Article Received:*10 January 2023* ***Revised:****14 February 2023* ***Accepted:*** *25 February 2023*

Cloud Storage Systems with Secure Attribute-Based Access Control

O.Pandithurai[1], R.Kennady[2]
[1]Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, Tamilnadu
[2]Department of Artificial Intelligence and Data Science, Rajalakshmi Institute of Technology, Chennai, Tamilnadu
[1]pandics@ritchennai.edu.in, [2]kennady.r@ritchennai.edu.in

Abstract: This research presents a novel approach to safe access procedure in cloud storage structure by addressing the challenges associated with managing and distributing complex secret keys. The proposed procedure utilizes attribute-based access control and incorporates a client process, an authentication terminal process, and a storage terminal process. The client generates a main secret key and public parameters for each user using an attribute password mechanism. The authentication terminal maintains user attribute, file attribute, and attribute secret key databases. Access control is determined by constructing an access control string from the attributes of the user, file, and file operation type, enabling fine-grained access control and accommodating large-scale user dynamic expansion. Consequently, the access control costs of the cloud storage structure are significantly reduced, while offering a flexible, effective, and secure access control mechanism for safe storage structure access.

Keywords: *Cloud storage, Attribute-based access control, Secure access, Storage technology, Information safety, Access control string, Fine-grained access control, Large-scale user dynamic expansion, Access control expenditure, Flexible access control mechanism, Secure storage structure access.*

Introduction

Cloud storage structure have revolutionized the way data is stored, accessed, and shared, providing convenient and scalable solutions for individuals and organizations. However, ensuring the security and integrity of data stored in the cloud remains a critical challenge. One fundamental aspect of secure cloud storage is the implementation of robust access control mechanisms, which govern the permissions and privileges granted to users for accessing stored data. Existing safe access procedure in cloud storage structure often rely on the management and dispensing of complex secret keys. However, this approach poses significant challenges in terms of key management, distribution, and overall structure security. As cloud storage structure continue to grow in complexity and scale, the need for a more efficient and effective access control mechanism becomes increasingly apparent.

This research aims to address the shortcomings of previous safe access procedure by proposing a novel approach based on attribute-based access control. Attribute-based access control (ABAC) is a flexible access control model that grants permissions based on attributes associated with users, files, and file operations. By incorporating ABAC into the access control mechanism, this research aims to provide fine-grained access control and accommodate the dynamic expansion of users in complex cloud storage structure. The proposed procedure consists of three main components: a client process, an authentication terminal process, and a storage terminal process. The client generates a main secret key and public parameters for each user using an attribute password mechanism, ensuring individualized access credentials. The authentication terminal maintains databases of user attributes, file attributes, and attribute secret keys, which are crucial for determining access rights. By constructing an access control string based on the attributes of the user, file, and file operation type, the proposed procedure enables precise control over data access. This approach allows for efficient and secure access management, even in large-scale cloud storage structure. Additionally, the proposed procedure aims to reduce the access control expenditure associated with traditional procedure, providing a cost-effective solution for secure storage structure access. The figure (**Fig.**1) illustrates the architecture for data security in cloud.[3]

Article Received:*10 January 2023* ***Revised:****14 February 2023* ***Accepted:*** *25 February 2023*

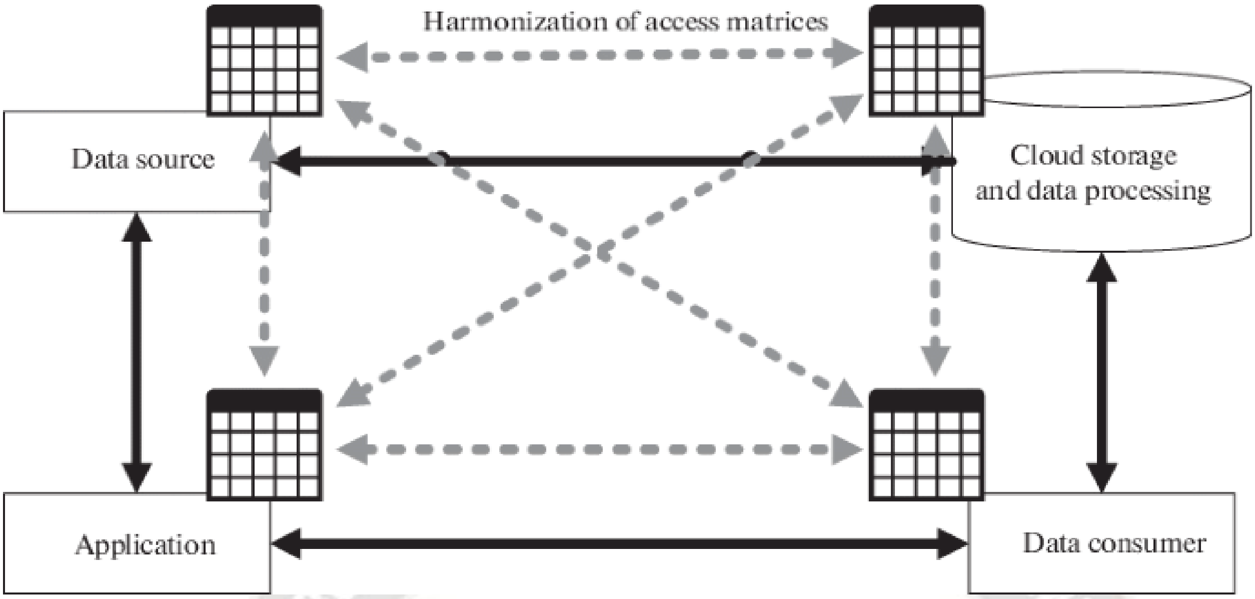
Harmonization of access matrices
Data source
Cloud storage and data processing
Application
Data consumer

Fig. 1: Ensuring Data Security in Cloud-Based Architecture

The research objectives of this study are to develop a safe access procedure for cloud storage structure that overcomes the challenges of managing complex secret keys, facilitates fine-grained access control, and accommodates the dynamic expansion of users. Moreover, this research endeavors to provide a flexible, effective, and secure access control mechanism, thereby enhancing the overall security and efficiency of cloud storage structure. In conclusion, this research introduces a new approach to safe access procedure in cloud storage structure, addressing the limitations of complex secret key management and distribution. By leveraging attribute-based access control and integrating client, authentication terminal, and storage terminal processes, this procedure aims to enhance access control efficiency, reduce costs, and provide a secure and flexible mechanism for safe storage structure access.

Related Work

Cloud storage structure have emerged as an integral part of the concept of cloud computing, offering users a convenient and scalable data access service. Unlike traditional storage devices, cloud storage structure are composed of multiple memory devices and servers, forming an aggregate entity.[1] However, despite the convenience provided by cloud storage structure, users have become increasingly concerned about trusting the service providers and ensuring the safety of their data.[2] The primary goal of ensuring the security of a cloud storage structure is to safeguard the confidentiality, integrity, and availability of stored data. Users need to have confidence in the safety of their private data within the cloud storage structure.[3] It is crucial to effectively protect user data and allow users to maintain control over their own data domains. Simultaneously, it is essential to improve the overall structure's security level while minimizing performance and cost implications, thus driving the design of secure architectures for cloud storage structure.

Access control plays a pivotal role in a cloud storage structure by providing users with controlled and authorized access to structure resources. The objective is to allow users maximum access rights based on resource sharing while preventing unauthorized operations and the unauthorized access of sensitive information.[4] When a user requests access to a data object, the structure queries the Access Control List (ACL) associated with that object. If the user's access control entry is found and grants the requested operation, the operation is permitted.[5] Otherwise, the request is denied. Existing safety access procedure in cloud storage structure typically rely on unique user identification, where user attributes participate in access control decisions as constraint rules. However, as cloud storage structure expand in scale and encounter increasing access strategy complexity, the number of constraint rules for user access to files escalates.[6] This leads to challenges in key management and distribution, resulting in inefficient access control structure. Consequently, PB-level large-scale storage structure face noticeable performance bottlenecks. In summary, the security architecture of cloud storage structure needs to address concerns related to user trust, data confidentiality, integrity, availability, and efficient

Article Received:*10 January 2023* ***Revised:****14 February 2023* ***Accepted:*** *25 February 2023*

access control. There is a demand for access control procedure that can handle the increasing complexity and scale of cloud storage structure, while minimizing the performance costs associated with key management and distribution.

Research Objective

The objective of this research is to develop a secure access procedure for cloud storage structure that overcomes the challenges associated with complex secret key management and distribution in existing safe access procedure. The research aims to employ attribute-based access control to enable fine-grained access control and accommodate the large-scale dynamic expansion of users in complex cloud storage structure. The research also seeks to reduce the access control costs of the cloud storage structure while providing a flexible, effective, and safe access control mechanism for secure storage structure access.

Access Control for Secure Cloud Storage Structure

This research focuses on developing a secure access procedure for cloud storage structure. The proposed procedure consists of three main processes: the client process, the certification end process, and the storage end process. Each process plays a crucial role in ensuring the safety of accessing the cloud storage structure. In the client process, a unique master key and open parameters are generated for each user. This is accomplished using a properties secret mechanism that takes into account specific attributes of the user. The master key and open parameters serve as individualized access credentials for the user.

The certification end process involves loading the user property storehouse, file attribute storehouse, and attribute cipher key store. The user property storehouse contains records of all user profiles, including their respective user IDs. The file attribute storehouse stores comprehensive information about each file, including the filename, file owner, and various attribute details. These attribute details comprise the file's former substrings, all attribute information associated with the file, and all cipher key numbers linked to the file. The attribute cipher key store preserves the cipher key numbers and their corresponding attribute keys for each file. The storage end process focuses on the correlation between former substrings, attribute keys, and cipher key numbers. Each former substring, attribute key, and cipher key number are associated with one another in a one-to-one correspondence. This correlation allows for efficient retrieval and identification of attribute keys based on the cipher key numbers. By implementing this safety access procedure, the proposed approach enhances the security of accessing the cloud storage structure. The generation of unique master keys and open parameters for each user ensures individualized access credentials. The comprehensive storage of user profiles and file attribute information in their respective storehouses enables efficient access control and management. The preservation of attribute cipher keys and their corresponding cipher key numbers facilitates secure retrieval and validation of attribute keys. The figure below (**Fig**.2) represents the doubling of data on cloud storage.

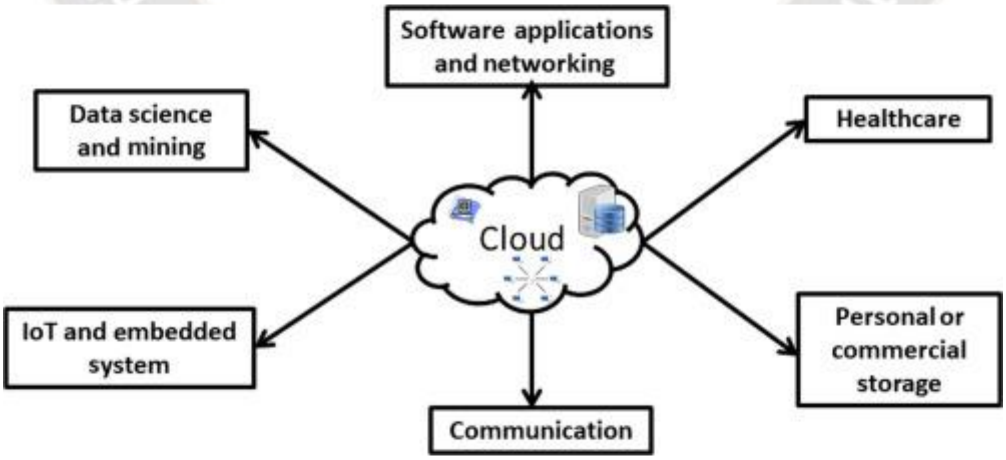

Fig. 2: Cloud Storage Data Deduplication

In summary, the research introduces a detailed safety access procedure for cloud storage structure, comprising client, certification end, and storage end processes. By generating unique master keys and open parameters, recording user profiles and file attribute information, and correlating former substrings, attribute keys, and cipher key numbers, the proposed procedure ensures secure and efficient access to the cloud storage structure.

Conclusion

In this research, we have presented a novel safety access procedure for cloud storage structure, addressing the challenges associated with complex secret key management and distribution in prior art procedure. By incorporating attribute-based access control (ABAC) and leveraging client, certification end, and storage end processes, we have developed a secure and efficient mechanism for accessing cloud storage structure. The proposed procedure offers several key advantages. Firstly, by generating unique master keys and open parameters for each user based on a properties secret mechanism, individualized access credentials are established. This enhances the security of the structure by ensuring that each user has their own distinct set of keys, reducing the risk of unauthorized access or data breaches. Secondly, the use of attribute-based access control allows for fine-grained access control, enabling precise management of user permissions based on attributes associated with users, files, and file operations. This granular level of control ensures that users only have access to the files and operations that are explicitly permitted based on their attributes. This greatly enhances the overall security of the cloud storage structure by preventing unauthorized access and potential data leakage. Moreover, the incorporation of the client, certification end, and storage end processes provides a comprehensive framework for implementing the safety access procedure. The client process generates the necessary keys and parameters, while the certification end process maintains the user property storehouse, file attribute storehouse, and attribute cipher key store. These components form the foundation for efficient access control decision-making and access rights management. The storage end process plays a critical role in correlating former substrings, attribute keys, and cipher key numbers, facilitating seamless retrieval and identification of attribute keys. This ensures that the access control mechanism operates with high efficiency and accuracy, even in large-scale cloud storage structure. Additionally, the use of these correlated components streamlines the key management and distribution process, reducing overhead and complexity.

By addressing the limitations of previous access control procedure, the proposed approach provides a flexible, effective, and secure access control mechanism for cloud storage structure. It enables users to have trust in the safety of their private data within the structure, effectively protects user data, and allows users to maintain control over their own data domains. Simultaneously, it aims to minimize performance costs associated with key management and distribution, making it a cost-effective solution for secure storage structure access. In conclusion, this research presents a significant contribution to the field of storage technology and information safety in computer structure. By introducing a safety access procedure based on attribute-based access control, complex secret key management and distribution challenges are overcome. The proposed procedure offers enhanced security, fine-grained access control, and efficient access management in cloud storage structure. Future work can focus on further optimizing the access control mechanism and conducting extensive evaluations and experiments to validate the effectiveness and performance of the proposed procedure in real-world scenarios. Overall, this research provides valuable insights and practical solutions for ensuring the secure access of cloud storage structure.

References

1. Oberko, P. S. K., Obeng, V. H. K. S., & Xiong, H. (2022). A survey on multi-authority and decentralized attribute-based encryption. *Journal of Ambient Intelligence and Humanized Computing*, 1-19.
2. Blockchain-based cloud storage system with CP-ABE-based access control and revocation process, P Sharma, R Jindal, MD Borah - The Journal of Supercomputing, 2022 - Springer
3. An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare, H Zhong, Y Zhou, Q Zhang, Y Xu, J Cui - Future Generation Computer, 2021 - Elsevier
4. Data security and privacy protection for cloud storage: A survey, P Yang, N Xiong, J Ren - IEEE Access, 2020 - ieeexplore.ieee.org
5. Secure data storage and recovery in industrial blockchain network environments, W Liang, Y Fan, KC Li, D Zhang- IEEE Transactions on, 2020 - ieeexplore.ieee.org
6. Efficient multi-authority access control using attribute-based encryption in cloud storage, PS Challagidad, MN Birje - Procedia Computer Science, 2020 – Elsevier
7. Attribute-based access control of data sharing based on hyperledger blockchain, A Alniamy, BD Taylor - Proceedings of the 2020 The 2nd International, 2020 - dl.acm.org

***Article Received:**10 January 2023 **Revised:**14 February 2023 **Accepted:** 25 February 2023*

8. Blockchain for secure ehrs sharing of mobile cloud based e-health structure, DC Nguyen, PN Pathirana, M Ding- IEEE access, 2019 - ieeexplore.ieee.org
9. Block-secure: Blockchain based scheme for secure P2P cloud storage, J Li, J Wu, L Chen - Information Sciences, 2018 – Elsevier
10. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage structure, S Wang, Y Zhang, Y Zhang - Ieee Access, 2018 - ieeexplore.ieee.org
11. Security and privacy in smart health: Efficient policy-hiding attribute-based access control, Y Zhang, D Zheng, RH Deng - IEEE Internet of Things Journal, 2018 - ieeexplore.ieee.org