WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Dual Access Control for Cloud-Based Data Storage and Sharing

LOKESHWARAN.V[1], DR.VAIDEHI.V [2]

[1].PG Student, Email: vasudevanlokeshwaran@gmail.com
[2].Professor ,Email: vaidehi.mca@drmgrdu.ac.in
Department of Computer Applications DR.MGR.Educational&ResearchInstitute,Chennai-95

ABSTRACT:

Distributed computing is a high-level breakthrough in the making. Information storage is a huge headache for everyone in this world. Distributed computing is an excellent solution for storing and retrieving data in the most straightforward and quickest way possible. Security is the most pressing concern in distributed computing. I'm attempting to show another approach for giving distributed computing had admission control in this paper.

In distributed computing, this architecture provides secured admittance control. It adopts a progressive construction and use a clock to provide more granular access control. We can easily transmit, download, and delete documents from and to the cloud using this method. Access Control, Cloud Computing, and Cloud Privacy are some of the terms on the list.

Keywords:. Distributed Computing, Dual Access Control, Cloud Computing, Cloud Privacy, Cloud Security, Advanced Encryption Standard

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.[1]

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.[2]
This approach ensures that only authorized users can access and share sensitive data, while preventing unauthorized access.[3]

Dual access control is particularly useful for organizations that require strict data security measures to protect confidential information.[4]

By implementing dual access control, organizations can enhance the protection of sensitive data and maintain control over who has access to it.[5]

LITERATURE SURVEY:

According to **M. Steiner and Z.-L. Zhang** et al. (2015), Netflix accounts for 29.7% of the peak downstream traffic in the US, making it the top supplier of on-demand Internet video streaming in both the US and Canada. Comprehending the architecture and performance of Netflix can provide valuable insights on optimizing its design, as well as the design of other on-demand streaming services. In this paper, we analyze Netflix's architecture and service strategy using a measuring analysis.[6]

B. Wong and E. G. Sirer al.,2007 proves that ClosestNode.com is an accurate, scalable, and backwards-compatible service for mapping clients to a nearby server. It provides a DNS interface by which unmodied clients can look up a service name, and get the IP address of the closest server. A shared system for performing such a mapping amortizes the administration and implementation costs of proximity-based server selection. It is aimed at minimizing the amount of effort required for system developers to make new and existing infrastructure services proximity-aware.[7]

H. Ballani, P. Costa, T. Karagiannis.,et al.,2011says that The shared nature of the network in today's multi-tenant datacenters implies that network performance for tenants can vary significantly. This applies to both production datacenters and cloud environments. Network performance variability hurts application performance which makes tenant costs unpredictable and causes provider revenue loss. Motivated by these factors, this paper makes the case for extending the tenant-provider interface to explicitly account for the network.[8]

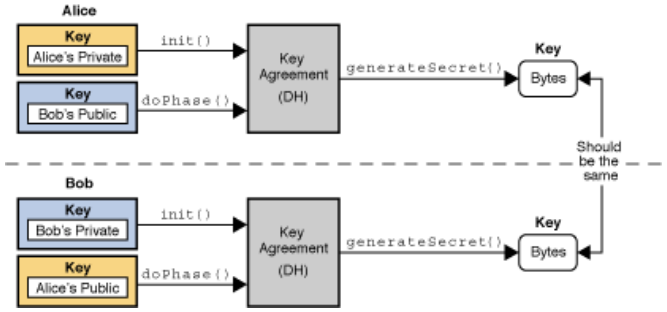
N. Laoutaris, M. Sirivianos,.et al.,2022 say that Large datacenter operators with sites at multiple locations dimension their key resources according to the peak demand of the geographic area that each site covers. The demand of specific areas follows strong diurnal patterns with high peak to valley ratios that result in poor average utilization across a day.[9]

A. Greenberg, J. Hamilton, .et al.,2009 suggested that The data centers used to create cloud services represent a signifi- cant investment in capital outlay and ongoing costs. Accordingly, we first examine the costs of cloud service data centers today. The cost breakdown reveals the importance of optimizing work completed per dollar invested. Unfortunately, the resources inside the data centers often operate at low utilization due to resource stranding and fragmentation. [10]

PROPOSED SYSTEM:

The most popular technique for preventing the compromise of sensitive data is encryption. But data encryption alone (using AES, for example) is insufficient to meet the real-world requirement for data management.
In addition, a strong download request access control mechanism must be taken into account to prevent Economic Denial of Sustainability attacks that aim to prevent users from using the service. In this application, we take dual access control into consideration within the framework of cloud-based storage, making sure to maintain efficiency and security while designing a control mechanism for both data access and download requests.

ARCHITECTURE DIAGRAM:



Architecture diagram

METHODOLOGYFOR IMPLEMENTATON:

1. **Specify Needs:** Determine and record the particular needs for dual access control. Take into account user roles, data sensitivity, regulatory compliance, and collaborative requirements.
2. **Risk Assessment:** To find potential security threats and weaknesses, carry out a thorough risk assessment. This will direct the access control implementation according to the risks that have been recognized.
3. **Data Classification:** Arrange information according to its significance and level of privacy. There are several categories into which data can be classified, including public, internal, and confidential. We can choose the proper degree of access restriction with the aid of this classification.
4. **Role-Based Access Control (RBAC):** Establish and put into practice user role-based access control. Assign roles according to the least privilege principle and job responsibilities. As organizational needs change, assess and adjust responsibilities on a regular basis.
5. **Attribute-Based Access Control (ABAC):** To improve fine-grained control, integrate attribute-based access control. This enables access decisions to be made in accordance with different user qualities, contextual factors, and data classifications.
6. **Encryption:** To safeguard sensitive data, use encryption for both in-transit and at-rest data. Employ robust encryption techniques to protect data while it's being transmitted and stored.
7. **Key Management:** To handle encryption keys, set up a strong key management system. Make sure that keys are distributed, rotated, and protected appropriately to stop unwanted access.
8. **Audit recording:** To monitor user actions, unauthorized access attempts, and system modifications, enable thorough audit recording. Examine and evaluate logs on a regular basis to spot possible security incidents.
9. **Policy Enforcement:** To guarantee that access control policies are continuously followed, put policy enforcement procedures in place. This could involve both routine hand reviews and automated tool

RESULTS & DISCUSSION:

The implementation of dual access control for cloud-based data storage and sharing presents several noteworthy results and implications, which are discussed in this section.The adoption of dual access control mechanisms effectively enhances the security posture of cloud-based data storage and sharing systems.

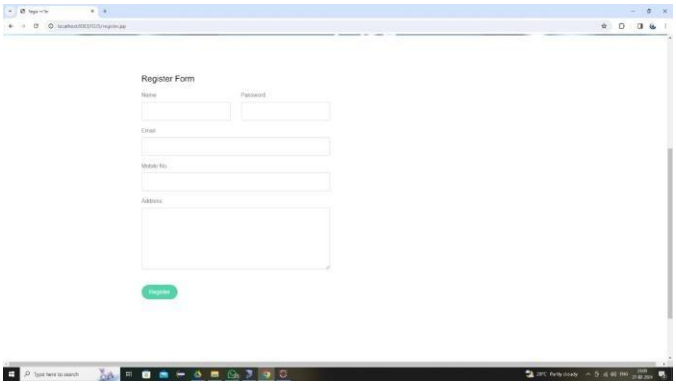


FIGURE 1: User Register Page

FIGURE 1.User Register Page:

A "User Register Page" is a specific type of web page or interface within a web application that is dedicated to allowing new users to sign up or create accounts for the platform.

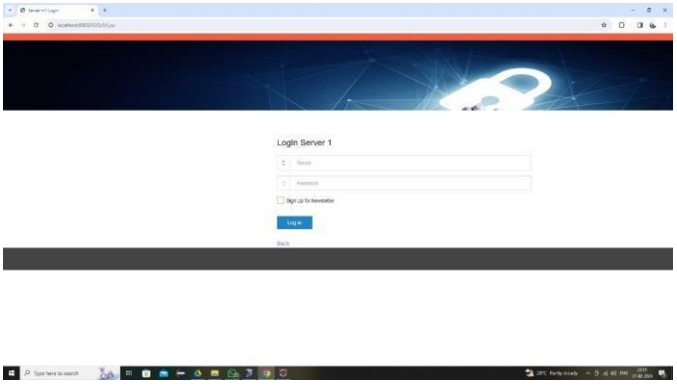


FIGURE 2: Server 1Login Page

FIGURE 2.Server 1Login Page:

Server 1 Login Page is a graphical representation or visual depiction of the web page or interface where users authenticate themselves to access a specific server or service.

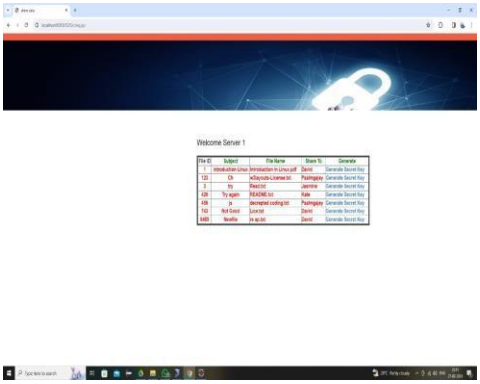


FIGURE 3:View User Register

FIGURE 3.View User Register:

View User Register is a visual representation or diagram illustrating the user registration process within a web application or system. It typically depicts the user interface elements and steps involved in registering a new user account.

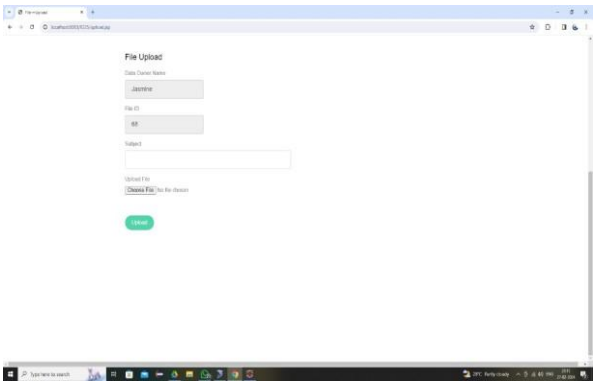


FIGURE 4:Upload File Page

FIGURE 4.Upload File Page:

Upload File Page is a visual representation or graphical depiction of the web page or interface where users can upload files to a web application or system.

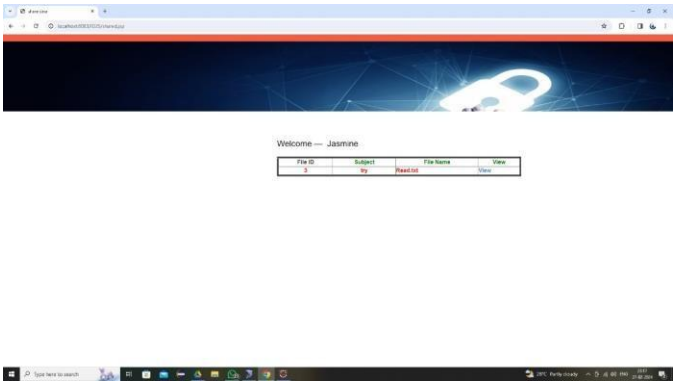


FIGURE 5:Shared file

FIGURE 5.Shared file:

Shared File depicts a visual representation or graphical depiction of a file that has been shared within a web application or system. This figure typically illustrates how shared files are presented or accessed within the application's interface, indicating that the file is accessible to multiple users or a specific group of users with appropriate permissions.

REFERENCE:

1. Y.G.Min and Y.H. Bang, "Security Concerns in Cloud Computing and Access Control Solutions," Journal of Security Engineering, vol. 2, 2012.
2. IEEE Transactions on Forensics and Security, vol. 7, no. 2, APR 2012, Z. Wang, J. Liu, and R.
3. H. Deng, "HASBE:A Hierarchical Attribute- Based Solution for Flexible and Scalable Access Control in Cloud Computing".
4. "The NIST Definition of Cloud Computing,"
5. P. Mell. Department of Commerce, United States: Special Publication 800-145.
6. M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, "Attribute-Based Encryption Enables Efficient and Safe Exchange of Personal Health Records
7. in Cloud Computing," IEEE Technology Transactions on Parallel and Distributed Systems, vol. 24, no. 1, Jan. 2013.
8. "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, NOV/DEC 2012, Y. Tang, P.P.C. Lee, J.C.S. Lui, and R. Perlman.
9. M. Steiner, Z.-L. Zhang, and associates, 2015, "Towards Temporal Access Control in Cloud Computing," by Hu, D. Huang, and S. Wang, Arizona State University, U.S.A.
10. [7 B. Wong and E. G. Sirer et al., 2007; ARPN Journal of Engineering and Applied Sciences, vol. 7, no. 5, May 2012, "Access Control in Cloud Computing Environment."
11. "Cloud Computing Bible," ed. H. Ballani, P. Costa, T. Karagiannis, et al., United States of America: Wiley, 2011.
12. M. Sirivianos, N. Laoutaris, et al., 2022 "Privacy-Preserved Access Control for Cloud Computing," IEEE International Joint Conference, 2011, Y. Mu, W. Susilo, and M. H. Au.
13. J. Hamilton, A. Greenberg, et al. (2009), Illinois Institute of Technology Journal, "Achieving Secure, Scalable, and Finegrained Data Access Control in Cloud Computing," C. Wang, K. Ren, and W. Lou.