IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

Publicly Verifiable and Efficient Fine-Grained Data Deletion Scheme in Cloud Computing

Mr. Pradeep Nayak, Mr. Darshan K Revankar, Mr. Gautham P Kini,
Mr. Yashash Raj C G, Ms. Dikshita Devadiga
Department of CSE (IoT, Cyber Security including BlockChain)
Alva's Institute of Engineering and Technology, Mijar, Karnataka, India
pradeep@aiet.org.in, darshankrevankar@gmail.com, gautham07049@gmail.com,
yashash426@gmail.com, dikshitadishu8@gmail.com

Abstract: *This paper explores the benefits of cloud storage, a fundamental component of cloud computing, which provides users with nearly limitless storage capabilities. Users can substantially decrease their local storage requirements by allowing data to be outsourced to cloud servers. However, the paper also addresses security privacy concerns linked to cloud storage, which stem from data ownership and management division, resulting in users losing direct control over their outsourced data.*

The authors concentrate on the challenge of verifiable outsourced data deletion, a significant issue that has not been adequately addressed in either industry or academic circles. They present an effective fine-grained outsourced data deletion scheme utilizing the invertible Bloom filter. This solution facilitates both public and private verification of the storage and deletion processes. Suppose the cloud server fails to manage or remove the data accurately and creates the associated evidence. In that case, users can detect any malicious actions by the cloud server with a high likelihood.

Additionally, the authors note that within their proposed scheme, the computational complexity of both data deletion and verification of deletion results remains unaffected by the quantity of outsourced data blocks. This property makes the scheme appropriate for extensive data deletion scenarios.

Ultimately, the paper includes a thorough security evaluation and performance assessment, validating the security and practicality of the proposed scheme. This comprehensive method for tackling the issue of verifiable outsourced data deletion in cloud storage represents a notable contribution to the field.

Keywords: cloud storage

I. INTRODUCTION

Importance of Cloud Computing

The paper begins by highlighting the critical role of cloud computing in today's digital landscape. Cloud computing has transformed data storage, access, and processing methods, creating a platform where data can be stored and retrieved online, thereby eliminating the requirements for local infrastructure and processing. This transformation has led to significant cost reductions as organizations no longer have to invest heavily in on-premises hardware and software.

Benefits of Cloud Storage Several advantages of cloud storage are emphasized in the paper. Cost-effectiveness is one of the primary benefits. With data stored on remote servers, organizations can cut down expenses related to storage and maintenance. Scalability is another crucial advantage, as cloud storage enables organizations to seamlessly adjust their storage needs. Accessibility also stands out as a major benefit, allowing data to be accessed anytime and anywhere, offering remarkable flexibility and convenience.

Challenges with Data Deletion in Cloud Storage

Despite these advantages, the paper points to challenges associated with data deletion in cloud storage. It is essential to ensure that deleted data is permanently eradicated and cannot be recovered to uphold data privacy and adhere to data protection regulations. However, confirming the complete deletion of data from cloud servers proves to be a complicated task due to the distributed nature of cloud storage and the application of redundancy techniques that prevent data loss.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

The paper sets the groundwork for the authors' proposed solution to tackle these challenges, which serves as the primary focus of their research. The introduction clearly outlines the context and motivation for the study, establishing a solid understanding of the issue the authors aim to resolve.

II. PROBLEM STATEMENT

The Criticality of Verifiable Outsourced Data Deletion

The authors underscore the importance of verifiable outsourced data deletion within the realm of cloud storage. The term 'data deletion' refers to the process of irrevocably removing data from cloud servers, which is pivotal for effective data management, especially regarding privacy maintenance and compliance with data protection regulations.

Nevertheless, the authors contend that this matter has not garnered adequate focus in either industry or academia. Such neglect of verifiable data deletion could give rise to considerable security vulnerabilities. For example, if data is improperly deleted, unauthorized individuals may access or recover it, leading to breaches of privacy and potential legal complications.

The Challenge of Verifying Data Deletion

A key difficulty in this field lies in verifying that data has been deleted. When data is removed, it is crucial to confirm that it has been completely and permanently eliminated. However, due to the distributed nature of cloud storage and the redundancy techniques employed to mitigate data loss, achieving this verification is challenging.

In many current systems, users cannot see the data deletion process. Cloud service providers might simply issue a confirmation of deletion without any definitive proof. This so-called 'one-bit-return' protocol necessitates that users place a high level of trust in their cloud service provider.

The Need for a New Scheme

The authors assert that a new approach is essential for overcoming these challenges. The new scheme should guarantee not only the secure deletion of data but also allow users to confirm that deletions are executed properly.

This new approach would involve the cloud server performing data deletions and issuing a proof of deletion. Users could then verify this proof to ensure that their data has indeed been eliminated, offering a higher level of assurance and transparency than current methods.

The Complexity of Large-Scale

Data Deletion Another concern raised by the authors is the complexity associated with deleting large volumes of data. In many existing schemes, the computational complexity tied to data deletion and verification is reliant on the quantity of outsourced data blocks. This dependency makes these schemes troublesome for situations where significant amounts of data require deletion.

The authors claim that their proposed solution solves this issue by guaranteeing that the computational complexity remains independent of the number of outsourced data blocks, enhancing efficiency and practicality for large-scale data deletion.

In summary, the problem statement effectively articulates the challenges related to verifiable outsourced data deletion in cloud storage, laying the foundation for the authors' proposed solution. It emphasizes the need for a fresh approach that not only secures data deletion but also allows users to verify the process, thereby boosting the transparency and reliability of cloud storage services.

III. PROPOSED SOLUTION

The Invertible Bloom Filter

The authors introduce a novel fine-grained outsourced data deletion scheme founded on the invertible Bloom filter. This data structure is a probabilistic tool used to determine if an element belongs to a set. While traditional Bloom filters are space-efficient, they lack deletion capability. The invertible Bloom filter, in contrast, not only supports deletion but can also recover original input items.

Under the proposed scheme, the cloud server executes the data deletion and subsequently provides proof of deletion. This proof, generated via the invertible Bloom filter, ensures both space efficiency and fine-grained deletion capability. This offers a considerable advancement over existing methods, which require users to rely solely on the cloud server's deletion confirmations.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

Public and Private Verifiability

The scheme achieves both public and private verifiability regarding the outcomes of storage and deletion. Public verifiability permits anyone, not just the data owner, to confirm the accuracy of the deletion result. This aspect significantly enhances the transparency of the deletion process, allowing third-party auditors to validate the deletion result.

Conversely, private verifiability ensures that only the data owner can confirm the deletion result, which is essential for protecting data privacy. If the cloud server fails to maintain or delete the data correctly and provides corresponding evidence, users can detect such malicious activities with a very high likelihood.

Efficiency in Large-Scale Data Deletion

Within the proposed scheme, the computational complexity related to data deletion and verification does not vary with the number of outsourced data blocks. This characteristic makes it well-suited for extensive data deletion scenarios. In contrast, many existing schemes experience a rise in computational complexity relative to the number of outsourced data blocks, resulting in inefficiency and impracticality for large-scale data deletion processes.

Security Analysis and Performance Evaluation

The authors conduct a comprehensive security analysis and performance assessment of the proposed scheme. The security evaluation highlights that the scheme effectively safeguards data integrity against various threats. The performance review indicates that the scheme is efficient and practical, particularly for large-scale data deletion cases.

In conclusion, the proposed solution addresses the challenges associated with verifiable outsourced data deletion in cloud storage. It allows users to confirm the deletion of their data, enhancing the transparency of this process while remaining suitable for large-scale scenarios. The authors' findings could greatly impact the future of data security within cloud computing.

IV. PERFORMANCE EVALUATION

Performance Evaluation Overview

The authors present a thorough performance evaluation of their proposed scheme, which is essential for illustrating the scheme's practicality and efficiency, particularly in large-scale data deletion contexts.

Computational Complexity

A primary focus of the performance evaluation is the assessment of computational complexity. The authors show that the complexity involved in data deletion and verification processes does not rely on the number of outsourced data blocks. This represents a significant advancement compared to many existing schemes, where this complexity correlates with the number of data blocks outsourced.

Efficiency in Large-Scale Data Deletion

The authors affirm that their proposed scheme excels in large-scale data deletion scenarios. This efficiency stems from the likely independence of computational complexity from the number of outsourced data blocks, rendering it practical for situations involving the deletion of substantial data volumes.

The practicality of the Proposed Scheme

The authors argue that their scheme is theoretically solid and practically applicable in real-world settings. Through a detailed performance assessment, they demonstrate the scheme's efficiency and its suitability for large-scale data deletion challenges.

In summary, the performance evaluation showcases the practicality and efficiency of the proposed solution, proving that the scheme can effectively manage large-scale data deletion tasks. This positions it as a viable option for verifiable outsourced data deletion in cloud storage.

V. SECURITY ANALYSIS

Security Analysis Overview

The authors furnish a detailed security analysis of their proposed scheme, which is critical for establishing the scheme’s robustness, particularly in protecting data integrity.

Protection Against Malicious Behaviors

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

The authors illustrate that users can easily identify malicious actions by the cloud server if it fails to maintain or delete data adequately, or if it does not generate the required evidence. This provides a significant improvement over existing schemes where users must rely heavily on the cloud provider's confirmation of deletion.

Public and Private Verifiability

The proposed scheme provides both public and private verification for the results of storage and deletion. Public verifiability allows any interested party to assess the accuracy of the deletion outcome, while private verifiability restricts this capability to only the data owner, which is crucial for ensuring data confidentiality.

Security Against Various Attacks

The authors argue that their scheme is resilient to a variety of attacks and can reliably protect data integrity. This is substantiated through an in-depth security analysis demonstrating that the scheme can withstand numerous potential threats.

In conclusion, the security analysis of the proposed solution affirms its robustness and reliability. It proves capable of safeguarding data integrity, detecting the cloud server's malicious actions, and granting both public and private verification capabilities for storage and deletion outcomes.

VI. CONCLUSION

Significance of the Proposed Scheme

The authors conclude by underscoring the importance of their proposed scheme, asserting that it effectively addresses the crucial issue of verifiable outsourced data deletion in cloud storage, an area that has not received adequate consideration in either industry or academia.

Achievements of the Proposed Scheme

The scheme achieves both public and private verification for storage and deletion results, allowing anyone—not just the data owner—to confirm the accuracy of deletion outcomes. This feature enhances the data deletion process's transparency while enabling third-party auditors to verify deletion results.

Security and Efficiency of the Proposed Scheme

The authors demonstrate through extensive security analysis and performance evaluation that their scheme can withstand multiple attacks and maintain data integrity. The performance review confirms that the scheme is both practical and efficient, especially when handling large-scale data deletion tasks.

Implications for the Future of Data Security in Cloud Computing

The authors propose that their research could significantly impact the future of data security within cloud computing. By enabling users to verify the deletion of their data, the proposed scheme enhances the transparency and reliability of the cloud storage service

In closing, the authors argue that their proposed solution is both secure and practical for deployment in cloud storage systems. They suggest that this work may pave the way for future studies in this domain, contributing to the ongoing development of safer and more transparent cloud storage options.

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, ``Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Gener. Comput. Syst., vol. 25, no. 6, pp. 599_616, Jun. 2009, doi: 10.1016/j.future.2008.12.001.

[2] C. Yang and J. Ye, ``Secure and ef_cient _ne-grained data access control scheme in cloud computing," J. High-Speed Netw., vol. 21, no. 4, pp. 259_271, Nov. 2015, doi: 10.3233/JHS-150524.

[3] S. Han, K. Han, and S. Zhang, ``A data sharing protocol to minimize security and privacy risks of cloud storage in the big data era," IEEE Access, vol. 7, pp. 60290_60298, 2019, doi: 10.1109/ACCESS.2019.2914862.

[4] C. Yang and X. Tao, ``New publicly veri_able cloud data deletion scheme with ef_cient tracking," in Proc. Int. Conf. Secure. Intell. Comput. Big-data Services, Guilin, China, 2018, pp. 359_372, doi: 10.1007/978-3-030- 16946-6_28.

[5] J. Li, Y. Wang, Y. Zhang, and J. Han, ``Full veri_ability for outsourced decryption in attribute-based encryption," IEEE Trans. Services Comput., early access, May 31, 2017, doi: 10.1109/TSC.2017.2710190.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

[6] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, ``Flexible and _negrained attribute-based data storage in cloud computing," IEEE Trans. Services Comput., vol. 10, no. 5, pp. 785_796, Sep. 2017, doi: 10.1109/ TSC.2016.2520932.
[7] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, ``Security and privacy challenges in cloud computing environments," IEEE Secur. Privacy Mag., vol. 8, no. 6, pp. 24_31, Nov. 2010, doi: 10.1109/MSP.2010.186.
[8] J. Li, H. Yan, and Y. Zhang, ``Certi_cateless public integrity checking of group shared data on cloud storage," IEEE Trans. Services Comput., early access, Jan. 8, 2018, doi: 10.1109/TSC.2018.2789893.
[9] H. Yan, J. Li, J. Han, and Y. Zhang, ``A novel ef_cient remote data possession checking protocol in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 12, no. 1, pp. 78_88, Jan. 2017, doi: 10.1109/TIFS.2016.2601070.
[10] J. Li, H. Yan, and Y. Zhang, ``Ef_cient identity-based provable multi-copy data possession in multi-cloud storage," IEEE Trans. Cloud Comput., early access, Jul. 16, 2019, doi: 10.1109/TCC.2019.2929045.
[11] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, and K. Muhammad, ``The impact of the hybrid platform of Internet of Things and cloud computing on healthcare systems: Opportunities, challenges, and open problems," J. Ambient Intell. Hum. Comput., vol. 10, no. 10, pp. 4151_4166, Oct. 2019, doi 10.1007/s12652-017-0659-1.
[12] M. Paul and A. Saxena, ``Proof of erasability for ensuring comprehensive data deletion in cloud computing," in Proc. Int. Conf. Netw. Secure. Appl., Chennai, India, 2010, pp. 340_348, doi: 0.1007/978-3-642 14478-3_35.
[13] L. Du, Z. Zhang, S. Tan, J. Wang, and X. Tao, ``An associated deletion scheme for multi-copy in cloud storage," in Proc. Int. Conf. Algorithms Archit. Parallel Process., Guangzhou, China, 2018, pp. 511_526, doi: 10.1007/978-3-030-05063-4_38.
[14] C. Yang, X. Tao, F. Zhao, and Y. Wang, ``A new outsourced data deletion scheme with public veri_ability," in Proc. 14th Int. Conf. Wireless Algorithms, Syst., Appl., Honolulu, HI, USA, 2019, pp. 631_638, doi: 10.1007/ 978-3-030-23597-0_53.
[15] C. Yang, X. Tao, and Q. Chen, ``New publicly veri_able data deletion supporting ef_cient tracking for cloud storage," Int. J. Netw. Secur., 2020.
[16] S. M. Diesburg and A.-I. A. Wang, ``A survey of con_dential data storage and deletion methods," ACM Comput. Surv., vol. 43, no. 1, pp. 2:1_2:37, 2010, doi: 10.1145/1824795.1824797.
[17] G. F. Hughes, T. Coughlin, and D. M. Commins, ``Disposal of disk and tape data by secure sanitization," IEEE Secur. Privacy Mag., vol. 7, no. 4, pp. 29_34, Jul. 2009, doi: 10.1109/MSP.2009.89.
[18] J. Lee, S. Yi, J. Heo, H. Park, S. Y. Shin, and Y. Cho, ``An ef_cient secure deletion scheme for _ash _le systems," J. Inf. Sci. Eng., vol. 26, no. 1, pp. 27_38, 2010.
[19] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui, ``A secure cloud backup system with assured deletion and version control," in Proc. 40th Int. Conf. Parallel Process. Workshops, Taipei City, Taiwan, 2011, pp. 160_167, doi: 10.1109/ICPPW.2011.17.
[20] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, ``FADE: Secure overlay cloud storage with _le assured deletion," in Proc. Int. Conf. Secure. Privacy Commun. Syst., Singapore, 2010, pp. 380_397, doi: 10.1007/978-3-642-16161-2_22.
[21] S. L. Gar_nkel and A. Shelat, ``Remembrance of data passed: A study of disk sanitization practices," IEEE Secur. Privacy, vol. 1, no. 1, pp. 17_27, Jan. 2003, doi: 10.1109/MSECP.2003.1176992.
[22] D. Perito and G. Tsudik, ``Secure code update for embedded devices via proofs of secure erasure," in Proc. 15th Eur. Symp. Res. Comput. Secur., Athens, Greece, 2010, pp. 643_662, doi: 10.1007/978-3-642 15497-3_39.
[23] Y. Luo, M. Xu, S. Fu, and D.Wang, ``Enabling assured deletion in the cloud storage by overwriting," in Proc. 4th ACM Int. Workshop Secur. Cloud Comput., Xi'an, China, 2016, pp. 17_23, doi: 10.1145/2898445.2898447.
[24] R. Kissel, A. Regenscheid, M. Scholl, and K. Stine, Guidelines for Media Sanitization, document SP 800-88, Revelation 1, US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2006.
[25] D. Boneh and R. J. Lipton, ``A revocable backup system," in Proc. 6th USENIX Secur. Symp., San Jose, CA, USA, 1996, pp. 91_96.
[26] Z. Mo, Y. Qiao, and S. Chen, ``Two-party _ne-grained assured deletion of outsourced data in cloud systems," in Proc. IEEE 34th Int. Conf. Distrib. Comput. Syst., Madrid, Spain, Jun. 2014, pp. 31_308, doi: 10.1109/ICDCS.2014.39.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

[27] B. Hall and M. Govindarasu, ``An assured deletion technique for cloud-based IoT," in Proc. 27th Int. Conf. Comput. Commun. Netw. (ICN), Hangzhou, China, Jul. 2018, pp. 1_9, doi: 10.1109/ICCCN.2018.8487372.
[28] C. Yang, X. Tao, F. Zhao, and Y. Wang, ``Secure data transfer and deletion from counting Bloom _lter in cloud computing," Chin. J. Electron., vol. 29, no. 2, pp. 273_280, Mar. 2020, doi: 10.1049/cje.2020.02.015.
[29] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, ``Secure overlay cloud storage with access control and assured deletion," IEEE Trans. Depend. Sec. Comput., vol. 9, no. 6, pp. 903_916, Nov. 2012, doi: 10.1109/ TDSC.2012.49.
[30] C. Yang, J. Wang, X. Tao, and X. Chen, ``Publicly veri_able data transfer and deletion scheme for cloud storage," in Proc. 20th Int. Conf. Inf. Commun. Secur., Lille, France, 2018, pp. 445_458, doi: 10.1007/978-3- 030-01950-1_26.
[31] F. Hao, D. Clarke, and A. F. Zorzo, ``Deleting secret data with public veri_ability," IEEE Trans. Dependable Secure Comput., vol. 13, no. 6, pp. 617_629, Nov. 2016, doi: 10.1109/TDSC.2015.2423684.
[32] L. Xue, Y. Yu, Y. Li, M. H. Au, X. Du, and B. Yang, ``Ef_cient attribute-based encryption with attribute revocation for assured data deletion," Inf. Sci., vol. 479, pp. 640_650, Apr. 2019, doi: 10.1016/j.ins.2018.02.015.
[33] C. Yang, X. Chen, and Y. Xiang, ``Blockchain-based publicly veri_able data deletion scheme for cloud storage," J. Netw. Comput. Appl., vol. 103, pp. 185_193, Feb. 2018, doi: 10.1016/j.jnca.2017.11.011.
[34] J. Xiong, X. Liu, Z. Yao, J. Ma, Q. Li, K. Geng, and P. S. Chen, ``A secure data self-destructing scheme in cloud computing," IEEE Trans. Cloud Comput., vol. 2, no. 4, pp. 448_458, Oct. 2014, doi: 10.1109/ TCC.2014.2372758.
[35] Y. Yu, L. Xue, Y. Li, X. Du, M. Guizani, and B. Yang, ``Assured data deletion with _ne-grained access control for fog-based industrial applications," IEEE Trans. Ind. Informat., vol. 14, no. 10, pp. 4538_4547, Oct. 2018, doi: 10.1109/TII.2018.2841047.
[36] C. Yang, Q. Chen, and Y. Liu, ``Fine-grained outsourced data deletion scheme in cloud computing," Int. J. Electron. Inf. Eng., vol. 11, no. 2, pp. 81_98, 2019, doi: 10.6636/IJEIE.201912_11(2).04.
[37] Y. Yu, J. Ni, W. Wu, and Y. Wang, ``Provable data possession supporting