Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, October : 2024

Dual Access Control for Cloud Based Data Storage and Sharing

[1]D.Akhila
M.Tech Student
Dept. of Computer Science Engineering
Vaagdevi College of Engineering
Email: davulapallyakhila@gmail.com

[3]Dr.N.Satyavathi
Associate professor
Head, Dept. of Computer Science Engineering
Vaagdevi College of Engineering
Email: satyanadendla15@gmail.com

[2]Dr.M.Sukesh
Assistant professor
Dept. of Computer Science Engineering
Vaagdevi College of Engineering
Email: manyam_s@vaagdevi.edu.in

[4]Dr.E.Balakrishna
Associate professor
Dept.of Computer Science Engineering
Vagdevi College of Engineering
Email: balakrishnakits@gmail.com

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.

Index Terms: medical record; text classification; capsule network

I.INTRODUCTION

Dual access control for cloud-based data storage and sharing represents a sophisticated security paradigm meticulously crafted to fortify the protection of sensitive information residing within cloud environments. This innovative approach operates on a stratified foundation, integrating two distinct tiers of access control. At the forefront, the cloud service provider assumes responsibility for formulating and implementing access control policies, deploying robust measures to safeguard data integrity. Concurrently, users are empowered to manage their own access control parameters, exerting granular control over data access and sharing activities at their discretion.

By adopting a dual-layered strategy, this security mechanism offers a comprehensive shield against unauthorized access attempts, effectively thwarting potential breaches and data leaks. Its multifaceted nature ensures that only duly authorized users, possessing requisite permissions and credentials, can interact with sensitive data assets. This heightened level of control is particularly invaluable for organizations operating within industries where data confidentiality is paramount, such as healthcare, finance, and government sectors.

Moreover, the implementation of dual access control fosters a collaborative security ecosystem, wherein cloud service providers and users collaborate synergistically to fortify data protection measures. This collaborative effort not only enhances the resilience of security frameworks but also instills confidence among stakeholders regarding the integrity and confidentiality of their data assets.

Furthermore, dual access control serves as a proactive measure for organizations seeking to navigate the intricate landscape of regulatory compliance. By adhering to stringent access control protocols, organizations can demonstrate compliance with data protection regulations and standards, thereby mitigating the risk of regulatory penalties and legal ramifications.

In essence, the adoption of dual access control for cloud-based data storage and sharing heralds a paradigm shift in cybersecurity practices, offering organizations a robust framework to fortify their defenses, uphold data integrity, and mitigate the ever-evolving threats posed by

cyber adversaries. Through its multifaceted approach and collaborative ethos, dual access control emerges as a cornerstone of modern data security strategies, empowering organizations to navigate the digital landscape with confidence and resilience.

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 PublicKey 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 encryptionbased 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. EXISTING SYSTEM

In the existing system of cloud-based data storage and sharing, access control is primarily managed by the cloud service provider. Users are granted permissions to access and share data stored in the cloud based on predefined policies set by the provider. This setup typically involves a single-layer access control mechanism where the cloud service provider is solely responsible for enforcing access policies. While this approach provides a basic level of security, it may lack the granularity and user-centric control needed to adequately protect sensitive data. Users have limited control over access permissions and are reliant on the cloud service provider to manage and enforce security measures.

DISADVANTAGES OF EXISTING SYSTEM:

1. Limited User Control: In the existing system, users have limited control over access permissions and security measures. They rely heavily on the cloud service provider to manage access policies, which may not align with their specific security requirements.
2. Lack of Granularity: The single-layer access control mechanism employed by the cloud service provider may lack the granularity needed to enforce fine-grained access policies. This could lead to potential security vulnerabilities and unauthorized access to sensitive data.

IV PROPOSED SYSTEM:

The proposed system introduces a dual access control mechanism for cloud-based data storage and sharing, aiming to enhance security and provide users with greater control over their data. In addition to the access control policies managed by the cloud service provider, users are empowered to define and enforce their own access control policies at their end. This dual-layered approach augments the existing cloud-level access controls, allowing users to customize permissions and restrict access to sensitive data according to their specific requirements. By integrating user-managed access control with the existing cloud-level controls, the proposed system offers a more comprehensive and customizable framework for data protection. This empowers users to exercise greater control over who can access their data and how it is shared, ultimately enhancing security and privacy in cloud-based environments.

ADVANTAGES OF PROPOSED SYSTEM:

Enhanced User Control: The proposed dual access control system empowers users with greater control over their data by allowing them to define and enforce their own access policies. This enables users to tailor security measures to their specific needs and preferences.

Customizable Permissions: With the ability to define granular access permissions, users can implement fine-grained access controls based on factors such as user roles, data sensitivity, and organizational policies.Improved Security: By combining cloud-level access controls with user-managed policies, the proposed system offers a layered approach to security that reduces the risk of unauthorized access and data breaches.

V.SYSTEM DESIGN

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, October : 2024

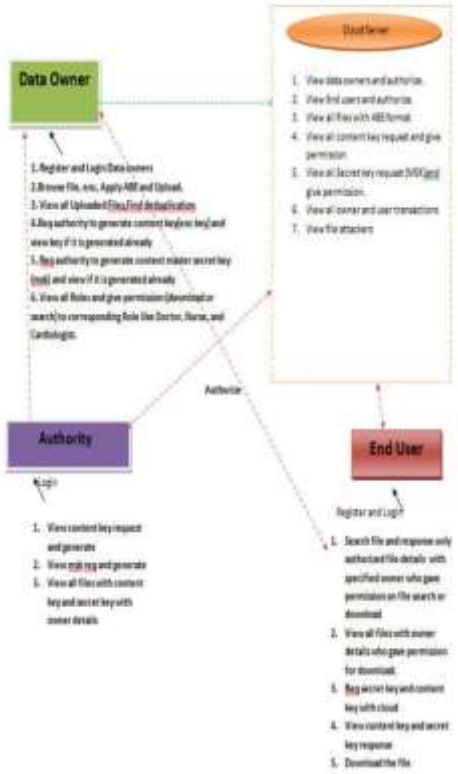


Fig1: Architecture of system.

DATA OWNER: In this module, initially the data owner has to register to the cloud server and get authorized. After the authorization from cloud data owner will encrypt and add file to the cloud server where in after the addition of file data owner requests the content key and the master secret key to the authority for the file he uploaded and finds Find deduplication ,only after the keys generated the file is uploaded to the cloud server. After the uploading of the file the data owner will have to provide download and the search permission for individual file for the users to perform search and download.

CLOUD SERVER

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with cloud End users. To access the shared data files users will request the permission of content key and the MSK master secret key. And the cloud will provide the permission .and also views all the transactions and attackers related to the files.

AUTHORITY

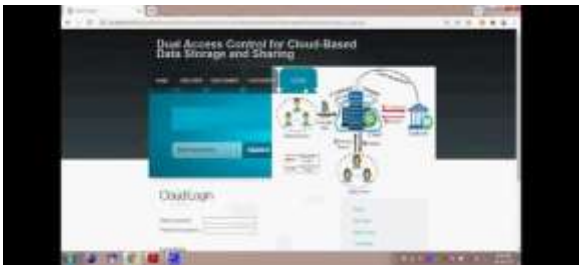
Authority generates the content key and the secret key requested by the end user. Authority can view all files with the content key and master secret key generated with the corresponding data owner details of the particular file.

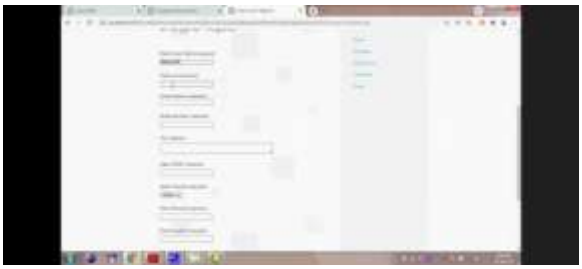
END USER

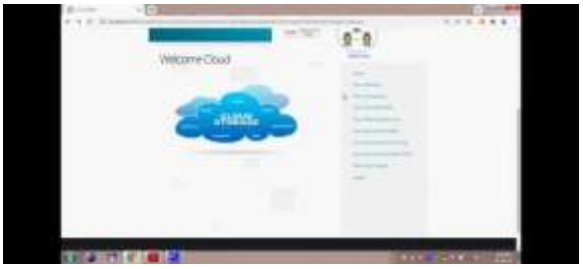
User has to register and login for accessing the files in the cloud. User is authorized by the cloud to verify the registration. User has to request for the MSK master secret key and content key to download the file. User can only download and serach the file if the data owner of the particular file has provided the permissions.

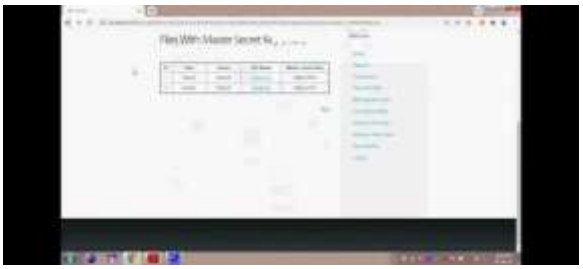
Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 10, October : 2024

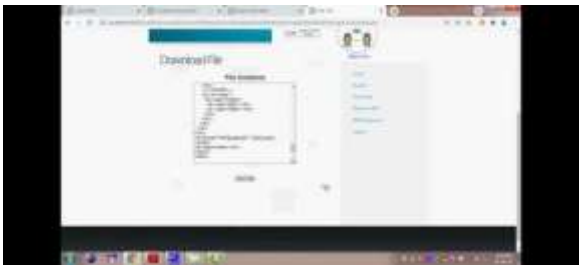
VI. RESULT:

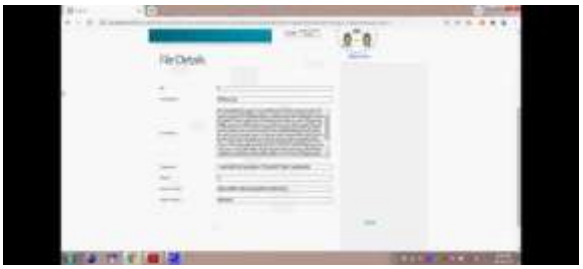


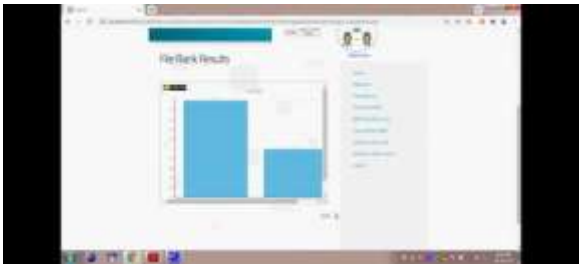












VII. CONCLUSION

We presented two dual access control systems to address an intriguing and longstanding issue related to cloud-based data sharing. DDoS/EDoS attacks are not a problem for the proposed systems. We claim that the technique used to achieve the feature of download request control is "transplantable" to other CP-ABE constructions. Our experimental results

show that the proposed systems have no significant computational or communication overhead (when compared to the underlying CP-ABE building block).

VIII. FUTURE ENHANCEMENT

The proposed dual access control system for cloud-based data storage and sharing has potential for future development. It can enhance data security and privacy by integrating advanced encryption techniques, machine learning for access control, blockchain integration, cross-platform compatibility, user-friendly interfaces, compliance framework integration, scalability and performance optimization, and continuous security auditing and monitoring.

IX. REFERENCES

[1] Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin. Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2):111–128, 2013.

[2] Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

[3] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.

[4] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[5] JohnBethencourt,AmitSahai,andBrentWate rs. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.

[6] Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.

[7] Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017.

[8] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in CryptologyCRYPTO 1999, pages 537–554. Springer, 1999.

[9] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.

[10] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au. Improving privacy and security in decentralized ciphertext-policy attributebased encryption. IEEE transactions on information forensics and security, 10(3):665–678, 2015.