- *Strength:* Strong data confidentiality even during processing.
- *Limitation:* Computationally expensive and slower compared to regular encryption.

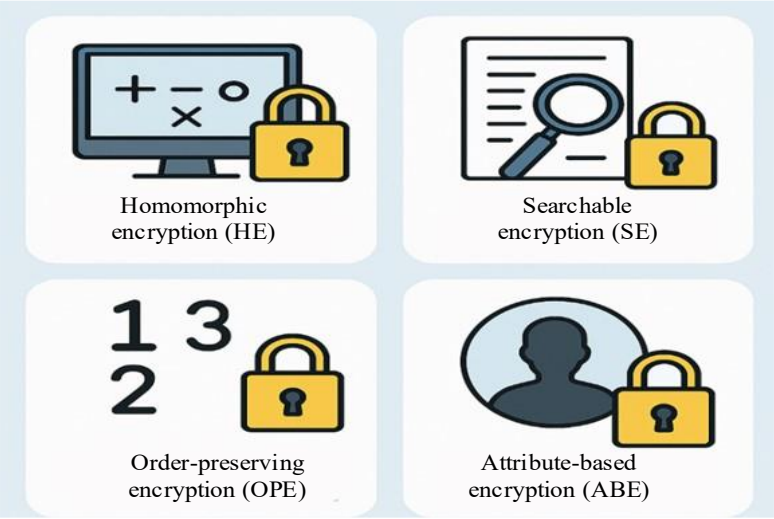

Figure 3. Cryptographic Techniques [19].

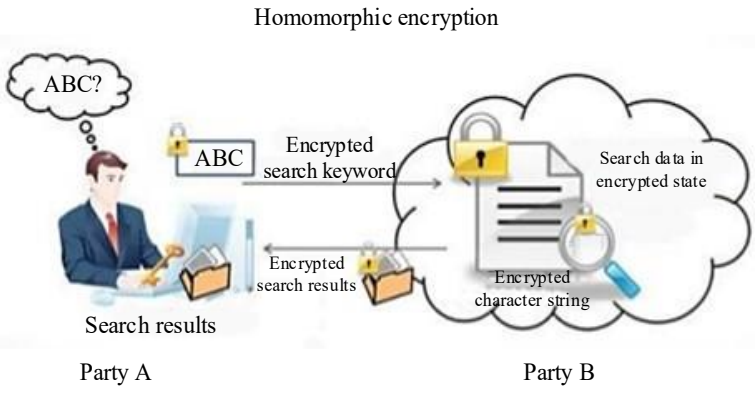

Figure 4. Homomorphic encryption [20].

Searchable Encryption (SE)

Figure 5 illustrates how users may utilize searchable encryption to look for particular keywords inside encrypted data without disclosing the content or search terms to the cloud provider [21]. There are two main types: symmetric SE, where only the data owner can search, and asymmetric SE, which supports public search capabilities.

- *Use Case:* Secures cloud-based document storage and encrypted email search.
- *Strength:* Enables encrypted keyword search.
- *Limitation:* Can leak access patterns (which keywords are searched and how often).

Order-Preserving Encryption (OPE)

OPE is a type of encryption where the order of plaintext values is preserved in their ciphertext form. This allows range queries (e.g., "find all salaries between 50k and 70k") to be performed without decrypting encrypted data.

- *Use Case:* Encrypted databases where sorting or range queries are needed.
- *Strength:* Enables efficient querying without full decryption.
- *Limitation:* Leaks relative order, which can lead to inference attacks.

Attribute-based Encryption (ABE)

Focusing on Attributes Encryption is a kind of granular encryption that allows data access depending on user characteristics (such as position, department, and clearance level). There are two categories. Figure 6 shows two possible ABE schemes: key-policy (KP-ABE) and ciphertext-policy (CP-ABE). The decision is based on whether the access policy is included in the key or the ciphertext [22].

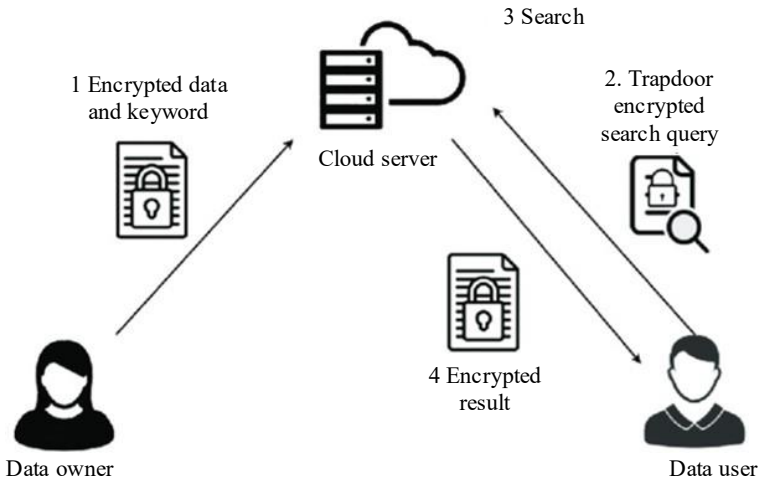

Figure 5. Searchable encryption [21].

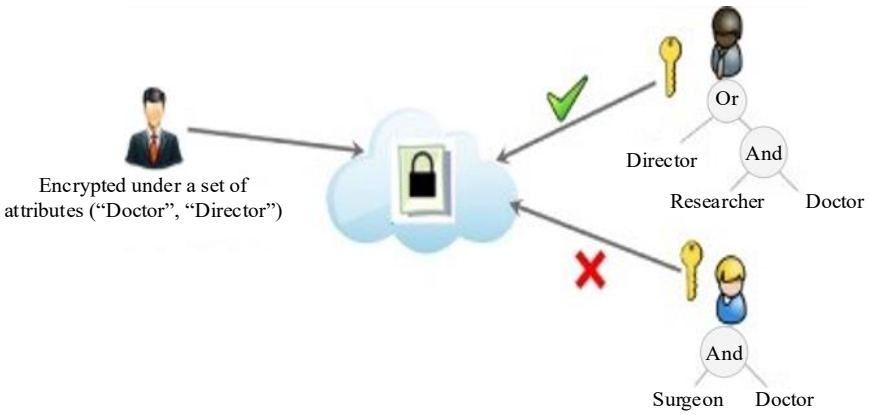

Figure 6. Attribute-based encryption [22].

- *Use Case:* Enforcing role-based access control in encrypted medical records or financial databases.
- *Strength:* Offers dynamic and scalable access control.
- *Limitation:* Complex key management and performance overhead.

Access Control Mechanisms

Reducing the danger of internal abuse or external exploitation, access management specifies who may access which data and under what conditions [23]. This is illustrated in Figure 7.

- *Role-based access control (RBAC):* Roles are allocated to users before they may access certain areas.
- *Attribute-based access control (ABAC):* Extends RBAC to support rules that are dependent on various characteristics, such as device, time, or location.
- *Fine-grained access policies:* Enable granular restrictions at the column, row, or field level in cloud databases, helping ensure only the necessary data is exposed.

Anonymization and Data Masking

These techniques reduce the risk of identifying individuals in datasets without necessarily encrypting the data.

- *k-anonymity, l-diversity, t-closeness:* Statistical anonymization methods that limit re-identification by ensuring individual records are indistinguishable within a group.
- *Differential privacy (DP):* Adds controlled noise to outputs of queries to prevent learning about individual data entries, even in aggregate analysis [24].
- *Tokenization and obfuscation:* Replaces sensitive data with surrogate values, useful in non-production environments and analytics workflows.

Secure Multi-Party Computation (SMPC)

Multiple parties can securely collaborate on data computations using SMPC, with inputs kept secret.

- *Federated querying over encrypted data:* Enables decentralized data analysis between nodes without storing sensitive information in one vault.
- *Applications in distributed cloud environments:* Used for privacy-preserving collaborations in healthcare, finance, and research without violating data boundaries [25].

Trusted Execution Environments (TEEs)

Secure computation, privacy, and data protection were the goals of the Trusted Computing specification. Figure 8 shows the original hardware module that the Trusted Platform Module relies on; it provides a functional interface for platform security. A system can safeguard cryptographic keys within a tamper-evident hardware module and offer proof of its integrity with the help of the

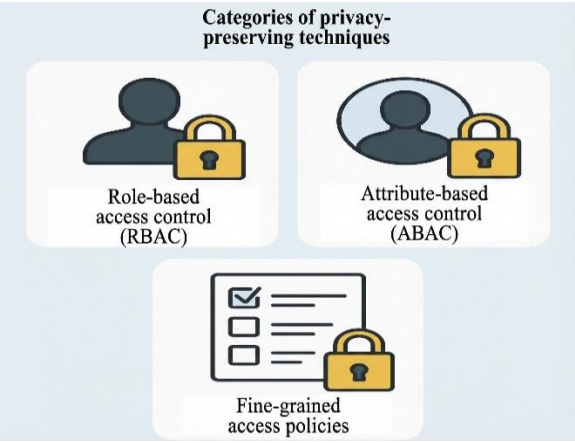

Figure 7. Access control mechanisms [23].

trusted Platform Module (TPM). Hardware-level techniques ensure secure and isolated execution of sensitive computations [26].

- *Intel SGX and secure enclaves:* These provide hardware-enforced isolation, ensuring that data and code remain protected during execution.
- *Isolation and verification of computation:* TEEs support attestation, which verifies that code is running as intended inside a protected environment.

Challenges in Cloud Database Security

Despite significant progress in privacy-preserving technologies for cloud database management systems, several technical and practical challenges persist. These issues often limit the real-world deployment, usability, and scalability of the proposed solutions [27]. Below are key challenges and research gaps that still demand attention, as shown in Figure 9.

Data Privacy and Confidentiality

The multi-tenant nature of cloud computing platforms makes it very difficult to guarantee the privacy and secrecy of data stored there. There is a heightened risk of data loss or unauthorized access when several tenants use the same physical infrastructure. In order to solve this, strong data encryption methods must be put in place. While data is stored or sent, it should be encrypted. Although it may seem like a simple task, handling the encryption keys and other concerns related to processing data securely may be rather intricate.

Access Control

To effectively protect the database in the cloud, access control is necessary. The Identity and Access Management (IAM) policies should be configured carefully so that specific data cannot be accessed by unauthorized users. Excessive permissions may be created due to

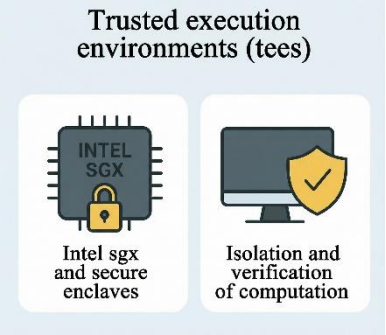

Figure 8. Trusted execution environments [26].

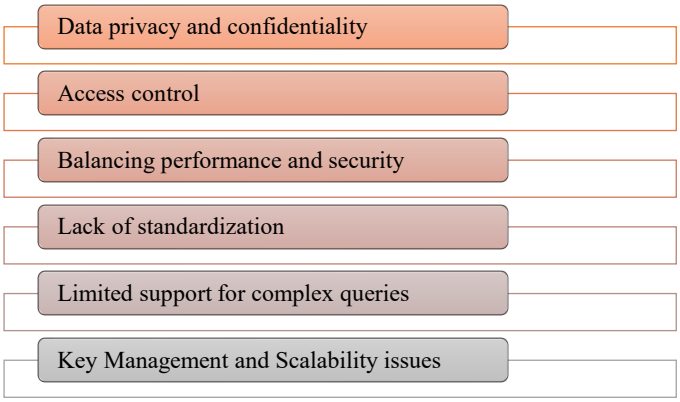

Figure 9. Key challenges of cloud database security [27].

misconfigurations, which will result in possible unauthorized access or breaches of data. Application of the Role-Based Access Control (RBAC) is another way, but it should definitely be planned with no over-permissioning. Correct determination of roles and permissions assists in mitigating the problem of abuse or unapproved access to information.

Balancing Performance and Security

The balance between offering good privacy guarantees and system performance is one of the most urgent issues. There are security-robust techniques, such as homomorphic encryption or secure multi-party computation, that are known to have a significant (competitive) latency and computational overhead [28]. This makes them hard to assimilate into systems that require the data in real-time, like healthcare analytics or financial trading.

Lack of Standardization

There is still no standard or general structure and methodology that could be applied to privacy-preserving in various cloud service providers and database structuring. This lack of interoperability hampers the adoption of these solutions, especially in multi-cloud or hybrid environments [29].

Limited Support for Complex Queries

Most encryption-based techniques struggle with supporting rich database operations such as joins, aggregations, range queries, or full-text searches on encrypted data. Current solutions often only support basic keyword or equality searches, which are insufficient for practical applications in enterprise and research settings [30].

Key Management and Scalability Issues

Efficient and secure key management is essential but often overlooked in privacy-preserving systems. Managing keys across thousands of users or devices in a cloud environment becomes complex, especially when dealing with revocation, distribution, or role changes.

LITERATURE REVIEW

The literature review section highlights evolving privacy-preserving methods in cloud computing, focusing on secure data sharing, federated learning, cryptography, and distributed systems while identifying key challenges and future research directions.

Li et al.: The development of cloud computing needs to continuously improve and perfect the privacy-preserving techniques for the user's confidential data. Multi-user join query, as an important method of data sharing, allows multiple legitimate data users to perform a join query over the data owner's encrypted database. However, some existing join query protocols may face some challenges in practical application, such as practicality, security, and efficiency. In this work, they propose a safe and dynamic join query protocol for a multi-user setting. Compared with some existing protocols, the proposed protocol has the following advantages. On the one hand, they utilize the dynamic oblivious cross tag's structure to realize an efficient join query with forward and backward security [31].

Uthej et al.: Organizing comprehensive information on automobiles, leveraging cloud technology, is not merely beneficial but imperative. As part of their strategic initiative, they are implementing a cutting-edge approach that involves the utilization of diverse cloud services, including S3 (Simple Storage Service), EC2 (Elastic Compute Cloud), AWS RDS (Relational Database Service), Cognito, Cloud Watch, IAM (Identity and Access Management), and Simple Notification Service (SNS). Their proactive strategy involves the development of an intuitive user interface hosted on the cloud. This interface empowers customers to seamlessly select and explore their preferred vehicles based on individual usage criteria. The innovative integration of cloud services, such as S3 for robust storage, EC2 for scalable computing power, and IAM for secure access control, ensures scalability, accessibility, and smooth functionality. RDS optimizes database management, SNS enables real-time communication, and CloudWatch ensures proactive monitoring [32].

Vyas et al.: They discussed the use of privacy-preserving techniques and their applications, with a particular emphasis on privacy-preserving federated learning for intrusion detection systems in IoT settings. Additionally, this poll identifies unanswered research topics and potential study paths. A number of attack vectors that target IoT ecosystems may be quickly and effectively detected and prevented with the help of privacy-preserving federated learning [33].

Sasikumar and Nagarajan: Databases, software, and computer resources are just a few of the online services provided by the rapidly expanding cloud computing sector. Its pricing approach is based on utilization, while resource-sharing is the basis for consistency. Because cloud storage lowers costs, promotes productivity, improves security, and improves efficiency, it is popular with both consumers and organizations. Nevertheless, because data is housed with third-party providers and Internet access restricts visibility and control, cloud computing entails security vulnerabilities. Cloud data security may be ensured in a number of ways, with cryptography being the most crucial. Numerous security aspects, including availability, secrecy, integrity, and authentication, are provided via cryptography. The many cryptographic techniques are not thoroughly examined in one research, though [34].

Afzal et al.: Use of ML has changed dramatically as a result of distributed and collaborative learning. A number of strategies have been developed to make distributed learning and pervasive computing possible in ubiquitous IoT systems. Several decentralized approaches have been put up to address the drawbacks of centralized learning, such as privacy concerns and latency resulting from local data sharing, while employing distributed computing as a potentially effective alternative to centralized learning. Nevertheless, these distributed learning systems raise additional privacy and security issues that need to be addressed [35].

Mishra et al.: Users who wish to utilize cloud storage services must prioritize data privacy. Cloud service providers are being heavily emphasized to meet this need. Cloud storage infrastructures are at risk of privacy violations, which are becoming more common in the dynamic and ever-changing cyberspace. Various models and methods were established by numerous investigations to guarantee the privacy of the material stored in cloud storage. Nevertheless, these models had a number of shortcomings in terms of the privacy-preserving features they addressed. Therefore, this study proposed a flexible and effective methodology to address the privacy issue by identifying a comprehensive collection of Cloud data storage privacy-preserving features [36].

Ming et al.: They created a brand-new integrated software management solution utilizing secure database technologies and cloud computing architecture. This article first presents the design system's general structure and the cloud computing architecture implementation procedure. GSM/GPRS communication technologies, embedded components, and cloud computing architecture are all included in the design of the power parameter analysis module. The primary structure comprises modules for power parameter analysis, office software administration, transmission capacity computation, service management, asset management, energy charge collecting, and so forth [37].

Table 1 summarizes recent studies on privacy and security techniques in cloud environments, outlining their focus areas, key contributions, associated challenges, and limitations, highlighting gaps for future research exploration.

CONCLUSION AND FUTURE WORK

Cloud computing is now quite advanced and successful. There are a number of risks associated with cloud computing. Existing threats include security and privacy. Numerous concerns about security and privacy still exist today, including instances of hacking and data manipulation. Cloud Database Management Systems (CDBMS) offer significant advantages in scalability, flexibility, and cost-efficiency, but they also introduce serious privacy challenges, including data breaches, insider threats,

Table 1. Summary of the study on privacy and security techniques in cloud.

Reference	Focus Area	Key Findings	Challenges	Limitations/Gap
Li *et al*. (2025) [31]	Privacy-Preserving Multi-User Join Query in Cloud DBMS	Proposed a dynamic and secure join query protocol using oblivious cross tags with forward and backward security	Security, practicality, and efficiency in multi-user join queries	Existing protocols lack comprehensive practicality and efficiency for real-world deployment
Uthej *et al*. (2024) [32]	Cloud Infrastructure for Automotive Information Systems	Developed a scalable, cloud-based interface using AWS services (S3, EC2, IAM, RDS, CloudWatch, etc.) for seamless vehicle selection and monitoring	Integrating various AWS services securely and efficiently	Limited insight into privacy implications and user data security in complex integrations
Vyas *et al*. (2024) [33]	Federated Learning for IoT Intrusion Detection with Privacy Preservation	Examined federated learning models for IoT-based IDS that protect privacy and indicated areas for further study.	Handling threat vectors efficiently while preserving privacy in federated environments	Lacks empirical validation and specific implementation frameworks
Sasikumar and Nagarajan (2024) [34]	Cryptography in Cloud Computing Security	Emphasized the significance of cryptography in ensuring authentication, integrity, confidentiality, and availability	Security risks in the cloud due to third-party storage and Internet-based control limitations	No unified comparative study on various cryptographic methods
Afzal *et al*. (2023) [35]	Distributed Learning in IoT Systems	Discussed shift to decentralized learning models to reduce privacy risks and latency in IoT	Privacy and security in collaborative, distributed environments	Emerging security risks in distributed systems are not yet fully addressed
Mishra *et al*. (2023) [36]	Privacy in Cloud Storage Systems	Determined a thorough set of characteristics for protecting privacy in cloud data storage.	Rising privacy infractions and cyber threats in dynamic cloud environments	Existing models fail to address a wide range of privacy-preserving attributes.
Ming *et al*. (2023) [37]	Cloud-Based Power Management System	Designed an integrated software management system using cloud architecture with modules for electricity, asset, and service management	System design complexity and integration of embedded and communication tech	Limited focus on security and data privacy mechanisms in power management systems

unauthorized access by cloud providers, query inference, metadata leakage, and complex regulatory compliance issues. Numerous privacy-enabling technologies have been developed to mitigate these dangers, such as Trusted Execution Environments (TEEs), Secure Multi-Party Computation (SMPC), sound access control mechanisms, anonymization schemes, and cryptographic techniques. Although these tools enhance the security of data confidentiality and integrity, they are undermined by incurring performance overheads, non-standardization, poor support on the query of encrypted data, and difficult management of keys in scalable ones in clouds. Thus, the process of privacy in the cloud has to be organized thoroughly through the perspective of a layered approach, and be both security and functionality-friendly, complying with the regulations, and keeping pace with the changing needs of the cloud-based ecosystem of data flows.

The potential areas of future research on preserving privacy in Cloud Database Management Systems (CDBMS) include engineering lightweight cryptographic algorithms and optimization techniques that can reduce excessive computational overhead in preserving privacy at the expense of security guarantees to support real-time and large-scale privacy preservation applications. The desire to establish common, interoperable structures that can be implemented within various cloud service providers and structures, particularly in multi-cloud and hybrid environments, is an urgent concern. Advancements in privacy-preserving query processing are essential, particularly for enabling

complex operations such as joins, aggregations, and full-text search over encrypted data without compromising confidentiality. Additionally, scalable and user-friendly key management systems must be designed to support dynamic access control, revocation, and multi-user collaboration. Integrating ML and AI with privacy-enhancing technologies like federated learning and differential privacy also offers promising avenues to balance utility and privacy.

REFERENCES

1. Kumar K, Pandey BK, editors. Next Generation Mechanisms for Data Encryption. CRC Press; 2025 Jan 24.
2. Murri S. Data Security Challenges and Solutions in Big Data Cloud Environments. Int J Curr Eng Technol. 2022 Jun; 12(06): 565–574.
3. Dunsin M. Comparative Analysis of Privacy-Preserving Techniques in Cloud Computing: Challenges and Future Directions. 03/02/2025
4. Thokala VS. Scalable Cloud Deployment and Automation for E-Commerce Platforms Using AWS, Heroku, and Ruby on Rails. Int J Adv Res Sci Commun Technol. 2023 Oct; 3(2): 349–62.
5. Chatterjee S. Risk management in advanced persistent threats (apts) for critical infrastructure in the utility industry. Int J Multidiscip Res. 2021; 3(4): 1–10.
6. Marpaung OS, Alvyn DA, William V, Anggereainy MS, Kurniawan A. Security and Privacy Issues in Cloud-Based Databases: A Literature Review. In 2023 IEEE 10th International Conference on ICT for Smart Society (ICISS). 2023 Sep 6; 1–6.
7. Ratheesh R. Privacy-Preserving Analysis Technique for Secure, Cloud-based Data Mining with Cloud Service Provider. J Inf Syst Eng Manag. 2025 Feb 1; 10(2): 215–23. Available from: https://jisem-journal.com/index.php/journal/article/view/1750
8. Khare P, Abhishek. Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development. Int J Curr Eng Technol. 2021; 11(06): 669–676.
9. Pasham SD. Privacy-preserving data sharing in big data analytics: A distributed computing approach. Metascience. 2023 Dec 19; 1(1): 149–84.
10. Gogineni A. Multi-Cloud Deployment with Kubernetes: Challenges, Strategies, and Performance Optimization. Int Sci J Eng Manag. 2022; 1(02): 1–6.
11. Neeli SS. Critical Cybersecurity Strategies for Database Protection against Cyber Attacks. J Artif Intell Mach Learn Data Sci. 2023; 1(1): 2102–2106.
12. Kabade S, Sharma A, Kagalkar A. Intelligent Automation in Pension Service Purchases with AI and Cloud Integration for Operational Excellence. Int J Adv Res Sci Commun Technol. 2023 Dec; 3(1): 725–735.
13. Joshi B, Joshi B, Mishra A, Arya V, Gupta AK, Peraković D. A comparative study of privacy-preserving homomorphic encryption techniques in cloud computing. Int J Cloud Appl Comput. 2022;12(1):1–11. doi: 10.4018/IJCAC.309936.
14. Duggasani AR. Scalable and Optimized Load Balancing in Cloud Systems: Intelligent Nature-Inspired Evolutionary Approach. Int J Innov Sci Res Technol. 2025 May 28; 10(5): 2153–60.
15. Dewangan RR, Soni S, Mishal A. An approach of privacy preservation and data security in cloud computing for secured data sharing. Recent Adv Electr Electron Eng. 2025 Feb; 18(2): 176–95.
16. Alam S, Bhatia S, Shuaib M, Khubrani MM, Alfayez F, Malibari AA, Ahmad S. An overview of blockchain and IoT integration for secure and reliable health records monitoring. Sustainability. 2023 Mar 23; 15(7): 5660.
17. Garg S. Predictive Analytics and Auto Remediation using Artificial Intelligence and Machine learning in Cloud Computing Operations. Available at SSRN 5267117. 2019 Apr 1.
18. Amaithi Rajan A, V V. Systematic survey: secure and privacy-preserving big data analytics in cloud. J Comput Inf Syst. 2024 Jan 2; 64(1): 136–56.
19. Tong Q, Miao Y, Li H, Liu X, Deng RH. Privacy-preserving ranked spatial keyword query in mobile cloud-assisted fog computing. IEEE Trans Mob Comput. 2021 Dec 13; 22(6): 3604–18.
20. Prajapati V. Cloud-Based Database Management: Architecture, Security, challenges and solutions. J Glob Res Electron Commun. 2025; 1(1): 07–13.

21. Bi R, Xiong J, Tian Y, Li Q, Liu X. Edge-cooperative privacy-preserving object detection over random point cloud shares for connected autonomous vehicles. IEEE Trans Intell Transp Syst. 2022 Oct 25; 23(12): 24979–90.
22. Sola RP, Malali N, Madugula P. Cloud Database Security: Integrating Deep Learning and Machine Learning for Threat Detection and Prevention: 0. Notion Press; 2025 Feb 22.
23. Lin L, Zhang X. PPVerifier: A privacy-preserving and verifiable federated learning method in cloud-edge collaborative computing environment. IEEE Internet Things J. 2022 Dec 30; 10(10): 8878–92.
24. Malali N, Praveen Madugula SR. Robustness and Adversarial Resilience of Actuarial AI/ML Models in the Face of Evolving Threats. Int J Innov Sci Res Technol. 2025 Mar 25; 10(3): 910–6.
25. Menghnani M. Modern Full Stack Development Practices for Scalable and Maintainable Cloud-Native Applications. Int J Innov Sci Res Technol. 2025; 10(2): 1206–16.
26. Hosam O, BinYuan F. A comprehensive analysis of trusted execution environments. In 2022 IEEE 8th International Conference on Information Technology Trends (ITT). 2022 May 25; 61–66.
27. Shah SB. Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure. J Glob Res Electron Commun. 2025 Feb; 2(2): 1–7.
28. Patel N. Secure access service edge (SASE): Evaluating the impact of converged network security architectures in cloud computing. Int J Emerg Technol Innov Res. 2024;11(3):e703–e714.
29. Patel R. Advancements in Renewable Energy Utilization for Sustainable Cloud Data Centers: A Survey of Emerging Approaches. Int J Curr Eng Technol. 2023 Oct; 13(5): 447–54.
30. Maddali G. An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments. Available at SSRN 5276651. 2025 May 15.
31. Li H, He D, Feng Q, Yang X, Luo Q. A Dynamic and Secure Join Query Protocol for Multi-User Environment in Cloud Computing. IEEE Transactions on Cloud Computing. 2025 Feb 21; 13(2): 512–525.
32. Uthej K, Keerthan NK, Musunuru NK, Beena BM. Cloud-Infused AWS Services: Automobile Database Management System. In 2024 IEEE 2nd International Conference on Networking, Embedded and Wireless Systems (ICNEWS). 2024 Aug 22; 1–7.
33. Vyas A, Lin PC, Hwang RH, Tripathi M. Privacy-preserving federated learning for intrusion detection in IoT environments: a survey. IEEE Access. 2024 Sep 4; 12: 127018–127050.
34. Sasikumar K, Nagarajan S. Comprehensive review and analysis of cryptography techniques in cloud computing. IEEE Access. 2024 Apr 5; 12: 52325–51.
35. Afzal MU, Abdellatif AA, Zubair M, Mehmood MQ, Massoud Y. Privacy and security in distributed learning: A review of challenges, solutions, and open research issues. IEEE Access. 2023 Oct 11; 11: 114562–81.
36. Mishra A, Jabar TS, Alzoubi YI, Mishra KN. Enhancing privacy‐preserving mechanisms in Cloud storage: A novel conceptual framework. Concurr Comput: Pract Exp. 2023 Nov 30; 35(26): e7831.
37. Ming C, Lei Z, Feng X, Xiaonan S, Qing L. Research on smart power grid big data information management system based on computer cloud security database technology. In 2023 IEEE 3rd International Conference on Data Science and Computer Application (ICDSCA). 2023 Oct 27; 1556–1561.

