Received: 16 December 2022 | Revised: 23 May 2023 | Accepted: 29 May 2023

DOI: 10.1002/cpe.7831

WILEY

RESEARCH ARTICLE

Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework

Alok Mishra[1,2] | Thr Satar Jabar[2] | Yehia Ibrahim Alzoubi[3] | Kamta Nath Mishra[4]

[1]Faculty of Engineering, Norwegian University of Science & Technology (NTNU), Gjøvik, Norway

[2]Department of Software Engineering, Atilim University, Ankara, Turkey

[3]Management Information Systems Department, College of Business, American University of the Middle East, Egaila, Kuwait

[4]Department of Computer Science & Engg, Birla Institute of Technology, Ranchi, India

Correspondence
Alok Mishra, Faculty of Engineering, Norwegian University of Science & Technology, Norway.
E-mail: alok.mishra@ntnu.no

Summary

Data privacy is critical for users who want to use Cloud storage services. There is a significant focus on Cloud service providers to address this need. However, in the evolving dynamic cyber-space, privacy infractions are rising and pose threats to Cloud storage infrastructures. Several studies developed various models and techniques to ensure the privacy of Cloud storage contents. However, these models came with several shortages in the privacy-preserving attributes they cover. Thus, this article identified a comprehensive set of Cloud data storage privacy-preserving attributes to propose a flexible and efficient framework to handle the privacy problem. This framework uses a multi-layer encryption storage structure and a one-time password authentication technique. The findings of this article intend to help future communities to enhance existing techniques or develop new research-based practical alternatives. Since Cloud computing is a rapidly growing technology, new privacy vulnerabilities emerge daily. Future research might confirm the findings of this article and test the suggested framework in different contexts.

KEYWORDS

Cloud privacy, Cloud storage, conceptual framework, encryption attributes, privacy preservation

1 | INTRODUCTION

There is an increasing interest in using Cloud Computing (CC) for digitally-connected and data-driven smart systems.[1] CC enables on-demand access to greater resources and data services at a scale to support data-driven systems.[2] With all of the hype around the Cloud's capacity to store data safely and dependably, a major problem has surfaced that concerns personal data or information privacy.[3] Privacy of the data is a critical requirement.[4]

Privacy attacks may disrupt Cloud storage services which will result in financial losses for both the users and service providers.[5] This aids in restricting access to sensitive data such as passwords, identifying information, health records, and other vital information that may put governments, organizations, or people at risk if it fell into the wrong hands.[6] In the last several years, the use of Cloud privacy-preserving techniques has gotten a lot of attention. We may describe privacy-preservation techniques as a variety of mathematical or cryptographic algorithms-based concepts and methods that handle crucial and dangerous challenges to various cyber sectors while also yielding the best techniques for establishing a dependable and safe system.[7] Depending on the nature of the threats, privacy-preserving techniques might differ in design and structure. However, they have a similar goal: to ensure that the operating system's privacy is protected.[8]

Several recommendations for privacy-preserving techniques have lately surfaced. In different ways, different attributes were taken into account in the proposed techniques. Moreover, although privacy-preserving techniques are distinctive in their design, the necessity to adapt them in the workplace is growing at a rapid pace.[9] However, the bulk of these techniques was created to achieve certain goals, such as improving user identity, data integrity, and data analysis, among others.[10–14] As a result, a comprehensive framework that can fulfill various privacy-preserving attributes is still a major demand.[7,15,16] The primary focus of this study is to provide a framework that meets different attributes of privacy-preserving while also introducing innovation in data storage and retrieval on Cloud storage. Accordingly, the following research questions are addressed in this article:

- What are the privacy-preserving attributes of Cloud data storage?
- How can these attributes be met in a privacy-preserving framework?

This study's contributions are as follows. Firstly, we reviewed the literature to identify the different attributes of privacy-preserving of Cloud data storage. Five attributes' categories were identified: design management (includes five attributes: design features, data auditing approaches, cryptographic techniques, external assets, and Cloud-storage structure), key management (includes four attributes: key generation mechanism, key length, key governance, and key function), test management (includes two attributes: test environment and tests applied), threat management (includes two attributes: threats types and threats addressed), and performance management (includes three attributes: performance standards, abnormality, and privacy achievements). By identifying these attributes, this article provides direction for designing appropriate, versatile, and trustworthy privacy-preserving techniques. Secondly, a privacy-preserving framework, based on the identified attributes, was developed. This framework deploys a multi-layer encryption system with one-time password (OTP) technology. The multi-layer encryption technique aims to achieve privacy and authentication while using OTP technology to provide the second line of defense against identity fraud threats. Finally, we compared the proposed framework with previous privacy-preserving techniques. The remainder of the article is laid out as follows. The research background and related work are presented in Section 2. The attributes of privacy-preserving Cloud data storage are discussed in Section 3. The proposed privacy-preserving of Cloud data storage framework is discussed in Section 4. The implications, future directions, and limits of this article are discussed in Section 5. This article comes to a close with Section 6.

2 | RESEARCH BACKGROUND

2.1 | Privacy-preserving

Data privacy can be described by several attributes including identity privacy (i.e., the identity of the users should be secret, except for authorized entities), data privacy (i.e., data should be secret, except for authorized users), and usage privacy (i.e., the activities of users should be secret, except for authorized parties).[17] Because of the fast expansion of the internet and informatics areas in recent years, privacy safeguards have begun to appear in cyberspace.[18] As a result, industry experts began to explore and build innovative solutions to address privacy concerns.[19] The first endeavor focused on gaining a better knowledge of data preservation and finding a valid definition for privacy-preserving techniques.[20]

Power outages, hardware issues, and network outages can all result in Cloud data failure. As a result, various recommendations were offered in the literature, such as randomization, micro-aggregation, and data condensing to preserve data stream privacy.[6] Furthermore, the creation of a privacy-preserving technique necessitates a one-of-a-kind approach that incorporates critical attributes of privacy-preserving.[7] Nagaraj and Kumar[21] proposed a four-component design for a privacy-preserving technique, comprising a user engine, user interface, Cloud database, and rule engine. Pixelated (an email user initiative) has been offered as a privacy-preserving technique for the email system. The pixelated user, which is a user interface created using a programming language for online applications, and an email election engine make up the architecture. This technique style allows users to create a connection with the server from the user site, ensuring that their data is kept private.[8]

2.2 | Related work

CC is set to be the cornerstone of future innovations.[22,23] The data privacy problem, on the other hand, is an evolving threat to CC services in a variety of forms. As a result, during the last decade, academics have focused on building privacy-preserving techniques to mitigate data threats. Initially, academics created a variety of frameworks and strategies without recognizing the threat type.[24] A few academics published survey studies focusing on the categorization of privacy threat types for Cloud storage.[24–27] Encryption, access control, and auditing measures were the most common attributes employed in each categorization. Integrity checking and keyword search were used in Reference25 work to protect the privacy of Cloud storage.

The integrity checking technique checks the purity of data transfer and compares it to a previous version of the same data to establish proof of validity. The keyword search strategy, on the other hand, entails turning a textual document into an encrypted document and allowing users to search the entire document for a specific keyword or complete phrase. This method provides a one-of-a-kind approach for encrypting native data before sending it to the Cloud. The remote data integrity checking protocol is among the emerging technologies that provide a verification tool to ensure data privacy when it is retrieved from Cloud storage.[28] In Reference29, the authors developed a methodology for sorting metadata in Cloud storage databases called dynamic metadata reconstruction. In Reference26, the authors concentrated on traditional techniques (encryption, access control, and audibility) without mentioning new and more sophisticated attributes. In Reference24, the authors divided privacy-preserving techniques into four groups (ranking, anonymization, probability, and cryptography). Cryptography and encryption are used in conjunction with other privacy-preserving measures. Probability is used to create methods in a distinctive way that produces consistent outcomes.[30] This method is being used by researchers to make the threat of data leaking a solved problem.

Data anonymization is another method, which is the process of coding or changing users' data in such a way that the data owner's identity is not revealed.[31] As a consequence, the original participant's identification is protected, as well as the user's susceptibility to identity theft assaults.[32] The ranking-driven method is applying a unique ranking algorithm to a piece of data while maintaining data privacy and attempting to achieve the most precise findings.[33] The separation of users' data and Cloud activities is among the newer options. Mutual trust between parties is essential to guarantee that every party completes its allocated work in a timely and error-free way.[34] Hardware trust approaches, on the other hand, have been devised to support soft-trust techniques in ensuring CC data privacy. Trust Computing Group, an organization that develops safe industrial standards, recently developed a new technique that improves the privacy of produced hardware, resulting in increased trust and dependability.[35] Moreover, the creation of a system of rules and laws that manage various actions in the CC system to combat possible hazards is also considered a crucial characteristic.[4]

3 | THE TAXONOMY OF PRIVACY-PRESERVING ATTRIBUTES FOR THE CLOUD DATA STORAGE

This section answers RQ1 and identifies the privacy-preserving attributes of Cloud data storage. To provide a comprehensive framework for privacy-preserving in Cloud data storage, all feasible privacy-preserving attributes must be included. This section reviewed the literature to identify these attributes that can be used to lessen the impact of privacy infractions. All available databases, including Science Direct, IEEE, Springer, Wiley, Google Scholar, and MDPI, were used to identify studies that discussed privacy-preserving in Cloud data storage. Several search phrases were used to find related studies, including “privacy,” “privacy-preserving,” “Cloud,” “CC,” “Cloud storage,” and “Cloud data storage,” with the Booleans “OR” and “AND.” The following are the studies that were used to create the set of privacy-preserving attributes.[6,9–14,16,26,29,36–63]

This article combines the most modern and well-known privacy attributes that are employed for Cloud data storage. These attributes are thought to represent the most recent discoveries of cyber security specialists in the sector. The taxonomy of these attributes is summarized in Figure 1, which comprises five categories: design management (includes five attributes: design features, data auditing approaches, cryptographic techniques, external assets, and Cloud-storage structure), key management (includes four attributes: key generation mechanism, key length, key governance, and key function), test management (includes two attributes: test environment and tests applied), threat management (includes two attributes: threats types and threats addressed), and performance management (includes three attributes: performance standards, abnormality, and privacy achievements).

Tan et al.[64] presented an innovative approach to image steganography, leveraging channel attention mechanisms within the generative adversarial network architecture. The experimental results highlight the advantages of the proposed model, including improved image quality, message extraction accuracy, and undetectability compared to traditional algorithms and existing GAN-based steganographic schemes. Hu et al.[65] introduced a novel approach to the detection of compressed Deepfake videos. The rapid advancement of technologies enabling the creation of Deepfake videos has led to a pressing need for effective detection methods. While significant progress has been made in detecting manipulations in high-definition video datasets, the forensic analysis of compressed videos warrants further exploration. Compressed videos, prevalent on social media platforms like Instagram, WeChat, and TikTok, pose a unique challenge in identifying Deepfake videos. Addressing this challenge, this article presents a two-stream method that analyzes the frame-level and temporality-level characteristics of compressed Deepfake videos. Considering that video compression introduces redundant information into frames, the proposed frame-level stream gradually prunes the network to prevent overfitting to compression artifacts. To address the issue of potential disregard for temporal consistency in Deepfake videos, a temporality-level stream is employed to extract temporal correlation features. By combining the scores obtained from both streams, the proposed method outperforms state-of-the-art techniques in detecting compressed Deepfake videos. Chen et al.[66] This article presents a novel signal noise separation-based (SNIS) network approach specifically designed for post-processed image forgery detection. The proposed approach addresses the detection of post-processed image forgeries. By formulating the problem as a signal noise separation task and introducing the SNIS network, we effectively tackle the challenges associated with post-processing effects. The experimental results demonstrate the efficacy of the proposed method, highlighting its robustness in detecting forged images with and without post-processing, as well as its ability to handle diverse post-processing attacks and images from various sources. In the following sections, we will discuss these attributes.

3.1 | Design management

Design is a significant component that the designer emphasizes to integrate additional capabilities into the functioning system. Professionals aim to implement new privacy design tiers, techniques, and approaches to produce a more competent and safe structure due to the high need for safe

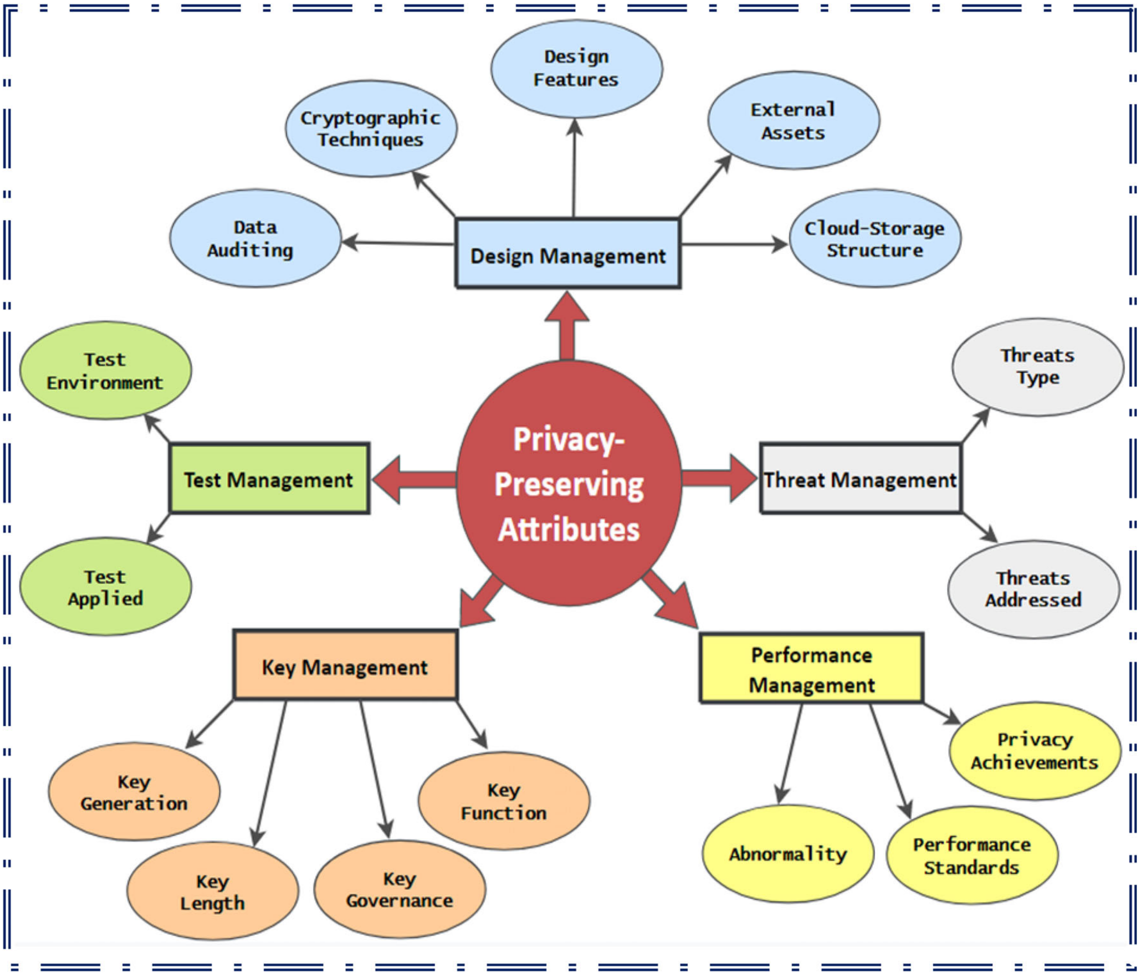

FIGURE 1 Privacy attributes taxonomy.

and multi-function privacy systems.[7] Design features, data auditing, cryptographic techniques, external assets, and Cloud-storage structure are the five attributes identified under this category.[67] The next sections go through these attributes. Table 1 summarizes the design management category attributes.

3.1.1 | Design features

In terms of Cloud storage privacy, design elements enable field workers to incorporate a variety of countermeasures into their privacy-preserving techniques.[11,14] The right application of privacy and design features will result in a trusted platform that can withstand any odd breaches that might put the Cloud environment at risk.[71]

3.1.2 | Data auditing approaches

Data auditing is defined as a means for checking Cloud service provider (CSP) services, as well as the sending and receiving communications among Cloud parties, in terms of CC.[43] Where the inspection process tries to verify the integrity of sent data utilizing a variety of detection methods such as review, analysis, protocols, and observation, among others.[46] It also guarantees that the data privacy policies and standards are followed, preventing any odd breaches. External third-party audits and internal auditing are the two forms of data auditing. External audit functions as a subordinate entity, evaluating and verifying the integrity of data sent across Cloud network participants. The internal audit examines and evaluates the data and services offered by CSP, and it is carried out by the user end to assess CSP's privacy capabilities.[43]

TABLE 1 Design management attributes.

Privacy-preserving attribute	Study	Characteristics
Design features	[11,14]	• To authenticate and validate the third-party audits, an automatic blocker protocol is used • OTP is used to verify and authenticate Cloud users • Phases of key generation and tag generation
Data auditing	[43,46]	• External third-party audits and internal auditing • The address of the data block and the data itself are stored in a special data block format • SQL procedures and queries are employed
Cryptographic technique	[10,11,13,14,16,68,6912,44,45]	• Lagrange interpolation encryption • Triple-encryption scheme • The Hash function and advanced encryption standards with a shared key • Public-key technique, digital certificates, digital certificates • Broadcast encryption, SHA-1, Hash function • Advanced Encryption Standard (AES) with ECB and randomized encryption, Homomorphic encryption method, and monotonic encryption method
External assets	[12,14,45,67]	• OTP algorithm, RFC (6238) • Lagrange interpolation algorithm • To cope with SQL queries, a non-linear order-preserving index algorithm and a custom cryptosystem were implemented • Monotonic encryption method
Cloud-storage structure	[36,53,70]	• Single CC structure • Multi-CC structure

3.1.3 | Cryptographic techniques.

Cryptographic techniques are approaches, methods, or instruments used to encrypt/decrypt various forms of digital data to safeguard the contents.[16] Encryption is defined as the process of converting clear text into a cryptic format that is safer and more dependable for communication among parties. There are several techniques to choose from such as RSA, AES, DES, and homomorphic encryption are encryption methods, which are used to safeguard Cloud data.[10,11,68] Decryption, on the other hand, is the opposite of encryption. The decryption method restores the original format (plain text) of the encrypted data.[12,13,44] Decryption algorithms are used in CC to obtain encrypted items from the Cloud repositories (Cloud storage) via requests from specified users. To obtain access to the required data, users must have the appropriate credentials and the decryption key.[14,45,69]

3.1.4 | External assets

We can refer to the external assets as the third-party tools added inside the privacy system to provide certain functionality to the overall technique structure.[67] External assets such as algorithms, data structures, mathematical representations, formulas, and other forms of materials can create a huge difference in the performance and privacy results of the entire system. External assets add a certain complexity level and abnormal features to provide a privacy-preserving technique with extraordinary privacy capability.[67] The addition of external mechanisms to the privacy-preserving techniques has elevated the privacy system's architecture to new heights. External assets, such as RFC (6238) for OTP[10] provide countermeasures for access control assaults, the Chinese remainder theorem[14] to design encryption and key generation techniques, Lagrange interpolation,[12] and Monotonic encryption algorithm[45] which can encrypt numerical representations of digital data while maintaining the order wherein the data are arranged.

3.1.5 | Cloud-storage structure

Cloud storage comes in a variety of structures, including public Cloud, private Cloud, and hybrid Cloud. However, when it comes to the protection of data privacy, there is a more essential factor to consider, which is the Cloud storage structure. The storage allotted for the deployment of privacy-preserving measures is referred to as the Cloud storage structure.[53] The multi-Cloud structure and the single Cloud structure are the two basic storage structures for Cloud storage. Each has its own set of advantages and disadvantages. Initially, corporations and individuals adopted a single Cloud infrastructure as an initial multi-service environment since it was more than adequate to store their data and provide major services at the time.[72] However, with the improvement of the CC industry and the continued rise of the cyber world applications,[70] it was unavoidable to accept the concept of multi-cloud infrastructure. The usage of several CC and storage services in a single heterogeneous design is referred to as multi-cloud technology.[36]

3.2 | Key management

The administration procedure over cryptographic keys is known as key management.[58] This category has four attributes: key generation, key length, key governance, and key function. The next sections go through these attributes. Table 2 summarizes the key management category attributes.

3.2.1 | Key generation techniques.

The key generation technique is an important part of the encryption and decryption process. The key generation technique provides encryption/decryption keys for use with the data being ciphered/deciphered.[74] To safeguard against data theft attempts in the Cloud, it employs a variety of key generation procedures, including dynamic key generation, public/private key generation, and symmetric key creation.[48] Even if the adversaries are aware of the privacy system used, privacy-preserving techniques with strong key potentials may withstand nearly any assault that targets Cloud sensitive data, since it makes it exceedingly difficult to uncover the exact decryption key.[48] Moreover, Yuan et al.[11] employed additional algorithms, such as IGEN, for establishing signature keys to put a bit more credibility to the process.

3.2.2 | Key length

A cryptographic key is a collection of numbers (0 and 1) created by a key generation process and utilized by cryptographic algorithms to secure sensitive data.[73] In cryptographic systems, key length is critical and is regarded as one of the privacy platform's basic pillars. Based on the methods utilized, there is a wide variety of key lengths. Symmetric encryption, such as 3DES and AES, has a key length range of 128–256 bits, while asymmetric encryption, such as RSA, has a key length range of 1024–4096 bits.[73] However, the longer the key, the more difficult and time-consuming it is to encrypt or decrypt data.[14]

3.2.3 | Key governance

To preserve the keys inside the CSP, key governance can be given as a service in the Cloud. However, data owners may not ensure the privacy of their keys. That is why hardware privacy modules were developed to enable key governance systems and provide an appropriate level of protection for encryption keys.[58] In terms of maintaining and preserving cryptographic keys, the technology of hardware privacy modules provided a considerable benefit.[75] Some of the key governance methods were provided such as using a group key governance system for handling encryption keys and limiting their distribution to only authenticated persons[14] as well as deploying a system for master and session key governance.[45]

TABLE 2 Key management attributes.

Privacy-preserving attribute	Study	Characteristics
Key generation technique	[11,48]	• Pair of private and public encryption keys • IGen is used to generate signing keys, SGen is used to generate symmetric keys, and PGen is used to generate public keys
Key length	[14,73]	• 56, 128, 512, and 1024-bit key length • Random key length
Key governance	[14,45]	• Group key governance system • System for master and session key governance
Key function	[69,73]	• Authentication, encryption, verification, master key, and digital signature

3.2.4 | Key function

The actions or responsibilities that a cryptographic key performs to give privacy capabilities to a certain entity are referred to as key functions. The kind and privacy features of the cryptographic key may vary.[69] Authentication, encryption, verification, master key, and digital signature are all functions of the cryptographic key.[73] These features may provide additional levels of protection to firewalls, preventing risks like message manipulation, masquerade, and other types of cyber-attacks.[69]

3.3 | Test management

The most important actions in the privacy-preserving technique are tests. Several performance assessment tests are usually required following the installation of a privacy-preserving technique.[76] These tests aid in the detection of performance flaws, vulnerabilities, potential privacy threats, and probable faults that might cause the technique's functionality to implode during a particular technique.[77] This category has two attributes: test environment and test applied. The next sections go through these attributes. Table 3 summarizes the test management category attributes.

3.3.1 | Test environment.

The test environment is a set of hardware, software, and networks that are used to assess the performance of privacy-preserving techniques.[39] It provides a suitable work environment for privacy-preserving technique creators to conduct testing operations.[51] Leading chipmakers including ARM, AMD, Qualcomm, and Intel have created such hardware.[15] Because both testing software and hardware have the same goal of guaranteeing the proper implementation of privacy-preserving techniques, they are more similar.[52]

3.3.2 | Test applied

Because of the importance of performance and efficiency testing in the privacy-preserving technique, they have been given top consideration. Tests such as session management and broken authentication, SQL injection, poor traffic, and cross-site request forgery were used in the previous work.[10] To prevent malevolent attackers from tampering with data, the zero-knowledge shuffle correctness proof test was introduced by Yuan et al.[11] Traditional tests, such as storage, time, and cost analyses, were used by several authors.[12–14] Other tests include a user accountability test to determine whether Cloud consumers are trustable, a data confidentiality test to determine whether data is transmitted securely between Cloud entities without alteration or theft attempts, and a test to determine whether the third-party authority is leaking data.[11] Moreover, SQL operations were used to compute the average execution time in web applications during the compatibility test.[45]

3.4 | Threat management

To acquire access to sensitive data, an attacker may use a variety of methods to degrade the structure of the cryptosystem. The threat management category has two attributes: threat type and threats addressed. The next sections go through these attributes. Table 4 summarizes the threat management category attributes.

TABLE 3 Test management attributes.

Privacy-preserving attribute	Study	Characteristics
Test environment	[15,39]	• Java, C++ programming language • Operating system
Test applied	[10,12–14,45]	• Session management, broken authentication, SQL injection, poor traffic, cross-site request forgery • Efficiency and performance tests • Zero-knowledge shuffle correctness proof, other traditional performance tests

TABLE 4 Threat management attributes.

Privacy-preserving attribute	Study	Characteristics
Threat type	[10,78,79]	• Active and passive threats
Threat addressed	[22,69]	• Message modification, MITM, altering of message contents • Denial of service, Chosen-plaintext, Cipher-text only, data tampering

TABLE 5 Performance management attributes.

Privacy-preserving attribute	Study	Characteristics
Performance standards	[11,12,14,80]	• Average communication cost, mean response time per process for block and storage • Analysis of key recovery time, encryption/decryption time, and key computation time • Privacy of data, storage space, time spent during upload/download procedures • Auditing time vs. number of blocks, communication cost vs. number of blocks performance in terms of maintaining privacy
Abnormality	[10,11,13,44]	• Certify the third-party authority using an automatic blocker protocol • Path-ORAM is a special Cloud storage architecture that decreased the cost of establishing a secure and reliable communication system • Authenticate data blocks using the Merkle hash tree
Privacy achievements	[81–83]	• Ensures the accuracy and transparency of data and the availability of services • Cloud data integrity and consistency are ensured by high-level privacy features • Unauthorized individuals are unable to do any actions on Cloud data, and the server is unable to reveal any sensitive data without the usage of access patterns

3.4.1 | Threats type

Creating a risk assessment report necessitates an understanding of the many types of privacy threats that will befall the system. A risk assessment or risk evaluation assists privacy-preserving technique designers in determining the sort of attack that may be launched against the system.[78,79] Early detection of such threats can help to strengthen the technique's privacy features. In terms of the sorts of privacy threats, our analysis shows that active attacks are the most common cause of privacy breaches. While the results of other studies demonstrated that there is a possibility of passive threats.[10]

3.4.2 | Threats addressed

The number of data breaches addressed by privacy-preserving techniques to attain optimal privacy levels is referred to as the threats handled attribute. With the growth of CC services, fixing privacy system vulnerabilities and faults has become a time-consuming effort with no guarantees.[69] The protection of personal information is a crucial part of privacy-preserving technique design. It permits designers to remedy all of the flaws and holes that jeopardize the system's operation. However, unless designers engage in new technologies that reduce the overall effect of the privacy hazard, privacy-preserving techniques will be exposed to a variety of risks.[22] A typical form of attack is handled by the running method algorithm in the most privacy-preserving including known plain-text and MITM, message alteration and access pattern assaults, data tampering and denial of service attacks, message manipulation, access control attacks, chosen-plaintext, and cipher-text-only attacks.

3.5 | Performance management

Performance management aid in defining which aspects of a system should be evaluated to determine its productivity and effectiveness.[7] This category has three attributes: performance standards, abnormality, and privacy achievements. The next sections go through these attributes. Table 5 summarizes the performance management category attributes.

3.5.1 | Performance standards

Performance standards provide quantifiable attributes to be used to assess the suitability of technique designs.[80] They are the criteria through which system capabilities and efficiency may be tested. The performance standards that have been applied in privacy-preserving techniques differ significantly. For example, to determine the length of time required to transmit and receive OTP passwords, the response time and average request were plotted against the number of Cloud users as well as throughput versus the number of existing clients.[80]

The amortized cost, the mean communication overhead for both read and write processes and the mean runtime for each transaction performed versus both storage and block sizes are all factors that were used to evaluate the performance of privacy-preserving techniques.[11] While others used other multiple variables as an evaluation standard to compare the proposed technique to other previous techniques like AES and DES, such as key recovery period, key computation time, and encryption/decryption time.[14] Moreover, auditing time vs. the number of blocks, communication cost vs. the number of blocks during an auditing process in which data is transmitted, and privacy-preservation performance during active attacks are other criteria suggested for evaluating privacy-preserving level.[13] Another metric that assesses the time required to complete the whole download/upload process for the proposed technique compared to other techniques was deployed also. This metric compares the storage capacity required during method execution between the suggested technique and other techniques.[12]

3.5.2 | Abnormality

The term "abnormality" refers to behavior that is out of the ordinary and differs from the norm.[40] In the context of privacy techniques, the abnormality may also indicate the design features and attributes that distinguish one privacy technique from the others.[40] The overall performance of the privacy-preserving technique is greatly influenced by unique traits and behavior. For example, an automated blocker protocol that prohibits unauthorized access to private data by issuing a stop operation to the third-party authority's auditing protocols was suggested by El-Booz et al.[10] Another method was suggested by Yuan et al.,[11] which uses Path-ORAM—a customized Cloud storage design that replaces the regular Cloud storage structure with a binary tree shape. Another method was suggested by Subha and Jayashri[13] that deployed a Merkle hash tree which is a hash-based data structure as an authentication tool to discover damaged data blocks and distinguish them from reliable ones. In Reference 44, the authors used certificates as verification for the auditing party. The third-party authority can use these certificates to tell the difference between allowed and unauthorized access to Cloud data.

3.5.3 | Privacy achievements

Another feature to evaluate for privacy-preserving techniques is privacy achievement. It may be defined as the successes or consequences of specific privacy-preserving technique functions. It provides the technique's end scores and abilities, such as obtaining information about the types of attacks resolved the level of privacy attained after implementing a specific algorithm, and a privacy assessment report that highlights critical elements that influence the final results.[81] The privacy measures applied can result in multiple privacy achievements, including the inability of unauthorized parties to deceive data and the third-party authority cannot reveal high-value data without permission. Moreover, dual key generation and encryption techniques, for example, can provide a private Cloud storage system.[82] In addition, using digital signatures and certifications can ensure the data's trustworthiness and validity. Furthermore, using a data concealing strategy and a multi-Cloud storage structure can meet two major privacy goals: data availability and integrity assurance. Finally, the triple-encryption method improves privacy by thwarting several efforts to divulge sensitive data from individual Cloud users.[83]

4 | THE PROPOSED CLOUD STORAGE FRAMEWORK

To create an efficient system, most privacy-preserving techniques employed complicated and advanced procedures. Complexity, on the other hand, may not necessarily provide positive benefits.[84] Indeed, the complexity of privacy-preserving techniques can have an impact on a variety of their functions. Complex designs are prone to issues such as cost, access, long computation times, maintenance challenges, and waste of resources.[85] To reduce the likelihood of performance issues, privacy-preserving techniques should be designed to be efficient, adaptable, and reliable.[86] The requirements, components, and process of the proposed framework are discussed in the following sections.

4.1 | Design requirements

Over the last several years, a variety of privacy-preserving techniques have been created, each with its own set of privacy features and modifications. The privacy-preserving technique, on the other hand, should be built according to design concepts and privacy-preserving attributes, as discussed in Section 3. Since many companies and online services, such as the CSPs, rely largely on what these attributes have to give, the design of privacy defenses is a delicate matter.[87] Before building the new privacy-preserving framework, a quick overview of the design elements, in addition to the discussed attributes in Section 3, must be addressed. These elements are discussed as follows according to[85,86,88]:

1. Knowledge of the technology: The privacy-preserving technique's developer should have a thorough grasp of the Cloud technology. This makes it simple for designers to solve any layout or thread issues.
2. Privacy policies and regulations: Throughout the creation of the privacy-preserving technique, a set of standards and rules should be defined that regulate the usage of services provided by the Cloud providers. Before creating any connection within the Cloud, network members must follow these requirements.
3. Auditing methods: It is highly suggested that network traffic be monitored. Whether there are network events, auditing procedures construct a watch post that keeps systems participants and data traffic under observation to detect any suspicious or odd behaviors.
4. Data segmentation: Dividing data into smaller chunks or segments has shown to be an effective way to conceal sensitive data. In addition, Cloud technology makes it possible to outsource data segments to a multi-Cloud storage technique.
5. Access control and authentication: It is critical to provide methods for controlling and governing access to Cloud services. The key to meeting privacy standards is access control measures.
6. Data encryption: Data transmitted within the Cloud environment must be protected from various cryptographic threats. At every level of the Cloud network, it is suggested that data be encrypted using adequate encryption protocols.

4.2 | Framework's components

In this part, we will combine the privacy-preserving attributes as well as the design elements into a novel framework for safeguarding Cloud storage against data privacy intrusions. The components that follow outline the structure of the proposed framework as well as the design components that are contained within it.

1. Participants: We offered three participants for this framework: the system CSP, users, and admin. The CSP provides consumers with a variety of services, including network connection, computation, and a multi-storage solution. Ordinary people wish to communicate with the CSP securely. The system administrator is in charge of several important tasks in the system, including receiving data and performing the initial AES, as well as generating a list of authorized individuals.
2. Registration: Users will be able to engage and enroll with the system, as well as take full benefit of the system's features and Cloud services, thanks to the addition of a registration process.
3. Data processing: To add some dispersion, we provided the option to divide and combine data segments. Customers are allowed to encrypt their data before outsourcing to the Cloud thanks to the installation of AES.
4. Cryptographic techniques: Two encryption levels are used to protect sensitive data. The first layer of encryption will be AES, which will be performed by authorized participants, and the second layer will be by applying Rivest-Shamir-Adleman (RSA) algorithm, which will be performed by the CSP.
5. Auditing: Internal auditing, which is conducted by the system administrator/data owner rather than a third-party auditor, is favored since internal auditing provides safer inspection than third-party auditing that may have the desire to obtain confidential material data whenever feasible.
6. Data controller function: It is necessary to provide a data controller mechanism so that data may be retrieved or stored from the Cloud storage via a CSP.
7. External assets: One of the distinctive technologies to be deployed for verification is the OTP. The OTP technology is used to generate the second level of verification for users.
8. Data combining and segmentation: Data combining and data segmentation mechanisms are used to improve the level of privacy. Before encryption, data will be segmented into smaller chunks. Data combining, on the other hand, combines all of the resultants from the decryption process segments into an outcome that may be presumed to be the actual data.
9. Multi-Cloud storage: Each Cloud storage node should hold a varied amount of data segments; hence multi-Cloud storage is suggested. The multi-storage architecture ensures data availability and anonymization in the event of storage failure.

4.3 | Functions of the proposed framework

The multi-layer encryption system contains numerous design features, such as the user interface, participants, registration, computation, data controller function, and pre-encryption function, as well as the CSP cryptographic system, as illustrated in Figure 2. Each of these functions processes

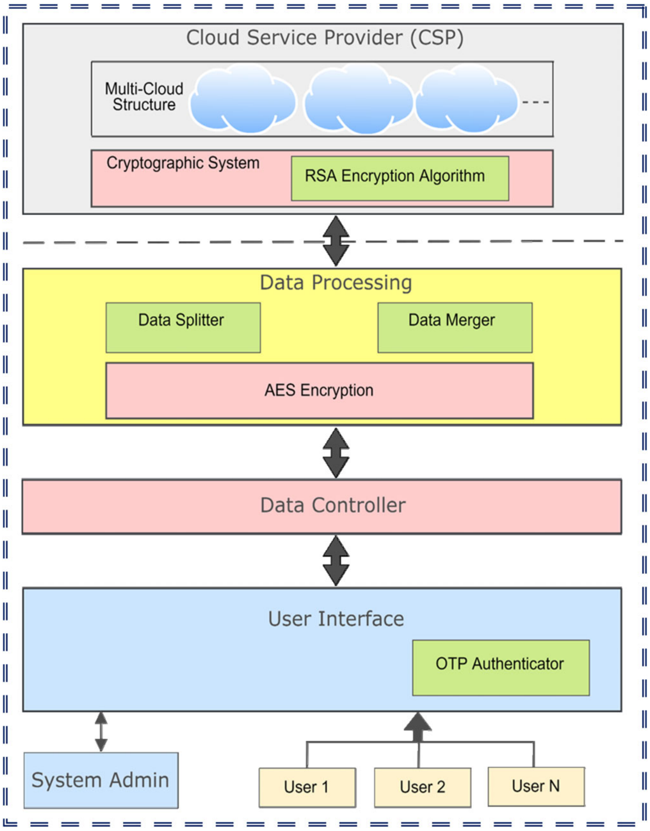

FIGURE 2 Provacy-preserving framework.

encrypts/decrypts, and transfers data in its unique way. The administrator is in charge of auditing and assessment tasks such as inspecting data transmitted, verifying user identity, and assessing the danger of potential privacy breaches. The user interface provides an appropriate setting for users to engage with the system and the Cloud services more effectively. The data controller serves as an intermediary between data and actions such as storage and retrieval. Pre-encryption and data processing are in charge of pre-processing plain data so that it may be used in the first layer of encryption. The cryptography mechanism is the framework's primary role. By creating the second encryption layer, the cryptographic system improves data confidentiality.

4.4 | The data workflow

The data flow process is covered in the following sections. The user registration, data string, and data retrieval operations are all part of this.

4.4.1 | Registration process

Users can first utilize the service's capabilities by completing enrollment requirements. Each user must fill out the registration form with their data so that it may be gathered and loaded into a database that contains all of the service's authorized users. To become an authorized user in the service and get the authentication codes, users must provide a mobile number and activate the OTP app. After each user has completed the registration procedure, the registration system generates a list of authorized users and transmits it to both the CSP and the system administrator.

4.4.2 | Storing data process

Data encryption is a simple procedure; authorized users, data owners, and system administrators may keep their data in the Cloud storage by using a multi-layer encryption technique. Users can begin the process by submitting the administrator a storage query. If the user is verified, the administrator sends an OTP code and informs the user that he or she must enter the code before proceeding with the store transaction. Users then proceed with the storage facility by passing plain data to the data controller service, which routes the data for processing and pre-encryption procedure. The user begins the data processing procedure by separating the data into numerous segments. By using AES as the initial encryption layer, each segment will be encrypted with the same algorithm. The generated encrypted segments will be directed to the CSP to finish the storing process in the following phase. However, by delivering the RSA to the CSP, this framework adds the second line of protection. Following the multi-Cloud storage structure, the second encryption will be applied to the data, and all of the encrypted segments will be delivered to diverse Cloud data storage.

4.4.3 | Retrieving Data Process

Initially, authorized users make a query to the administrator for a retrieve action. The same authentication method is used here, by verifying the user's identity through the OTP technique. After authentication, users can continue the retrieval process. The CSP delivers a query to the user that wishes to get data segments from the Cloud repository as the first stage in the retrieval process. The users will be required to supply their private key to enable the CSP to decrypt the outer layer, which was encrypted using RSA, and deliver it to the users (since the CSP encrypted the data with a shared public key). The processing module will then decrypt the encrypted segments in the inner layer. Then merging algorithm will return the details to the data's original format. Then the original data are handled by the data controller, which will route data to the user interface, after being checked for integrity by the administrator.

4.5 | Data-related operations in Cipher text domain of the proposed Cloud storage framework

Data-related operations in the ciphertext domain provide ways to manipulate encrypted data while preserving privacy and security. These operations enable computations on encrypted data without the need for decryption. Here are several common data-related operations in the ciphertext domain:

1. *Homomorphic encryption*: Homomorphic encryption allows computations to be directly performed on encrypted data, generating an encrypted output that, when decrypted, corresponds to the result of the computation on the plaintext. Addition and multiplication operations on ciphertexts are supported.
2. *Addition*: Homomorphic encryption schemes often allow addition operations on ciphertexts. Adding two ciphertexts generates a new ciphertext that, upon decryption, yields the sum of the corresponding plaintexts.
3. *Multiplication*: Certain homomorphic encryption schemes support multiplication operations on ciphertexts. Multiplying two ciphertexts produces a new ciphertext that, when decrypted, yields the product of the corresponding plaintexts.
4. *Comparison*: Ciphertexts can be compared in the ciphertext domain to determine relationships between encrypted values. Comparison operations enable determining if one ciphertext is greater than, less than, or equal to another ciphertext without decrypting them.
5. *Subset and superset operations*: Operations can be performed to determine if one ciphertext represents a subset or superset of another ciphertext. This facilitates set-related operations on encrypted data.
6. *Search operations*: Techniques like searchable encryption enable searching encrypted data without exposing the actual content. Encrypted search operations involve building searchable indices on encrypted data, allowing efficient retrieval based on specific search criteria.
7. *Secure multiparty computation* (*MPC*): MPC protocols enable multiple parties to collaboratively compute a function on their encrypted inputs without revealing their private data. Encrypted data can be used in collaborative computations while maintaining privacy.

The availability and feasibility of these above operations can vary depending on the chosen encryption scheme and its level of homomorphic properties. Different encryption schemes provide varying degrees of homomorphism, which affects the practicality and efficiency of specific operations within each scheme.

4.6 | Implementation steps of the proposed Cloud storage and privacy framework

Creating and deploying the proposed cloud storage and privacy framework involves several essential steps to guarantee the security and authenticity of user data. Below is an outline of the process:

Step 1: Requirement assessment: Gain an understanding of the specific needs and prerequisites of the cloud storage solution, including data types, storage capacity, access control, and privacy regulations.

Step 2: Architecture planning: Develop a comprehensive architecture that focuses on data privacy, encryption, access controls, and data segregation. Consider utilizing a multi-layered security approach to protect data at rest and in transit.

Step 3: Infrastructure setup: Implement the necessary infrastructure, including servers, storage devices, and network components. It is advisable to choose reputable cloud service providers that offer robust security features and comply with privacy regulations.

Step 4: Data encryption: Deploy robust encryption techniques to secure data both during transit and while at rest. Employ industry-standard encryption algorithms and ensure secure key management practices.

Step 5: Access control mechanisms: Establish granular access controls to manage user permissions and prevent unauthorized access. Implement authentication mechanisms such as multi-factor authentication (MFA) and role-based access control (RBAC).

Step 6: Privacy policy and compliance: Develop a comprehensive privacy policy outlining data collection, storage, and usage practices. Ensure compliance with relevant privacy regulations, such as GDPR or CCPA.

Step 7: Data segregation: Implement measures to logically and physically segregate user data. This aids in preventing unauthorized access and enhances data privacy.

Step 8: Redundancy and backup: Establish data redundancy and backup mechanisms to ensure data availability and facilitate disaster recovery. Regularly back up data to multiple locations to minimize the risk of data loss.

Step 9: Monitoring and audit: Implement robust monitoring and auditing mechanisms to promptly detect and respond to security incidents. Utilize intrusion detection systems (IDS), log analysis tools and real-time alerts.

Step 10: Incident response and recovery: Develop an incident response plan to handle security breaches or privacy incidents. Define procedures for containment, investigation, communication, and recovery.

Step 11: Regular security assessments: Conduct periodic security assessments and penetration testing to identify vulnerabilities and weaknesses. Promptly address any identified issues to maintain a secure environment.

Step 12: User awareness and training: Educate users on privacy practices, data handling procedures, and security best practices. Conduct regular training sessions to raise awareness of potential threats and reinforce secure behaviors.

Step 13: Regular updates and patch management: Stay up to date with the latest security patches and software updates. Implement a robust patch management process to address known vulnerabilities.

Step 14: Continuous improvement: Continuously monitor the cloud storage and privacy framework, evaluate its effectiveness, and make necessary improvements based on emerging technologies, threats, and regulatory changes.

Step 15: Regular audits and compliance checks: Conduct regular internal and external audits to assess compliance with privacy regulations and security standards. Promptly address any non-compliance issues.

By following these implementation and deployment steps (*Step 1* to *Step 15*), organizations can establish a robust cloud storage and privacy framework that safeguards user data, ensures compliance with privacy regulations, and maintains the trust of their customers.

4.7 | Comparison with existed techniques

In this section, we compare the proposed framework to several proposed techniques to evaluate its validity. We specifically compare it with techniques provided by.[10–14,44,45] Table 6 outlines the strengths and weaknesses of each technique as well as the proposed framework in addressing the identified privacy-preserving attributes.

El-Booz et al.[10] presented a privacy-preserving technique based on the OTP to prevent unauthorized access to Cloud storage data. Furthermore, this technique introduces a well-known tool that serves as a verification method for determining the validity and integrity of Cloud data. The authors also employed a third-party audit, which is a trustworthy authority that can detect damaged data and unlawful access to Cloud storage. Moreover, the technique incorporates a unique authentication process known as the Automatic Blocker Protocol to determine the third-party audit's sincerity, which may be tainted due to its interest in vital and sensitive data belonging to Cloud customers. In terms of privacy performance, as well as the efficacy of the techniques utilized, the access control-based technique demonstrated encouraging results.[10] However, efforts are required to establish internal auditing and cryptographic techniques.

Yuan et al.[11] introduced a privacy-preserving technique based on Oblivious Ram technology, which protects the privacy of shared data across numerous users. Path-oblivious Ram, a binary tree representation of Cloud storage, is a method for Cloud storage management provided by this technique. This method increases the efficiency of the technique while lowering the overall communication cost. Furthermore, by applying Identity-Based Signature and Basic Symmetric Cryptography algorithms, the technique prevents rogue users from generating access pattern activity. Data owners may obtain a high-efficiency degree in prior versions of the Oblivious Ram-based designs. To achieve the system's high degree of efficiency, data owners must undertake storage scrambling activity, but this activity is time-consuming, difficult, and needs a lot of effort.[11]

To satisfy the demands of IoT and the Cloud in terms of safeguarding storage and regulating access to various forms of sensitive and personal data, Kavin and Ganapathy[14] suggested a storage technique based on the Chinese remainder theorem. The Chinese remainder theorem was utilized to develop a key generation algorithm capable of producing complicated and safe keys. A key management system is also in place for safeguarding

TABLE 6 Overview of the previous privacy-preserving techniques against the proposed framework.

Study	Advantages	Limitations
[10]	• An auditing technique that uses an automated blocker authentication protocol • Authentication using OTP	• Internal auditing was replaced with third-party audits, and cryptographic techniques were used to minimize responsibility, which entails more effort.
[11]	• Obtaining a higher level of performance than existing Oblivious Ram methods • For all involved parties, it addresses the issue of access patterns	• Users must exert considerable effort to store/access certain data blocks
[14]	• The use of key management creates a secure connection with CS • Encryption, decryption, and key generation techniques based on the Chinese Remainder Theorem	• The use of standard key sizes may make establishing a particular level of privacy difficult • Complex in terms of computation
[13]	• To authenticate data blocks and eliminate the potential of a Man-in-the-Middle (MITM) attack, the Merkle Hash tree is utilized	• Instead of employing internal audits, third-party audits might expose data to other risks
[12]	• To secure data confidentiality and service availability, Lagrange interpolation and multi-Cloud storage are used	• If the attackers have more than two data blocks, they can use the interpolation polynomial to reveal the actual data
[44]	• Without adding extra privacy risks, hashed client aliases and confidentiality-based certificates increase auditing efficiency and data privacy	• When adopting third-party audits, the cost of communication rises
[45]	• SQL queries can be run on data that has been encrypted • Reduce the amount of time spent on the calculation • Encryption system with multiple layers that can handle float numbers	• It is inefficient to do a performance test on a cryptographic system • An increase in the computing cost and the amount of space required
The proposed framework	• This framework is a comprehensive attempt based on an exhaustive list of privacy-preserving attributes identified in the literature as well as design elements	• a viable mechanism for implementing Cloud scalability in the present framework is necessary

and maintaining encryption/decryption keys. The network manager or data owner can use the key management system to create an authentication system that restricts access to essential data. In terms of privacy protection, this technique yields promising results. The adoption of common key sizes, on the other hand, may make determining a certain level of privacy problematic.

To address the hazards posed by the MITM attack, Subha and Jayashri[13] developed a technique to address the possible risks that might compromise communication between customers and Cloud service providers. This technique is based on the data purity analysis approach in Cloud storage. In this technique, the use of digital signatures and certificates assures that the demand and answer messages sent are from a trustworthy source. Furthermore, customers can employ digital certificates and signatures in every connection with the Cloud service provider to guarantee that the sent data is not susceptible to attacks from malevolent attackers. However, employing third-party audits might expose data to other risks.

Jin and Wang[12] developed an improved version of the first Lagrange interpolation approach to provide a privacy-preserving technique that adheres to the data-concealing concept. In a single model, the technique combines the properties of service availability and privacy. Instead of resorting to external assets such as Reed-Solomon coding to hide sensitive data, the Lagrange approach employs the concept of data hiding. It also has the special ability to employ a multi-Cloud storage solution, which allows it to divide the client's data into various blocks and spread them over different storage settings. This technique, however, does not have the entire capacity to secure user data, but it can at least reduce total data breaches. Yang et al.[44] proposed a privacy-preserving hash-based technique. To safeguard the user's data, this technique uses an authentication method that includes the hashed client aliases feature. To accomplish privacy-preservation properties, the authentication tool has been re-developed in a way that allows it to incorporate the data identifier and hashed customer identities. In addition, confidentiality-based certificates have been established to help against data privacy assaults. However, the deployment of third-party audits might expose data to other risks.

Liu et al.[45] suggested a privacy-preserving technique that offers a realistic privacy-preserving option for creating a private Cloud database environment, according to authors. The goal of this technique was to create a private Cloud database that could apply and execute SQL queries on a variety of data encryption forms. To encrypt plain data, the authors presented a triple encryption scheme to boost privacy and improve the overall technique's efficiency. The design's distinctiveness arises from the fact that SQL commands may be run over any sort of encrypted data without putting additional strain on the Cloud service provider or user, allowing the workload to be focused only on the Cloud server. The experimental results reveal considerable reductions in computing overheads for encryption/decryption operations while maintaining the outsourced data's privacy.[45] However, doing a performance test on a cryptographic system is inefficient and may increase the processing cost and space required.

5 | DISCUSSION

Privacy of data is an important concern. This article, firstly, discusses the privacy-preserving attributes that are intended to address this important concern in the current context of Cloud storage. By providing the required elements to protect the user's privacy in Cloud storage, these attributes can assist the design of privacy-preserving techniques. By answering two predefined research questions (the privacy-preserving attributes of Cloud data storage—RQ1 and how these attributes can be met in a privacy-preserving framework—RQ2), this article investigates and provides a comprehensive set of privacy-preserving attributes and proposed a privacy-preserving framework to the Cloud data storage. The next sections go through the implications, the importance of coupling, and future directions.

5.1 | Implications

This study identified and analyzed 16 distinct privacy-preserving attributes—grouped into five categories. The research into the protection of privacy in Cloud storage is growing regularly. Most of the techniques discussed in this article rely on a single CSP, do not report key management attributes, address active threats like message modification and MITM attacks, and use traditional performance evaluation metrics like cost and time. External assets, the key length used, abnormality features, and hardware and software components employed in the test, on the other hand, were discovered to be very varied. These findings can serve as a blueprint for future studies on the subject, resulting in CC storage privacy.

Numerous key elements in the literature can help determine the optimal background to create an effective privacy-preserving technique for Cloud storage. To survive various privacy infractions, privacy-preserving techniques must be adaptive and cohesive in design. It is strongly advised that such a technique employs an internal auditing procedure, which is more dependable and efficient than third-party auditors, who are frequently untrustworthy and may put Cloud services in danger. Cryptography techniques, on the other hand, are preferred to utilize asymmetric cryptography mechanisms, which use several keys for data encryption and decryption, and they are more responsible and dependable than other techniques. When delegating to Cloud storage, it is also critical to encrypt vital data at every level of data transference. Data privacy will be ensured via iterative encryption, which will prohibit CSPs from tampering with sensitive data. External algorithms should not be very complex, as this might degrade the scheme's overall effectiveness. However, key generation mechanisms should be complicated and include a variety of algorithms.

When it comes to CC, if Cloud server resources are scarce, then scalability may play a significant attribute in the privacy-preserving technique.[89] Unfortunately, in the environment of CC, privacy issues have become a major issue, and using the scalability function may be inefficient or detrimental.[89] According to *The Wall Street Journal*, the Coronavirus epidemic has resulted in a massive surge in the use of Google, Amazon, and Microsoft's data storage.[90] PaaS, which can be implemented by expanding the number of database imitations, and IaaS which can be depicted by expanding the number of virtual machines or attaching load balancers, are two ways presented in Reference89 to endorse the scalability characteristic for the CC services. There are a few privacy-preserving techniques that adopted scalability features including the HASBE[87,91] and MapReduce.[92,93]

Because of the flexibility and efficiency that key management solutions provide such as key distribution among users, safe key storage, and revising certificates and regulations, privacy-preserving techniques must contain them. To avoid brute-force attempts and other types of attacks on cryptographic keys, key lengths should be sufficiently substantial and unpredictable. Random and big keys, on the other hand, may take a long time to analyze and decrypt, but they can provide good protection of data. Furthermore, the privacy-preserving techniques must have several means to validate the communications created within the Cloud network, as well as a variety of key functions to assure maximum privacy.[57]

To establish which kinds of attacks put Cloud storage in jeopardy and which types of attacks the technique can counter, privacy issues must be thoroughly investigated. The test environment should be flexible and consistent with the established technique, such as the use of suitable hardware and software, adequate programming language expertise, and selection of the right Cloud server. Similarly, assessment tests to determine the number of alternatives that the technique can supply should be conducted. Data sets, mathematical forms, and distinctive calculations are examples of exceptional elements that must be included in the development of privacy-preserving techniques.[94] These additions improve the technique's effectiveness and add another level of protection. Moreover, privacy-preserving techniques should be enthusiastic to achieve meaningful and successful outcomes. The application of proper tools in each model might result in a strong technique that can reverse the tide in the case of data breaches.

5.2 | Importance of coupling in the proposed Cloud security storage model

Reducing the coupling of a system refers to minimizing the interdependencies and interactions between its components. This is done to improve the system's flexibility, modularity, and maintainability. By reducing coupling, changes to one component are less likely to affect other components, resulting in a more robust and scalable system. In the multi-layer encryption system proposed by the author, each function is responsible for encryption and decryption operations. This creates a coupling between the data processing function and the encryption/decryption function of the system. Essentially, the data processing function relies on the encryption/decryption function to perform its operations effectively. It is important to note that the coupling in this case is intentional and necessary for the proper functioning of the encryption system. Encryption and decryption are crucial operations in ensuring data security, and they need to be tightly integrated with the data processing function to achieve the desired level of protection.

While it is true that this coupling increases the interdependencies between the data processing function and the encryption/decryption function, it does not necessarily mean that the overall system is less optimized. In the context of an encryption system, it is expected that encryption and decryption operations will be closely coupled with the data processing function. This tight coupling ensures that the data processing function operates on encrypted data when required and can securely decrypt it when necessary. The authors likely made a deliberate design choice to prioritize security over reducing coupling in this specific case. By integrating the encryption and decryption operations directly into the system's functions, the author ensures that data remains encrypted during processing and is only decrypted when needed. This approach aligns to create a robust and secure multi-layer encryption system.

Hence, it can be said that while the coupling between the data processing function and the encryption/decryption function may increase in the multi-layer encryption system, it is a deliberate design choice to ensure data security. The coupling is necessary to properly handle encryption and decryption operations within the system and does not necessarily imply that the system is less optimized overall.

5.3 | Conceptual examples of the proposed Cloud storage privacy-preserving model

The conceptual framework for Cloud Storage Privacy-Preserving involves various techniques and approaches to safeguard the confidentiality and security of data stored in the cloud. Here are a few examples that illustrate this framework:

1. *Data encryption*: Cloud storage providers can utilize encryption algorithms to safeguard data both at rest and in transit, preventing unauthorized access.
2. *Secure multi-party computation*: This technique allows multiple parties to collaboratively perform computations on shared data while preserving privacy and confidentiality.
3. *Secure data deletion*: Cloud storage providers should ensure the permanent and unrecoverable deletion of data to prevent any unauthorized retrieval.
4. *Privacy-preserving auditing*: Techniques like zero-knowledge proofs enable users to verify data integrity without exposing its contents, ensuring privacy.
5. *Data minimization*: Storing only essential data and removing or anonymizing personally identifiable information helps reduce privacy risks.
6. *Anonymization*: Personal data can be protected by removing direct identifiers or substituting them with pseudonyms to safeguard privacy.
7. *Secure data transfer protocols*: Utilizing secure protocols such as SSL/TLS during data transfer guarantees encryption and data integrity.
8. *Privacy policies and transparency*: Cloud storage providers should maintain transparent privacy policies and disclose data handling practices to build user trust.
9. *Privacy impact assessments*: Conduct assessments to identify and mitigate privacy risks associated with cloud storage systems.
10. *Consent management*: Implementing mechanisms to manage user consent and permissions for data storage and processing.
11. *Secure key management*: Employ robust practices to safeguard encryption keys and prevent unauthorized access to data.
12. *Data classification and segregation*: Categorizing data based on sensitivity and segregating it accordingly limits access and minimizes privacy risks.
13. *Secure authentication and identity management*: Implementing strong authentication mechanisms and proper identity management prevents unauthorized access.
14. *Anomaly detection*: Deploying techniques to identify unusual activities or access patterns that may indicate privacy breaches.
15. *Data leakage prevention*: Implementing measures to prevent accidental or intentional data leakage from the cloud storage environment.
16. *Regular security audits*: Conduct periodic security audits to identify vulnerabilities and ensure continuous improvement of privacy-preserving measures in cloud storage systems.

These examples (Examples 1–16) represent some of the fundamental elements and techniques within the conceptual framework for Cloud storage privacy-preserving. They aim to protect user data and maintain confidentiality in cloud storage environments.

5.4 | Impact of real-time password verification on the proposed system's performance

Applying real-time password verification in the proposed framework has implications for both system performance and potential delays. These aspects are described in Sections 5.4.1 and 5.4.2.

5.4.1 | Impact on system performance

The impacts of real-time password verification system performance of the proposed cloud storage privacy model are as follows:

1. *Authentication overhead*: The inclusion of real-time password verification adds computational overhead to the system. Each time a password is entered, the system must compare it with the stored password to ensure its correctness. This verification process requires CPU cycles and memory resources, which can affect the overall system performance.
2. *Network communication*: If the password verification process involves communication with a remote server or database, the system's performance can be influenced by network latency and bandwidth limitations. The time required to transmit the password for verification and receive the verification result can introduce delays in the system.
3. *Computational complexity*: The complexity of the password verification algorithm can impact system performance. If the verification algorithm is computationally intensive or requires extensive computations, it can increase processing time and potentially affect the overall system performance.

5.4.2 | System delay

The use of real-time password verification can introduce some level of delay in the system, and its significance depends on several factors. The factors are described below:

1. *Verification process duration*: The duration of the password verification process directly affects the delay experienced by the user. If the verification process involves complex computations or requires communication with external services, then the delay can be more noticeable.
2. *User experience*: The impact of system delay on user experience varies depending on the context of password verification. In certain scenarios like user login processes, users might tolerate a slight delay during the verification process. However, in time-sensitive applications or situations that involve repeated password entry, even a small delay can become noticeable and impact user satisfaction.
3. *System load*: The overall load on the system can influence the delay experienced during real-time password verification. If the system is already handling a high volume of concurrent requests or is constrained by limited resources, the verification process may take longer, leading to increased delays.

Hence, it can be said that it is essential for system designers to strike a balance between the security provided by real-time password verification and its potential impact on system performance and delays. Implementing efficient password verification algorithms, optimizing network communication, and considering system scalability can help minimize delays and maintain an acceptable level of system performance while ensuring robust security measures.

5.5 | Future directions

This article might be expanded in terms of expanding the search area for more privacy attributes to validate this article's findings. Most privacy-preserving techniques discussed in this article, on the other hand, have been proposed without any consideration for the need of achieving scalability capability. Researchers are encouraged to endorse the idea of scalability as the Cloud privacy industry develops, as well as the notable growth in on-demand Cloud services. Future work can build on the proposed framework, in this article, for greater development and improvements, such as improving its structure by incorporating new cryptographic mechanisms that increase its efficiency. Furthermore, there are some enhancements to the authentication system that should be considered, such as integrating extra authentication mechanisms or even developing new and trustworthy authentication apps. In addition, several issues must be examined, including risk assessment criteria for potential attacks and new data pre-processing procedures. To provide a level of flexibility to the framework in case the CSP decides to extend its infrastructure, a viable mechanism for implementing Cloud scalability in the present framework is also necessary.

It is more challenging to have a thorough grasp of CC since the infrastructure is in the hands of the CSP. Furthermore, about half of the obstacles to CC adoption are caused by the absence of regulations.[95] On the other hand, emerging technologies will represent a big issue for many CC services that exist nowadays including data storage privacy. Offering services based on deep learning, artificial intelligence, machine learning, edge computing, fog computing, serverless computing, and quantum computing has grown in popularity.[96] To use these innovations to their full potential while dealing with CC and to address issues like scalability, latency, and privacy protection, new techniques, and strategies are required.[95] Ever-increasing CC bandwidth requirements are necessary due to the proliferation of IoT and mobile devices. Data must be processed in real-time, at the edge, to maximize its value.[95] CC infrastructures need to be more flexible and ready to manage more devices in the future. Create Cloud quantum computing infrastructures is most likely how we'll utilize quantum computers in the future. Quantum computing, with high processing capacity, poses a major concern for cryptography systems. As a result, it poses a severe data privacy challenge for CC data storage.[5]

For fog and edge technologies, it has become increasingly difficult to offer sufficient computational power for edge apps. There are no globally applicable regulations or guidelines for edge computing and fog computing. Fog is less adaptable than the Cloud in terms of resource allocation and has fewer capabilities. Due to the absence of data owner control over their data in fog computing, encryption, and data privacy can also represent a future concern.[96] IoT devices generate enormous volumes of data, which may be handled by sophisticated deep learning, artificial intelligence, or machine learning. These learning approaches, however, require, in addition to data, details on clients and suppliers, which compromises data privacy. It gets harder for the Cloud to set up a redundant AI-integrated edge network, for example, to handle incoming data traffic from many nodes as more enterprises migrate to a multi-Cloud environment.[97] Approximately, 30% of the total energy used by Cloud datacenters worldwide is needed for the entire transmission of such a large amount of data, and this percentage is rapidly increasing.[95] With an emphasis on power-off methods, research is needed to make sure the upcoming serverless paradigm is sustainable.[98] Moreover, to offer all stakeholders a safe environment that facilitates this paradigm change, the privacy techniques established for serverless computing require special consideration, which might represent a challenge in the future.[5]

6 | CONCLUSIONS

CC has been regarded as one of the areas of interest, which is subject to continuous attention for processing and managing data in the online environment. Privacy techniques were created to enable and provide a variety of privacy-preserving attributes for safeguarding users' privacy and data privacy. Accordingly, before building the framework, it was essential to identify a comprehensive set of privacy-preserving attributes of Cloud data storage. The nature of these attributes provides a feature that allows a privacy-preserving framework to adapt to different types of cyber threats. This study identified and discussed 16 attributes that were organized into five attribute categories: design management, key management, test management, threat management, and performance management. Each category includes relevant attributes.

After identifying the privacy-preserving attributes and combining the multi-Cloud storage structure and the OTP authentication mechanism, this study proposed a unique multi-layer encryption framework to maintain data privacy in Cloud storage. This framework was developed based on the privacy-preserving attributes and the main phases of the design guidelines to construct a trustworthy and appropriate Cloud privacy solution that can address threats to data kept on Cloud storage. The findings of this article can serve as a blueprint for future research, resulting in a CC environment that is private and efficient. The findings will not only assist scholars and practitioners in evaluating and improving existing privacy techniques but will also help them to develop new techniques for the evolving Cloud storage and relevant privacy threat landscape. Such a study might be expanded by identifying other privacy-preserving attributes that would improve the overall outcome of the proposed framework.

FUNDING INFORMATION

The authors declare that the study was not funded. In case of acceptance funding will be provided by the open access fund of the University and Norwegian Universities' agreement with Springer open access publications.

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no competing interests.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

ORCID

Alok Mishra https://orcid.org/0000-0003-1275-2050

REFERENCES

1. Akremi A, Rouached M. A comprehensive and holistic knowledge model for cloud privacy protection. *J Supercomput*. 2021;77:7956-7988.
2. Salek MS, Khan SM, Rahman M, et al. A review on cybersecurity of cloud computing for supporting connected vehicle applications. *IEEE Internet Things J*. 2022;9:8250-8268. doi:10.1109/JIOT.2022.3152477
3. Rashid Z, Noor U, Altmann J. Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. *Fut Gener Comput Syst*. 2021;124:436-466.
4. Mishra A, Alzoubi YI, Gill AQ, Anwar MJ. Cybersecurity enterprises policies: a comparative study. *Sensors*. 2022;22:538.
5. Gill SS, Kumar A, Singh H, et al. Quantum computing: a taxonomy, systematic review and future directions. *Softw: Pract Exp*. 2022;52:66-114.
6. Kumar R, Goyal R. On cloud security requirements, threats, vulnerabilities and countermeasures: a survey. *Comp Sci Rev*. 2019;33:1-48.
7. Gupta BB, Agrawal DP, Haoxiang W. *Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives*. CRC Press: Taylor & Francis Group; 2019.
8. Alzahrani A, Alyas T, Alissa K, Abbas Q, Alsaawy Y, Tabassum N. Hybrid approach for improving the performance of data reliability in cloud storage management. *Sensors*. 2022;22:5966.
9. Jayaraman I, Stanislaus Panneerselvam A. A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud. *J Amb Intell Human Comput*. 2021;12:4911-4924.
10. El-Booz SA, Attiya G, El-Fishawy N. A secure cloud storage system combining time-based one-time password and automatic blocker protocol. *EURASIP J Inform Sec*. 2016;2016:1-13.
11. Yuan D, Song X, Xu Q, et al. An ORAM-based privacy preserving data sharing scheme for cloud storage. *J Inform Sec Appl*. 2018;39:1-9.
12. Jin Y, Wang Y. An improved scheme of privacy preserving based on Lagrange interpolation in cloud storage. *In Proceedings of the 2nd International Conference on Artificial Intelligence and Industrial Engineering (AIIE 2016)*. Atlantis Press; 2016:424-428.
13. Subha T, Jayashri S. Efficient privacy preserving integrity checking model for cloud data storage security. *In Proceedings of the 8th International Conference on Advanced Computing (ICoAC)*. IEEE; 2017:55-60.
14. Kavin BP, Ganapathy S. A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications. *Comput Netw*. 2019;151:181-190.
15. Fritze M, Schiller-Wurster K. Time to get serious about hardware cybersecurity. Accessed March 2, 2022 2018 https://www.defenseone.com/ideas/2018/01/time-get-serious-about-hardware-cybersecurity/145210/
16. Kalaivani A, Ananthi B, Sangeetha S. Enhanced hierarchical attribute based encryption with modular padding for improved public auditing in cloud computing using semantic ontology. *Clust Comput*. 2019;22:3783-3790.
17. Alzoubi YI, Al-Ahmad A, Kahtan H. Blockchain technology as a fog computing security and privacy solution: an overview. *Comput Commun*. 2022;182:129-152.
18. Razaque A, Rizvi SS. Privacy preserving model: a new scheme for auditing cloud stakeholders. *J Cloud Comput*. 2017;6:1-17.
19. Kuang L, Tu S, Zhang Y, Yang X. Providing privacy preserving in next POI recommendation for mobile edge computing. *J Cloud Comput*. 2020;9:1-11.
20. Chamikara MAP, Bertók P, Liu D, Camtepe S, Khalil I. Efficient data perturbation for privacy preserving and accurate data stream mining. *Pervasive Mob Comput*. 2018;48:1-19.
21. Nagaraj J, Kumar P. Review on privacy-preserving in cloud computing. *Int J Comput Appl*. 2014;975:23-26.
22. Tissir N, El Kafhali S, Aboutabit N. Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *J Reliab Intell Environ*. 2021;7:69-84.
23. Ghantous GB, Gill AQ. Devops reference architecture for multi-cloud iot applications. *In Proceedings of the 20th Conference on Business Informatics (CBI)*. IEEE; 2018:158-167.
24. Singh N, Singh AK. Data privacy protection mechanisms in cloud. *Data Sci Eng*. 2018;3:24-39.
25. Joseph NM, Daniel E, Vasanthi N. Survey on privacy-preserving methods for storage in cloud computing. *In Proceedings of the Amrita International Conference of Women in Computing*. International Journal of Computer Applications® (IJCA); 2013:1-4.
26. Bhagyashri S, Gurave Y. A survey on privacy preserving techniques for secure cloud storage. *Int J Comput Sci Mobile Comput*. 2014;3:675-680.
27. Liu Y, Sun YL, Ryoo J, Rizvi S, Vasilakos AV. A survey of security and privacy challenges in cloud computing: solutions and future directions. *J Comput Sci Eng*. 2015;9:119-133.
28. Li J, Yan H, Zhang Y. Identity-based privacy preserving remote data integrity checking for cloud storage. *IEEE Syst J*. 2020;15:577-585.
29. Waqar A, Raza A, Abbas H, Khan MK. A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata. *J Netw Comput Appl*. 2013;36:235-248.
30. Gundert L, Shen M-Y, Lee M. Understanding security through probability. Accessed March 1, 2022 https://blogs.cisco.com/security/understanding-security-through-probability
31. Karthiban K, Smys S. Privacy preserving approaches in cloud computing. *In 2018 2nd International Conference on Inventive Systems and Control (ICISC)*, IEEE; 2018:462-467.
32. Zhang X, Yang C, Nepal S, Liu C, Dou W, Chen J. A MapReduce based approach of scalable multidimensional anonymization for big data privacy preservation on cloud. *In 2013 International Conference on Cloud and Green Computing*. IEEE; 2013:105-112.
33. Nuray R, Can F. Automatic ranking of information retrieval systems using data fusion. *Inf Process Manag*. 2006;42:595-614.
34. Prasad VK, Shah M, Patel N, Bhavsar M. Inspection of trust based cloud using security and capacity management at an IaaS level. *Proc Comput Sci*. 2018;132:1280-1289.
35. Ibrahim FA, Hemayed EE. Trusted cloud computing architectures for infrastructure as a service: survey and systematic literature review. *Comput Secur*. 2019;82:196-226.
36. Torkura KA, Sukmana MI, Cheng F, Meinel C. Continuous auditing and threat detection in multi-cloud infrastructure. *Comput Secur*. 2021;102:102124.
37. Rizvi S, Karpinski K, Kelly B, Walker T. Utilizing third party auditing to manage trust in the cloud. *Proc Comput Sci*. 2015;61:191-197.
38. Gupta L, Salman T, Ghubaish A, Unal D, Al-Ali AK, Jain R. Cybersecurity of multi-cloud healthcare systems: a hierarchical deep learning approach. *Appl Soft Comput*. 2022;118:108439.
39. Hamilton T. Test environment for software testing. Accessed March 1, 2022. https://www.guru99.com/test-environment-software-testing.html

40. Dong B, Chen Z, Wang H, et al. Efficient discovery of abnormal event sequences in enterprise security systems. In *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*. ACM; 2017:707-715.
41. Zhang Z, Zhang W, Qin Z. A partially hidden policy CP-ABE scheme against attribute values guessing attacks with online privacy-protective decryption testing in IoT assisted cloud computing. *Fut Gener Comput Syst*. 2021;123:181-195.
42. Yi P, Li J, Liu C, et al. An efficient identity-based signature scheme with provable security. *Inform Sci*. 2021;576:790-799.
43. Gao G, Fei H, Qin Z. An efficient certificateless public auditing scheme in cloud storage. *Concurr Comput: Pract Exp*. 2020;32:e5924.
44. Yang Z, Wang W, Huang Y, Li X. Privacy-preserving public auditing scheme for data confidentiality and accountability in cloud storage. *Chin J Electron*. 2019;28:179-187.
45. Liu G, Yang G, Wang H, Dai H, Zhou Q. QSDB: an encrypted database model for privacy-preserving in cloud computing. *KSII Trans Internet Inform Syst*. 2018;12:3375-3400.
46. Garg N, Bawa S, Kumar N. An efficient data integrity auditing protocol for cloud computing. *Fut Gener Comput Syst*. 2020;109:306-316.
47. Schneier B. Key management. *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*. Wiley; 2015:169-187.
48. Chinnasamy P, Padmavathi S, Swathy R, Rakesh S. Efficient data security using hybrid cryptography on cloud computing. In: Ranganathan G, Chen J, Rocha A, eds. *Inventive Communication and Computational Technologies*. Vol 145. Springer; 2021:537-547.
49. Domingo-Ferrer J, Blanco-Justicia A. Privacy-preserving technologies. In: Christen M, Gordijn B, Loi M, eds. *The Ethics of Cybersecurity*. Vol 21. Springer; 2020:279-297.
50. Alzoubi YI, Al-Ahmad A, Jaradat A. Fog computing security and privacy issues, open challenges, and blockchain solution: an overview. *Int J Electr Comput Eng (2088–8708)*. 2021;11:11.
51. GetConnectedBlog. The importance of product certification. Accessed March 1, 2022. https://blog.nordicsemi.com/getconnected/the-importance-of-product-certification
52. Jokela M, Kutila M, Pyykönen P. Testing and validation of automotive point-cloud sensors in adverse weather conditions. *Appl Sci*. 2019;9:2341.
53. Vonnegut S. Cloud or clouds? How and why to choose a single or multi-cloud approach. Accessed March 11, 2022. https://www.stratoscale.com/blog/it-leadership/cloud-clouds-choose-single-multi-cloud-approach/
54. Tian H, Nan F, Chang C-C, Huang Y, Lu J, Du Y. Privacy-preserving public auditing for secure data storage in fog-to-cloud computing. *J Netw Comput Appl*. 2019;127:59-69.
55. Zhang L, Xiong H, Huang Q, Li J, Choo K-KR, Jiangtao L. Cryptographic solutions for cloud storage: challenges and research opportunities. *IEEE Trans Serv Comput*. 2019;15:567-587.
56. Anwar MNB, Hasan M, Hasan MM, Loren JZ, Hossain ST. Comparative study of cryptography algorithms and its' applications. *Int J Comput Netw Commun Secur*. 2019;7:96-103.
57. Li Z, Liu Y, Liu D, Li C, Cui W, Hu G. A key management scheme based on hypergraph for fog computing. *China Commun*. 2018;15:158-170.
58. Kamaraju A, Ali A, Deepak R. Best practices for cloud data protection and key management. In: Arai K, ed. *Lecture Notes in Networks and Systems*. Vol 360. Springer; 2021:117-131.
59. Abdalrdha ZK, Al-Qinani IH, Abbas FN. Subject review: key generation in different cryptography algorithm. *Int J Scient Res Sci, Eng Technol*. 2019;6:230-240.
60. Casola V, De Benedictis A, Rak M, Rios E. Security-by-design in clouds: a security-SLA driven methodology to build secure cloud applications. *Proc Comput Sci*. 2016;97:53-62.
61. Khanghahi N, Ravanmehr R. Cloud computing performance evaluation: issues and challenges. *Int J Cloud Comput: Serv Architect*. 2013;3:29-41.
62. Ezhilarasan E, Dinakaran M. Privacy preserving and data transpiration in multiple cloud using secure and robust data access management algorithm. *Microprocess Microsyst*. 2021;82:103956.
63. Sharma R, Sungheetha A. An efficient dimension reduction based fusion of CNN and SVM model for detection of abnormal incident in video surveillance. *J Soft Comput Parad*. 2021;3:55-69.
64. Tan J, Liao X, Liu J, Cao Y, Jiang H. Channel attention image steganography with generative adversarial networks. *IEEE Trans Netw Sci Eng*. 2021;9:888-903.
65. Hu J, Liao X, Wang W, Qin Z. Detecting compressed deepfake videos in social networks using frame-temporality two-stream convolutional network. *IEEE Trans Circ Syst Video Technol*. 2021;32:1089-1102.
66. Chen J, Liao X, Wang W, Qian Z, Qin Z, Wang Y. SNIS: a signal noise separation-based network for post-processed image forgery detection. *IEEE Trans Circ Syst Video Technol*. 2022;33:935-951.
67. Thompson M. CISOs should work closely with their ITAM colleagues. *Netw Sec*. 2021;2021:9-12.
68. Shukla DK, Dwivedi VK, Trivedi MC. Encryption algorithm in cloud computing. *Mater Today: Proc*. 2021;37:1869-1875.
69. Thabit F, Alhomdy S, Jagtap S. Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing. *Global Transit Proc*. 2021;2:100-110.
70. Ramalingam C, Mohan P. Addressing semantics standards for cloud portability and interoperability in multi cloud environment. *Symmetry*. 2021;13:317.
71. Alzoubi YI, Osmanaj VH, Jaradat A, Al-Ahmad A. Fog computing security and privacy for the internet of thing applications: state-of-the-art. *Sec Privacy*. 2021;4:e145.
72. Connectria.com. Why multi-cloud strategy beats single cloud almost every time. Accessed March 2, 2022. https://www.connectria.com/blog/why-multi-cloud-strategy-beats-single-cloud-almost-every-time/
73. Stubbs R. Classification of cryptographic keys. Accessed March 1, 2022, 2018. https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties
74. Amiruddin A, Ratna AAP, Sari RF. Construction and analysis of key generation algorithms based on modified fibonacci and scrambling factors for privacy preservation. *Int J Netw Sec*. 2019;21:250-258.
75. Amirany A, Jafari K, Moaiyeri MH. True random number generator for reliable hardware security modules based on a neuromorphic variation-tolerant spintronic structure. *IEEE Trans Nanotechnol*. 2020;19:784-791.
76. Yamato Y. Automatic verification technology of software patches for user virtual environments on IaaS cloud. *J Cloud Comput*. 2015;4:1-14.
77. Potter B, McGraw G. Software security testing. *IEEE Sec Privacy*. 2004;2:81-85.
78. Cayirci E, Garaga A, Santana de Oliveira A, Roudier Y. A risk assessment model for selecting cloud service providers. *J Cloud Comput Secur*. 2016;5:1-12.
79. Cayirci E, De Oliveira AS. Modelling trust and risk for cloud services. *J Cloud Comput*. 2018;7:1-16.

80. Öztayşi B, Kutlu AC. Determining the importance of performance measurement criteria based on total quality management using fuzzy analytical network process. In: Wang Y, Li T, eds. *Practical Applications of Intelligent Systems. Advances in Intelligent and Soft Computing*. Springer; 2011:391-400.
81. Bergh DD, Ketchen DJ Jr, Orlandi I, Heugens PP, Boyd BK. Information asymmetry in management research: past accomplishments and future opportunities. *J Manag*. 2019;45:122-158.
82. Yang E, Joshi GP, Seo C. Improving the detection rate of rarely appearing intrusions in network-based intrusion detection systems. *Comput Mater Contin*. 2021;66:1647-1663.
83. Turk Ž, de Soto BG, Mantha BR, Maciel A, Georgescu A. A systemic framework for addressing cybersecurity in construction. *Autom Constr*. 2022;133:103988.
84. Hu F, Qiu M, Li J, et al. A review on cloud computing: design challenges in architecture and security. *J Comput Inform Technol*. 2011;19:25-55.
85. Educative. Security on the Cloud – design principles. Accessed March 6, 2022. https://www.educative.io/courses/cloud-architecture-a-guide-to-design-and-architect-your-cloud/7nnxwPxALZj
86. Nexor. The 14 cloud security principles – what do they mean for you? https://www.nexor.com/cloud-security-principles/
87. Ahuja R, Mohanty SK, Sakurai K. A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing. *Comput Electr Eng*. 2017;57:241-256.
88. Ismail UM, Islam S. A unified framework for cloud security transparency and audit. *J Inform Secur Appl*. 2020;54:102594.
89. Patibandla R, Kurra SS, Mundukur NB. A study on scalability of services and privacy issues in cloud computing. In: Ramanujam R, Ramaswamy S, eds. *Distributed Computing and Internet Technology. ICDCIT 2012. Lecture Notes in Computer Science*. Vol 7154. Springer; 2012:212-230.
90. Tilley A. One business winner amid coronavirus lock-downs: the cloud. *Wall Street J*. 2020. Accessed August 31, 2022. https://www.wsj.com/articles/one–business–winner–amid–coronavirus–lockdowns–the–cloud–11585327905
91. Wan Z, Deng RH. HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *IEEE Trans Inform Forens Secur*. 2011;7:743-754.
92. Zhang X, Liu C, Nepal S, Yang C, Dou W, Chen J. SaC-FRAPP: a scalable and cost-effective framework for privacy preservation over big data on cloud. *Concurr Comput Pract Exp*. 2013;25:2561-2576.
93. Dean J, Ghemawat S. MapReduce: simplified data processing on large clusters. *Commun ACM*. 2008;51:107-113.
94. Khan SK, Shiwakoti N, Stasinopoulos P. A conceptual system dynamics model for cybersecurity assessment of connected and autonomous vehicles. *Acc Anal Prevent*. 2022;165:106515.
95. Gill SS, Xu M, Ottaviani C, et al. AI for next generation computing: emerging trends and future directions. *Internet Things*. 2022;19:100514.
96. Alzoubi YI, Al-Ahmad A, Kahtan H, Jaradat A. Internet of things and blockchain integration: security, privacy, technical, and design challenges. *Fut Internet*. 2022;14:216.
97. Masdari M, Khoshnevis A. A survey and classification of the workload forecasting methods in cloud computing. *Cluster Comput*. 2020;23:2399-2424.
98. Singh A, Satapathy SC, Roy A, Gutub A. Ai-based mobile edge computing for iot: applications, challenges, and future scope. *Arab J Sci Eng*. 2022;47:9801-9831.

How to cite this article: Mishra A, Jabar TS, Alzoubi YI, Mishra KN. Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework. *Concurrency Computat Pract Exper*. 2023;e7831. doi: 10.1002/cpe.7831