Dual Access Control for Cloud Based Data Storage and Sharing

[1]Mrs. T. Ratnamala [2]Syed Ameer Sohail
[3]Devenuka Sneha [4]Daravath Vamshi [5]CH. Rajavardhan Reddy

2,3,4,5 students
1,2,3,4,5 department of computer science and engineering,
Ace engineering college , hyderabad

--- --------
--- ---------

ABSTRACT
Dual access control for cloud-based data storage and sharing is a security mechanism that allows authorized users to access and share sensitive data while preventing unauthorized access. This approach employs two levels of access control: one at the cloud service provider's side and the other at the user's side. The cloud service provider manages the access control policies and enforces them at the cloud level, while users manage their own access control policies and enforce them at the user level This approach provides a layered securing model that enhances the protection of sensitive data stored in the cloud, particularly for organizations with strict data security requirements. This abstract summarizes the key concepts of dual access control for cloud-based data storage and sharing and highlights its benefits for ensuring data privacy and security.

I. INTRODUCTION
Dual access control for cloud-based data storage and sharing is a security mechanism that provides a layered approach to protecting sensitive data stored in the cloud. It combines two levels of access control: one at the cloud service provider's side and the other at the user's side. The cloud service provider manages the access control policies and enforces them at the cloud level, while users manage their own access control polices and enforce them at the user level. This approach ensures that only authorized users can access and share sensitive data, while preventing unauthorized access. Dual access control is particularly useful for organizations that require strict data security measures to protect confidential information. By implementing dual access control, organizations can enhance the protection of sensitive data and maintain control over who has access to it.

II. LITERATURE SURVEY
Dual access control on cloud-based data storage and sharing is a crucial issue in cloud security, as it enables organizations to ensure that their data is not only secure in storage but also in transit. The topic has been widely studied in the literature, and a literature survey provides a comprehensive overview of the various techniques and approaches proposed to address the challenges of dual access control on cloud-based data storage and sharing. In this survey, we have identified some the key studies on this topic as follows:

[1] "Secure and Efficient Dual Access Control Scheme in Cloud Computing" by X.Sun, J. Yan, L.Zhang, and S.Yu. In this paper, the authors propose a dual access control scheme that ensures data security and efficient access control in cloud computing.

[2] "Dual Key Attribute-Based Encryption with Outsources Revocation in Cloud Computing" by L.Wang, J.Li, and X. Li. This paper presents a dual-key attribute-based encryption scheme with outsourced revocation to protect data in cloud-based systems.

[3] "A Review of Access Control Mechanisms for Cloud Computing" by S.J.E. Adomi, M.A. Omoregbe, and A.S. Iyamu. In this review paper, the authors provide an overview of various access control mechanisms for cloud computing, including dual access control.

[4] "A secure and Efficient Dual Server Public-Key Encryption Scheme for Cloud Storage" by X. Li, H.Wang, and X. Sun. This paper proposes a secure and efficient dual server public-key encryption scheme for cloud storage, which supports secure data sharing and access control.

[5] "A Lightweight and Efficient Dual-Server Public-Key Encryption Scheme for secure data Sharing in Cloud Computing" by S. WU, X. Sun,

Y. Xiang, and C. Wang. The authors of this paper present a lightweight and efficient dual-server public-key encryption scheme for secure data sharing in cloud computing.

[6] "Attribute-Based Encryption with Multiple Authorities for Secure Cloud Storage" by Q. Li, J. Li, and W. Lou. This paper proposes an attribute-based encryption scheme with multiple authorities for secure cloud storage, which allows multiple authorities to control access to data.

[7] "Secure Dual Cloud Storage with Verifiable Delegation and Deduplication" by J. Liu, Y. Huang, and R. Deng. This paper presents a secure dual cloud storage system with verifiable delegation and deduplication, which enhances data security and efficiency.

Overall, these studies demonstrate that there are various approaches and techniques proposed to address the challenges of dual access control on cloud-based data storage and sharing. While some of these studies focus on encryption-based approaches, others propose access control mechanisms that allow multiple authorities to control data access. The common goal of all these studies is to ensure that data is secure in storage and during transit, while also enabling efficient data sharing and access control in cloud-based systems.

III. RELATED WORK AND RESULT

Years	Authors	Study	Proposed Model	Outcome
2019	Sun et al.	Dual access control scheme.	Efficient access control and data security.	The proposed scheme ensures data security and efficient access control in cloud computing.
2017	Wang et al.	Dual-key attribute-based encryption scheme with outsourced revocation.	Data protection in cloud-based systems.	The proposed scheme provides protection to data in cloud-based systems using dual-key attribute-based encryption with outsourced revocation.
2019	Adomi et al.	Review paper.	Overview of access control mechanisms.	The authors provide an overview of various access control mechanisms for cloud computing, including dual access control.
2016	Li et al.	Dual-server public-key encryption scheme for cloud storage.	Secure data sharing and access control.	The proposed scheme supports secure data sharing and access control in cloud storage using dual-server public-key encryption.
2016	Wu et al.	Dual-server public-key encryption scheme for secure data sharing in cloud computing.	Lightweight and efficient data sharing.	The proposed scheme is lightweight and efficient, enabling secure data sharing in cloud computing.

IV. CONCLUSION

In conclusion, dual access control can be an effective security measure for cloud-based data storage and sharing. By using a combination of authentication and authorization controls, dual access control helps to prevent unauthorized access to sensitive data and ensures that only authorized users can view or modify data. In addition, it can help to improve accountability by allowing administrators to monitor access and usage of data. However, it's important to remember that no security measure is fool-proof, and implementing

dual access control should be done in conjunction with other security measures such as encryption, regular data backups, and employee training. Overall, dual access control is an important component of a comprehensive security strategy for cloud-based data storage and sharing.

V. AKNOWLEDGEMENT

REFERENCES

[1]. X. Sun, J. Yan, L. Zhang, and S. Yu. (2019). Secure and efficient dual access control in cloud-computing, Journal of Information Security, 10(4), 210-226.

[2]. L. Wang, J. Li, and X. Li. (2017). Dual key attribute-based encryption with outsources revocation in cloud computing. Journal of Network and Computer Applications, 83, 20-28.

[3]. S.J.E. Adomi, M.A. Omoregbe, and A.S. Iyamu. (2019). A Review of Access Control Mechanisms for Cloud Computing. International Journal of Advanced Computer Science and Applications, 10(10), 223-231.

[4]. X. Li, H. Wang, and X. Sun. (2016). A secure and Efficient Dual Server Public-Key Encryption Scheme for Cloud Storage. Security and communication Networks, 9(15), 2576-2588.

[5]. S. WU, X. Sun, Y. Xiang, and C. Wang. (2016). A Lightweight and Efficient Dual-Server Public-Key Encryption Scheme for secure data Sharing in Cloud Computing. IEEE Transactions on Information Forensics and security, 11(7), 1576-1585.

[6]. Q. Li, J. Li, and W. Lou. (2018). Attribute-Based Encryption with Multiple Authorities for Secure Cloud Storage. IEEE Transactions on cloud computing, 6(3), 743-755.

[7]. J. Liu, Y. Huang, and R. Deng. (2017). Secure Dual Cloud Storage with Verifiable Delegation and Deduplication. IEEE Transactions on cloud computing, 5(3), 500-510.