E-ISSN: 2707-6644
P-ISSN: 2707-6636
Journal's Website
IJCPDM 2024; 5(2): 61-67
Received: 16-10-2024
Accepted: 26-11-2024

Mohammad Khalaf Abdulmajeed
Department of Computer Sciences, College of Computer Sciences and Information Technology, University of Kirkuk, Kirkuk, Iraq

Baban Ahmed Mahmood
Department of Computer Sciences, College of Computer Sciences and Information Technology, University of Kirkuk, Kirkuk, Iraq

Corresponding Author:
Mohammad Khalaf Abdulmajeed
Department of Computer Sciences, College of Computer Sciences and Information Technology, University of Kirkuk, Kirkuk, Iraq

Cloud data deletion: Cryptographic challenges and requirements

Mohammad Khalaf Abdulmajeed and Baban Ahmed Mahmood

DOI: https://doi.org/10.33545/27076636.2024.v5.i2a.106

Abstract
The rapid development of cloud services reports a noticeably quick increase in users and things utilizing the cloud platform. The support of data storage at a very low cost, which the cloud platform provides, can reduce the storage limitation in local devices. An obvious worry, however, is raised by the data owners about the possibility of losing direct control of their outsourced data. This fear and concern have alarmed a real problem about the data confidentiality and assurance of data deletion within the utilized cloud platform. Users need to get some level of guarantee about their deleted data being away from getting recovered by unauthorized users or cloud servers. Issues about assured deletion have gained lots of attention; this paper presents a study and analysis of this topic aiming to reduce the gap by reviewing many closely relevant published literatures about assured data deletion in clouds. The advantages and limitations of most existing schemes are analyzed and discussed, together with various challenges facing the issue of assured deletion. Moreover, the paper identifies some supporting proposals for future research, which will dig further into this area. The basic set of challenges and requirements for approaching best practices to gain and possibly developing new techniques for assured deletion are presented in this paper.

Keywords: Data deletion, cloud storage, cryptography, access control, data privacy

Introduction
Cloud computing has become the most growing utilized computation model. Point it to the modern era because it is easy to use by providing better services for those who do not want to buy expensive hardware and instead rent in the cloud. Cloud computing can be used in marketing, storage, applications, servers, business, etc. [1, 2]. These services are frequently used in both daily life and the workplace [3]. Therefore, many companies and people have benefited from the use of the cloud by decreasing the overhead of their data management in a wide range. Also, it encourages more use of the cloud by uploading private data such as financial accounts, e-mails, and health records [4]. Despite many cloud computing issues such as Attacks by other customers, Security of third-party access, Failures in Providers' Security, Availability and reliability issues, Lack of security and quality levels, and Identity and access management [2]. Nevertheless, Users absolutely lose control over the uploaded data as soon as they upload their personal information to cloud storage, leading to a serious problem through a breach of data security and data integrity, which allows the hacker, the cloud service provider, or the unauthorized user to access, modify, or manipulate personal data. Toward this end, many suggested schemes came into existence. They are attribute-based encryption (ABE) [5], role-based access control (RBAC) [6], policy-based puncturable encryption (P-PUN-ENC) [5], etc. Unfortunately, there was no finding system to provide all these features to solve all issues [7, 8]. Potential risks include attacks by other customers sharing the same cloud infrastructure, security vulnerabilities arising from third-party access, failures in the security measures implemented by cloud providers, availability and reliability issues, and deficiencies in security and quality levels [7-9]. These problems remain to be solved through several methods and mechanisms [4]. Many suggestions study the possibility of issuing assured deletion and data integrity in the cloud. To overcome the difficulties and challenges by creating a technique that can provide the appropriate level of security for uploading data, which presents a study that tackles the requirements, theories, and challenges of assured deletion. To maintain a high level of security, it is crucial to prevent a user's information leakage.

Since there are four main techniques for ensured data deletion attribute-based encryption (ABE), proven data possession (PDP), overwrite-based and blockchain-based. We will explore how to implement trust data deletion and verification for cloud data [10]. Choosing the proper method depends on the flexible access control policy, authentication, authorization, verification, key management, and execution environment. Three main features need to be achieved when accessing the cloud, namely authentication, authorization, and auditing (AAA) [11, 12].

The structure of this paper is as follows: Section 2 presents the literature review. In Section Three, different types of assured data deletion methods are discussed. In Section Four, a thorough discussion of the surveyed protocols is presented. In Section Five, we conclude and summarize this paper.

Literature Review

Joshi and Panhchal [13] proved that the need for current assured deletion when the customer does not trust the cloud service provider was necessary. Wang and Luo [14] explained a brief of cloud data deletion based on cryptography from the perspective of having or not having a third-party key management center. Aziz and Mahmood [15] explored the proposed solutions classified by scaling overhead, trusted third parties, single point of failure, delays, and other reasons for inefficiencies. Thames and Barsoum [16] presented the efforts to delete private data from the cloud, just as cloud service providers offer technologies that facilitate storage operation and pointed to the requirement of services as fine-grained cloud computation. Lim *et al*. [17] viewed the research gaps of valid authentication infrastructure. And discuss the strengths and limitations of different authentication strategies. And highlight open issues and main challenges in this relevant area. Ramokapane *et al*. [18] Study assessing assured deletion criteria, presenting numerous problems, and finding cloud factors that threaten ensured deletion. Finally, systematization of challenges and requirements of assured deletion in the cloud. Sun *et al*. [19] reviewed different security challenges and techniques from both hardware and software aspects for protecting data in the cloud and aimed at improving privacy protection and data security for a trustworthy cloud server environment. Yang *et al*. [20] presented an inclusive review of the works of literature on privacy issues and data security, data encryption technology, and appropriate countermeasures in a cloud storage system. Specifically, the overview of cloud storage, with definition, architecture, classification, and application, gives a full analysis of the requirements and challenges of data security and privacy protection in cloud storage systems. Tabrizchi *et al*. [6] studied cloud computing mechanisms and security and privacy issues. They methodically investigated the security risks of the cloud, such as service providers, data owners, and cloud consumers. This study presented a number of security concerns about cloud computing services, analyzed unresolved difficulties, and suggested potential solutions. Li *et al*. [21]. A comprehensive review was conducted on various auditing schemes, focusing on two main scenarios: auditing a single copy of a file in a single cloud, and auditing multiple copies across multiple clouds in a distributed cloud system. The researchers evaluated these schemes using ten estimation criteria and highlighted several flaws in the current approaches. They emphasized the need for further research to address these shortcomings and proposed potential future research directions. One crucial issue they mentioned was the lack of systematic examination of data deletion problems in public clouds, which can have severe financial and reputational consequences if not handled properly.

Requirement for Cloud Data Deletion

In the situation. When a cloud tenant does not trust the cloud server, ensuring assured data deletion becomes more complex and critical. Here are the key requirements to be considered in such a scenario [18]:

1. **Permanent Erasure:** Deleted data must be completely and permanently removed from all storage locations, ensuring that neither cloud service providers nor attackers can recover or restore the data.
2. **Verification Capability:** Users need the ability to verify that their data has been securely deleted, using mechanisms that provide confirmation of data removal without solely relying on the cloud provider's claims.
3. **Secure Deletion Techniques:** The process must employ secure methods, such as cryptographic approaches, to guarantee that deleted data cannot be reconstructed or retrieved. Techniques like key destruction or robust encryption should render any residual data inaccessible.
4. **Independence from Trust:** The deletion mechanism should not depend entirely on the trustworthiness of the cloud service provider. Instead, it should include independent verification or cryptographic proofs to reassure users of the deletion's effectiveness.
5. **Efficiency:** The assured deletion process should be optimized to minimize impact on system performance, ensuring that it remains practical in large-scale cloud environments by keeping computational, storage, and communication costs low.
6. **Compatibility with Existing Systems:** The deletion mechanism should integrate smoothly with existing cloud storage systems, requiring minimal modifications to the infrastructure while still ensuring robust security.
7. **Legal and Regulatory Compliance:** The deletion process should adhere to relevant laws, regulations, and contractual obligations regarding data retention and deletion, ensuring it meets privacy and industry standards.
8. **Attack Resilience:** The deletion scheme must be designed to withstand potential attacks, protecting against both external and internal threats to maintain the integrity of the deletion process.
9. **Auditability:** The deletion procedure should be auditable, allowing for third-party verification to confirm that data has been securely removed, which is essential for compliance and accountability in cloud storage environments.
10. **User Authorization:** Users should maintain control over their data throughout its lifecycle, including the ability to initiate and verify deletion according to their own privacy and security requirements.

Classification Cloud Data Deletion Methods with Advantages and Limitation

Cloud services offer significant convenience for users, leading many to store large amounts of data with cloud service providers (CSPs) [22, 23, 24]. However, once data is

uploaded, ownership becomes separate from its management, resulting in users losing full control over their data. This separation introduces issues such as unauthorized access, privacy breaches, and challenges in verifying deletion. Researchers have identified various approaches to secure data deletion in the cloud. For instance, Xiong *et al*. [20] categorized these methods into three main types: trusted execution environments, key management, and access control policies. However, these approaches do not address the verification of deletion outcomes. Current research on cloud data deletion and verification can be primarily classified into four main solutions [25].

Overwrite-Based Cloud Deletion

Regarding various overwrite-based data deletion verification schemes have been proposed to ensure secure deletion of expired data in cloud environments. Each approach offers different methods for verifying deletion, including validator comparisons, encryption and re-encryption techniques, use of trusted hardware modules, and metadata validation. While these schemes enhance data deletion transparency and security, they also come with challenges such as increased computational and storage overhead or hardware limitations. Overall, these methods aim to provide stronger guarantees for data deletion in cloud storage systems.

Provable Data Possession-Based Cloud Deletion

This method proposed an enhanced data transfer and deletion verification scheme that leverages the dynamic provable data possession (PDP) mechanism to ensure secure deletion and irrecoverability of expired cloud data. By utilizing a skip-list authentication structure and allowing for a custom destruction mode, the scheme provides data owners with greater control over the deletion process. Additionally, it maintains data confidentiality through encryption and key-based partitioned storage, effectively balancing security and data management during deletion in cloud environments.

Blockchain-Based Cloud Deletion

This method introduced data deletion verification schemes utilizing blockchain technology to ensure secure and transparent deletion in cloud environments. Many approach combines a Merkle hash tree, timestamp server, and blockchain to construct a hash chain that verifies whether the CSP has deleted the expired data. Many protocol uses smart contracts for personal identity authentication and records the deletion process on the blockchain, allowing users to verify the deletion through hash values. Both schemes leverage blockchain's immutability and transparency to strengthen public verification of data deletion.

Attribute Based Encryption-Based Cloud Deletion

The proposed secure deletion solution based on Key-Policy Attribute-Based Encryption (KP-ABE) ensures data security by revoking the attributes associated with expired data, making it inaccessible. The data is encrypted and digitally signed before storage, with the Merkle Hash Tree (MHT) providing a validator for verifying deletion. While encryption protects the data, key management issues such as potential leakage persist. Additionally, PDP-based schemes, which do not delete ciphertext, expose data to unauthorized access and brute-force attacks. This work addresses these challenges by focusing on fine-grained, secure cloud data deletion and verification through flexible key management.

Study of some Cloud Data Deletion Schemes

In this section, we review some current schemes for ensuring data deletion in cloud storage. By discussing these schems and their limitations, we seek to identify the necessary criteria for reliable data deletion in cloud environments.

Assured Deletion: A Scheme Based on Strong Nonseparability

Xie *et al*. [26] the paper presents a novel approach to ensuring the assured deletion of cloud data by leveraging the concept of strong nonseparability. The main issue in cloud storage is the difficulty in ensuring that deleted data cannot be recovered by cloud servers or attackers. Traditional methods that rely on destroying encryption keys still leave the encrypted data vulnerable if the key is compromised. The proposed scheme addresses this by making the ciphertext strongly nonseparable, meaning that the loss of any part of the cipher data makes it impossible to recover the original data.The proposed scheme combines XOR operations with block ciphers to create a strongly nonseparable encryption process. When a deletion request is initiated, both the encryption key and a portion of the cipher data are destroyed, ensuring that the original data cannot be recovered. The authors compare their method with existing schemes and demonstrate through theoretical analysis and experimental results that their approach provides better security and performance.

Limitations

- **Dependence on Trusted Third Party (TTP):** The scheme relies on a trusted third party to manage the encryption keys and partial cipher data. If the TTP is compromised, the security of the scheme could be at risk.
- **Assumption of Secure Deletion:** The effectiveness of the scheme assumes that the TTP securely deletes the keys and cipher data as intended. If the deletion process is flawed or bypassed, the assured deletion may not be guaranteed.

CP-ABE-based secure and verifiable data deletion in cloud

Ma *et al*. [25] the paper presents a scheme designed to address the challenges of secure data deletion and verification in cloud environments, particularly in the context of the fifth-generation mobile communication (5G). The proposed Secure Data Deletion and Verification (SDVC) scheme is based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and aims to provide fine-grained control over data deletion while ensuring that deleted data is truly unrecoverable and that the deletion process can be verified. Key components of the SDVC scheme include: Attribute Association Tree (AAT): This structure allows for efficient management and revocation of attributes in the CP-ABE system, enabling the quick re-encryption of keys and ensuring that data associated with revoked attributes becomes inaccessible. Rule Transposition Algorithm (RTA): This algorithm is used to generate random data blocks that overwrite the expired data, ensuring that the original data is irretrievably deleted. Merkle Hash

Tree (MHT): The MHT is employed to generate a validator that can be used to verify the integrity and success of the data deletion process.

Limitations

- **Decryption Overhead:** The scheme involves some computational overhead in the decryption process, particularly when dealing with large numbers of attributes, which could impact performance in resource-constrained environments.
- **Dependence on Trusted Authority (TA):** The scheme requires a trusted authority to manage keys and attribute revocation. If the TA is compromised or becomes unavailable, the security and functionality of the scheme could be affected.
- **Scalability Issues:** The use of complex cryptographic operations and the management of large attribute sets may present scalability challenges as the system grows, particularly in environments with a large number of users or data items.

Secure data transfer and deletion from counting bloom filter in cloud computing

Changsong *et al.* [27] the paper introduces a novel scheme to ensure secure data migration between cloud service providers and reliable data deletion from the original cloud storage. With the growing reliance on cloud storage services, users often need to transfer their data between different cloud providers. However, this process raises concerns about data integrity during the transfer and the proper deletion of data from the original cloud to prevent unauthorized access. The proposed scheme uses a Counting Bloom Filter (CBF) to achieve secure data transfer and verifiable data deletion. The key aspects of the scheme include: Data Confidentiality, the data is encrypted before being transferred, ensuring that unauthorized parties cannot access the plaintext. Data Integrity, the integrity of the transferred data is verified using hash functions, ensuring that the data has not been altered during the migration process. Public Verifiability, the deletion and transfer results can be publicly verified without the need for a trusted third party (TTP). The scheme allows the data owner and the new cloud provider to verify that the original cloud provider has properly deleted the transferred data.

Limitation

- **False Positives in Counting Bloom Filter:** Although the probability of false positives in the CBF is minimized, it is not completely eliminated. This could potentially lead to incorrect verification results, though the likelihood is low.
- **Limited to Two Clouds:** The current scheme is designed for data transfer between two cloud providers. It does not address scenarios where data might need to be migrated to multiple clouds simultaneously, which could involve more complex interactions and potential collusion between cloud providers.
- **Performance Overhead:** While the scheme is designed to be efficient, there is still some computational and time overhead associated with encryption, data integrity verification, and the generation of deletion evidence.

A Secure and Efficient Fine-Grained Deletion Approach over Encrypted Data

Lavania *et al.* [28] The paper presents a Secure and Efficient Fine-Grained Deletion Approach for encrypted data stored on cloud servers. The method focuses on the deletion of specific keywords from documents without compromising the precision of ranked search queries or user privacy. The approach maintains the size of the Term Frequency-Inverse Document Frequency (TF-IDF) matrix even after processing deletion queries, ensuring that the precision of ranked search remains high. The method works by replacing deleted keywords with dummy values rather than completely removing them, thereby preserving the document's structure and avoiding significant changes to the TF-IDF matrix. This approach is efficient, privacy-preserving, and scalable, making it suitable for real-world cloud environments.

Limitations

- **Scalability with Extremely Large Datasets:** While the approach is efficient for the tested dataset of 1500 documents, its performance on significantly larger datasets with millions of documents may need further evaluation.
- **Dummy Value Selection:** The method relies on replacing deleted keywords with dummy values. However, the selection of these dummy values is crucial as improper selection could potentially impact the precision of the ranked search.
- **Partial Privacy Protection:** Although the approach obscures the deleted data, it may still be possible for a cloud provider with sophisticated methods to infer some information based on the patterns in the TF-IDF matrix, especially in cases of frequent deletions.
- **Dependency on TF-IDF:** The approach is specifically designed around the TF-IDF matrix. Other ranking or search methods might not be directly compatible without significant modifications to the algorithm.

Toward Assured Data Deletion in Cloud Storage

Zheng *et al.* [29] The article titled "Toward Assured Data Deletion in Cloud Storage" discusses the challenges and solutions for assured data deletion in cloud environments. Assured data deletion is critical for ensuring that sensitive data stored in the cloud can be permanently removed when it is no longer needed. The paper identifies several key challenges, including data migration, unauthorized access, key management, and proof of deletion, and reviews existing solutions for these issues. The authors propose several assured deletion schemes, focusing on fine granularity, availability, timeliness, and verifiability. They introduce methods such as using Rank-Based Merkle Hash Trees (RMHT) for verifying deletion and attribute-based encryption for fine-grained access control. The proposed solutions aim to address the challenges of data deletion across different cloud platforms, ensuring that deleted data cannot be recovered and providing proof that the deletion was successful.

Limitations

- **Complex Key Management:** The solutions rely heavily on complex key management systems, which can introduce additional overhead and potential points of failure, especially in scenarios with large-scale deployments and frequent key updates.
- **Scalability Issues:** While the proposed methods are efficient, their scalability to very large datasets or environments with high-frequency deletion requests is

not fully explored, which may pose challenges in real-world applications.

- **Limited Support for Dynamic Environments:** The paper primarily focuses on static scenarios and may not fully address the dynamic nature of modern cloud environments where data and access policies frequently change, requiring more adaptive deletion mechanisms.
- **Reliance on Cloud Service Providers:** The effectiveness of assured deletion often depends on the trustworthiness and compliance of cloud service providers, which could be a limitation in cases where the provider's actions cannot be fully verified.
- **Partial Solutions:** Some of the proposed solutions, such as the use of sentinel blocks or RMHTs, may only provide partial guarantees of deletion, particularly in complex cloud architectures where data replication and backup strategies are in place.

Multi-authoritative Users Assured Data Deletion Scheme in Cloud Computing

Tian *et al*. [30] the paper titled "Multi-authoritative Users Assured Data Deletion Scheme in Cloud Computing" presents a novel approach for ensuring secure and efficient data deletion in cloud environments without relying on a trusted third party. The proposed scheme, called MAU-AD, involves multiple authoritative users who jointly manage encryption keys and oversee the deletion process. The system enhances security by ensuring that no single authoritative user can compromise the data, and it introduces blockchain technology for traceability, recording actions related to data access and deletion. The scheme leverages access policy graphs for fine-grained access control, and it uses blockchain's immutability to maintain a transparent and accountable record of all operations. The inclusion of primary and subordinate authoritative users ensures system robustness, mitigating the risk of a single point of failure.

Limitations

- **High Communication Costs:** The MAU-AD scheme involves significant communication overhead due to the interaction between multiple authoritative users and the use of blockchain for recording transactions, which can impact system performance, particularly in environments with frequent data deletion requests.
- **Scalability Concerns:** While the system is designed to handle multiple authoritative users, its efficiency in larger-scale deployments with many users and large datasets remains a challenge, potentially leading to delays in key management and data access.
- **Complex Implementation:** The use of blockchain and multi-authoritative user structures introduces complexity in the system's implementation and maintenance, which may require specialized knowledge and resources.
- **Reliance on Blockchain:** The success of the system heavily depends on the integrity and performance of the blockchain network. Any issues with the blockchain, such as latency or security vulnerabilities, could undermine the overall effectiveness of the data deletion process.
- **Limited Support for Dynamic Changes:** The scheme may face challenges in adapting to dynamic changes in user access rights or system configuration, which could complicate key management and data deletion process

Secure and effective assured deletion scheme with orderly overwriting for cloud data

Tian *et al*. [31] the paper proposes SEAD-OO, a scheme designed to ensure the assured deletion of cloud data while maintaining efficiency and security. The scheme utilizes ciphertext-policy attribute-based encryption (CP-ABE) for fine-grained access control and data sharing. To prevent the persistence of encrypted data after key deletion, SEAD-OO introduces physical deletion and logical deletion mechanisms. These mechanisms, combined with deletion queues, ensure orderly and timely deletion processes. The integration of Hyperledger Fabric guarantees the traceability and verification of deletions, preventing any potential forgery of deletion proofs.

Limitations

- **Increased complexity:** The reliance on both physical and logical deletion, along with the use of multiple keys (RSA for encryption and control keys for management), may increase computational overhead, particularly in large-scale deployments.
- **Blockchain overhead:** The integration of Hyperledger Fabric for verification adds transparency but also introduces extra maintenance and scalability concerns.
- **Encryption/decryption costs:** As the number of attributes in the access policy increases, so do the costs of encryption and decryption, impacting the scheme's overall performance. This could become more significant with a higher number of attributes or users.

Secure Overlay Cloud Storage with Access Control and Assured Deletion

Tang *et al*. [32] presents FADE, a secure overlay cloud storage system that provides both fine-grained access control and assured file deletion. FADE is designed to work seamlessly atop existing cloud storage services, allowing organizations and users to outsource data to the cloud while ensuring strong security guarantees. The system associates files with user-defined access policies and ensures that files are permanently deleted and become irrecoverable upon the revocation of those policies. The system employs a combination of cryptographic techniques: Attribute-Based Encryption (ABE) for fine-grained access control, where access is governed by specific attributes linked to users. Threshold secret sharing to distribute cryptographic keys among multiple key managers, preventing any single point of failure and enhancing reliability. FADE also implements policy-based file assured deletion, where files are permanently deleted when their associated policies expire or are revoked. This deletion is achieved by erasing the cryptographic keys required to decrypt the data, even if the data remains on the cloud. FADE was tested on Amazon S3, where it was shown to provide security with minimal performance and cost overhead.

Limitations

- **Performance Overhead**: Although FADE introduces only minimal overhead, the cryptographic operations, especially with attribute-based encryption and key management, could slow down the upload/download process for larger or more complex files.
- **Scalability Concerns:** The use of multiple key

managers with threshold secret sharing, while enhancing security, could introduce scalability challenges as the number of files and policies grows.

- **Dependency on Trust**: The system relies on a quorum of key managers, which must be trusted to handle the keys securely. If any key managers are compromised, there is a risk to the security of the stored data.
- **Limited to Specific Cloud Services**: While FADE was tested on Amazon S3, the system's applicability to other cloud platforms may require further adjustments, particularly in environments with different data access protocols.

Results And Discussion

In [26] scheme, it reduces the storage, communication, and calculation overhead because it depends on XOR operation and both data encryption and decryption use shorter time compared with other operations and achieves higher security.

In SDVC [25] scheme, the time cost increases by increasing the number of attributes, encryption/decryption operation, key sizes, and the size of blocks in linearity. More security levels showed in this proposal and applied to the technique to achieve the best security steps without being concerned about the cost of equipment.

In [27] scheme, they put up a plan that can also achieve verified data deletion, allow cloud B to verify the integrity of the transferred data, and ensure that all of the data has been migrated. Additionally, cloud A should use CBF to provide deletion evidence after deletion. The outcome demonstrated a decrease in the overhead associated with time, storage, and communication. However, there is a chance of a false-positive phase, thus the other approaches are preferable to this one.

In [28] scheme, the suggested method enables high precision and fine-grained deletion, and following this deletion, it returns the keywords to the search algorithm. This demonstrates how the outcome was influenced by the quantity of documents and dictionary size. After running the deletion request query, the search time for words in the query is shorter, demonstrating linearity over time.

In [29] scheme, viewed that the reduction of block size leads to a decrease the time consumption. The time cost overhead rises as the number of attributes used in the block of ciphertext does.

In [30] scheme, gave a view of the increased costs needed to manage keys securely without the aid of a reliable third party. The outcome demonstrates a linear time cost rise with data key size and attribute count in an access control structure.

In [31] scheme, the results shows that the file size has an impact on the overhead cost of encryption, and the number of attributes has an impact as well. If the number of attributes increases, the overhead cost rises practically linearly.

In [32] scheme, presents that the running time cost increases by the size of the file and renewing the set of policies associated with files.

Table 1: Algorithms for deletion and verification use certain qualities and techniques.

Solutions	Communication overhead	Computational overhead	Proof of deletion	Third-party	Over-writing	Sharing other users	limitation
Xie *et al.* [26]	No	No	No	Yes	No	Yes	Require proper trusted third party
Ma *et al.* [25]	Yes	Yes	Yes	Yes	Yes	Yes	The third-party must be trusted key management issues
Changsong *et al.* [27]	Yes	No	Yes	Yes	Yes	No	false positive results from the counting Bloom filter
Lavania *et al.* [28]	No	Yes	No	No	Yes	No	Increasing time cost by increasing document
Zheng *et al.* [29]	No	Yes	No	Yes	Yes	Yes	Key management problem
Tian *et al.* [30]	Yes	Yes	Yes	No	No	Yes	Very complex to add any entities in future
Tian *et al.* [31]	Yes	Yes	Yes	Yes	Yes	Yes	The third party must be trusted key management issues
Tang *et al.* [32]	Yes	Yes	No	Yes	Yes	Yes	Key management problem

Conclusion

In this study, we presented the controlled and managed access and deletion to cloud data. Many schemes for many years came into existence around cloud outsourced data control. Some of the proposed schemes focus on provable data possession and auditing and proof of unrecoverability and other schemes threw light on the assured deletion of the cloud computing data. While granting privileges to accessing outsourced data depends on attributed-based encryption has got significant fine-grained control over outsourced data. In future work, the suggestion that a method that researchers can use to give us controlled access to cloud-based outsourced data with multi-attribute authority-based encryption and elliptic curve cryptography, which provide more flexibility and efficiency for auditing and verifying the outsourced data. combine any approach with predicate algorithms to extend improvement of assured deletion and security on outsourced data, and compare the pros and cons and show the drawback of different combinations.

Acknowledgements

I would like to thank the University of Kirkuk / College of Computer Science and Information Technology

References

1. Mohammad. Distributed authentication and authorization models in cloud computing systems: A literature review. Journal of Cybersecurity and Privacy. 2022;2(1):107–123. DOI:10.3390/jcp2010008.
2. Faraj ST. Trusted cloud computing. 2019;6(2):12–27. DOI:10.4018/978-1-5225-7924-3.ch002.
3. Yang C, Liu Y, Tao X. Assure deletion supporting dynamic insertion for outsourced data in cloud computing. International Journal of Distributed Sensor Networks. 2020, 16(9). DOI:10.1177/1550147720958294.
4. Mohammed H, Abdulsada A. Secure multi-keyword similarity search over encrypted data with security improvement. Iraqi Journal for Electrical and Electronic Engineering. 2021;17(2):1–10. DOI:10.37917/ijeee.17.2.1.
5. Hao J, Liu J, Wu W, Tang F, Xian M. Secure and fine-grained self-controlled outsourced data deletion in cloud-based IoT. IEEE Internet of Things Journal. 2020;7(2):1140-1153. DOI:10.1109/JIOT.2019.2953082.
6. Tabrizchi H, Kuchaki Rafsanjani M. A survey on

security challenges in cloud computing: Issues, threats, and solutions. Springer US. 2020, 76(12). DOI:10.1007/s11227-020-03213-1.
7. Juels A, Szydlo M. Attribute-based encryption: Using identity-based encryption for access control. 2004.
8. Dar AR, Ravindran D, Islam S. Fog-based spider web algorithm to overcome latency in cloud computing. Iraqi Journal of Science. 2020;61(7):1781–1790. DOI:10.24996/ijs.2020.61.7.27.
9. Younis MI, Younis MF, Abed MM, Alsewari AR. Development of an attendance system based on cloud/fog computing with data recovery capability. Iraqi Journal of Science. 2020;61(5):1190-1201. DOI:10.24996/ijs.2020.61.5.26.
10. Yang C, Tan L, Shi N, Xu B, Cao Y, Yu K. Auth Privacy Chain: A blockchain-based access control framework with privacy protection in cloud. IEEE Access. 2020;8:70604-70615. DOI:10.1109/ACCESS.2020.2985762.
11. Tian Y, Shao T, Li Z. An efficient scheme of cloud data assured deletion. Mobile Networks and Applications. 2021;26(4):1597-1608. DOI:10.1007/s11036-019-01497-z.
12. Perlman R. File system design with assured delete. Proceedings of the Third IEEE International Security in Storage Workshop; c2005. p. 83-88. DOI:10.1109/SISW.2005.5.
13. Joshi SB, Panchal SD. A survey on assured data deletion in cloud storage. International Journal of Computer Sciences and Engineering. 2019;7(6):548-553. DOI:10.26438/ijcse/v7i6.548553.
14. Wang G, Luo Y. A review on assured deletion of cloud data based on cryptography. Procedia Computer Science. 2021;187:580-585. DOI:10.1016/j.procs.2021.04.111.
15. Aziz KQ, Mahmood BA. Assured data deletion in cloud computing: Security analysis and requirements. Indonesian Journal of Electrical Engineering and Computer Science. 2022;28(2):1174–1183. DOI:10.11591/ijeecs.v28.i2.pp1174-1183.
16. Thames R, Barsoum A. Cloud storage assured deletion: Considerations and schemes. Journal of Network and Information Security. 2018;6(1):1-4. Available from: https://www.academia.edu/download/60779525/120191002-69958-1gzji89.pdf.
17. Lim SY, Mat Kiah ML, Ang TF. Security issues and future challenges of cloud service authentication. Acta Polytechnica Hungarica. 2017;14(2):69-89. DOI:10.12700/APH.14.2.2017.2.4.
18. Ramokapane KM, Rashid A, Such JM. Assured deletion in the cloud: Requirements, challenges and future directions. Proceedings of the 2016 ACM Cloud Computing Security Workshop (CCSW 2016); c2016. p. 97-108. DOI:10.1145/2996429.2996434.
19. Sun Y, Zhang J, Xiong Y, Zhu G. Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks; c2014. DOI:10.1155/2014/190903.
20. Yang P, Xiong N, Ren J. Data security and privacy protection for cloud storage: A survey. IEEE Access. 2020;8:131723-131740. DOI:10.1109/ACCESS.2020.3009876.
21. Li A, Chen Y, Yan Z, Zhou X, Shimizu S. A survey on integrity auditing for data storage in the cloud: From single copy to multiple replicas. IEEE Transactions on Big Data. 2022;8(5):1428-1442. DOI:10.1109/TBDATA.2020.3029209.
22. Ali M, Tang Jung L, Hassan Sodhro A, Ali Laghari A, Belhaouari SB, Gillani Z. A confidentiality-based data classification-as-a-service (C2aaS) for cloud security. Alexandria Engineering Journal; c2022. DOI:10.1016/j.aej.2022.10.056.
23. Patil JM, Chaudhari SS. Efficient privacy-preserving and dynamic public auditing for storage cloud. In: 2019 International Conference on Nascent Technologies in Engineering (ICNTE 2019) - Proceedings; c2019. p. 1-6. DOI:10.1109/ICNTE44896.2019.8945817.
24. Singh P, Saroj SK. A secure data dynamics and public auditing scheme for cloud storage. In: 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS 2020); 2020:695–700. DOI:10.1109/ICACCS48705.2020.9074337.
25. Ma J, Wang M, Xiong J, Hu Y. CP-ABE-based secure and verifiable data deletion in cloud. Security and Communication Networks; c2021. DOI:10.1155/2021/8855341.
26. Xie Z, Fu W, Xu J, Zhu T. Assured deletion: A scheme based on strong nonseparability. Journal of Sensors. 2022. DOI:10.1155/2022/9691724.
27. Changsong Y, Xiaoling T, Feng Z, Yong W. Secure data transfer and deletion from counting bloom filter in cloud computing. Chinese Journal of Electronics. 2020;29(2):273-280. DOI:10.1049/cje.2020.02.015.
28. Lavania K, Gupta G, Kumar DVNS. A secure and efficient fine-grained deletion approach over encrypted data. In: Proceedings of the 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC 2022); c2022. p. 1123-1128. DOI:10.1109/COMPSAC54236.2022.00176.
29. Zheng D, Xue L, Yu C, Li Y, Yu Y. Toward assured data deletion in cloud storage. IEEE Network. 2020;34(3):101-107. DOI:10.1109/MNET.011.1900165.
30. Tian J, Bai R, Zhang T. Multi-authoritative users assured data deletion scheme in cloud computing. In: Proceedings of the 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop Volume (DSN-W 2022); c2022. p. 147-154. DOI:10.1109/DSN-W54100.2022.00033.
31. Tian J, Zhang T. Secure and effective assured deletion scheme with orderly overwriting for cloud data. Journal of Supercomputing. 2022;78(7):9326-9354. DOI:10.1007/s11227-021-04297-z.
32. Tang Y, Lee PPC, Lui JCS, Perlman R. Secure overlay cloud storage with access control and assured deletion. IEEE Transactions on Dependable and Secure Computing. 2012;9(6):903-916. DOI:10.1109/TDSC.2012.49.