**International Journal of Innovative Research in Engineering**
*Volume 5, Issue 5 (September-October 2024), PP: 01-04.*
*www.theijire.com* ***ISSN No: 2582-8746***

# Dual Security Control for Cloud-Based Data Storage and Sharing

**Ch.V.V.N. Rama Laxmi[1], Anjum Fathima[2], P. Harini[3], D. Snehith[4], Dr. X.S. Asha Shiny[5]**
*[1,2,3,4] B. Tech 4 t h Year, Department of Information Technology, CMR Engineering College (UGC Autonomous), Hyderabad, Telangana, India.*
*[5] Professor, Department of Information Technology, CMR Engineering College (UGC Autonomous), Hyderabad, Telangana, India.*

**How to cite this paper:**
Ch.v.v.n. Rama Laxmi[1], Anjum Fathima[2], P. Harini[3], D. Snehith[4], Dr. X.S. Asha Shiny[5], "Dual Security Control for Cloud-Based Data Storage and Sharing", IJIRE-V5I05-01-04.



***Abstract***: *Cloud data storage service has drawn increasing interests from both academic and industry in the recent years due to its efficient and low cost management. In recent years, the rapid adoption of cloud-based data storage services has revolutionized data management practices across academia and industry due to its effectiveness and affordability. While encryption techniques like AES (Advanced Encryption Standard) are widely employed to prevent the compromise of sensitive data, they alone are insufficient to meet the complex requirements of real-world data management scenarios Since itprovides services in an open network, it is urgent for service providers to make use of secure data storage and sharing mechanism to ensure data confidentiality and service user privacy. To protect sensitive data from being compromised, the most widely used method is encryption. However, simply encrypting data (e.g., via AES) cannot fully address the practical need of data management. Besides, an effective accesscontrol over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, we consider the dual security control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. Two dual security control systems are designed in this paper, where each of them is for a distinct designed setting. The security and experimental analysis for the systems are also presented. By ensuring that only authenticated and authorized users can access and manipulate data, we mitigate the risk of unauthorized access and data breaches.This work addresses these challenges by proposing a comprehensive approach: Our solution recognizes that effective security in cloud environments requires not only encryption but also a strong access control mechanism to mitigate threats such as Economic Denial of Sustainability (EDoS) attacks, which aim to disrupt service availability by preventing legitimate users from accessing their data.*

***Key Word :*** *Searchable Encryption, Multi-Keyword Search, Multi-User Access, Search Pattern, Access Pattern.*

## I.INTRODUCTION

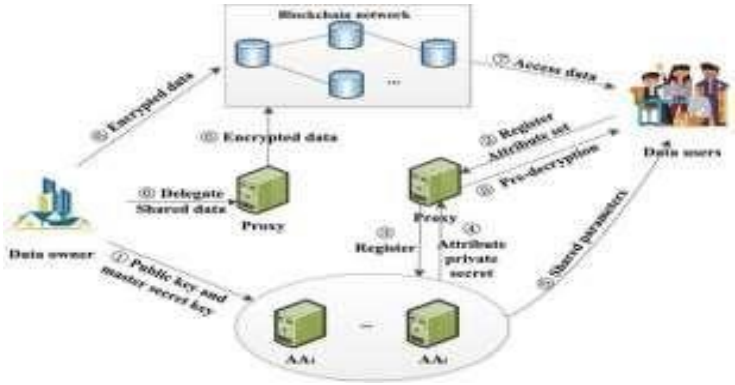
In the recent decades, cloud-based storage service has attracted considerable attention from both academia and industries. It may be widely used in many Internet-based commercial applications (e.g., Apple iCould) due to its long-list benefits including access flexibility and free of localdata management. Increasing number of individuals and companies nowadays prefer to outsource their data to remote cloud in such a way that they may reduce the cost of upgrading their local data management facilities/devices However, the worry of security breach over outsourced data may be one of the main obstacles hindering Internet users from widely using cloud-based storage service. In many practical applications, outsourced data may need to be further shared with others. For example, a Dropbox administration level (e.g., administrator could reach the link). Since the cloud (which is deployed in an open network) is not be fully trusted, it is generally recommended to encrypt the data prior to being uploaded to the cloud to ensure data security and privacy. One of the corresponding solutions is to directly employ an encryption technique(e.g., AES) on the outsourced data before uploading to cloud, so that only specified cloud user (with valid decryption key) can gain access to the data via valid decryption. To prevent shared photos being accessed by the "insiders" of the system, a straightforward way is to designate the group of authorized data users prior to encrypting the data. In some cases, nonetheless, Alice may have no idea about who the photo receivers/users are going to be. It is possible that Alice only has knowledge of attributes w.r.t. photo receivers. In this case, traditional public key encryption (e.g., Paillier Encryption), which requires encryptor to know who the data receiver is in advance, cannot be leveraged. Providing policy-based encryption mechanism over the outsourced photos is therefore desirable, so that Alice makes use of the mechanism to define access policy over the encrypted photosto guarantee only a group of authorized users is able to access the photos.In a cloud-based storage service, there exists a common attack that is well known as resource-exhaustion attack. Since a (public) cloud may not have any control over download request(namely, a service user may send

unlimited numbers of download request to cloud server), a malicious service user may launch the denial-of service (DoS)/distributed denial-of service (DDoS) attacks to consume the resource of cloud storage service server so that the cloud service could not be able to respond honest users' service requests, The best way is to secure the data in cloud-based storage and data sharing service, attribute- based encryption (ABE) [9] is one of the promising candidate that enables the confidentiality of out sourced data as well asfine- grained control over the outsourced data. In particular,Ciphertext-Policy ABE (CP-ABE) [5] provides an effective way of data encryption such that access policies, defining access privilege of potential data receivers, can be specified over encrypted data. Note that we consider use of CP-ABE in our mechanism in this paper. Nevertheless, employing CP-ABE technique is not sufficient to design an elegant mechanism guaranteeing the control of both data access and download request. •Cloud-based storage services have gained significant attention in recent decades due to their benefits such as access flexibility and cost-effectiveness.However, concerns about security breaches over outsourced data are a major obstacle to widespread use. •For example, users may need to share data with others without data encryption, which can be visible within the Dropbox administration level.

## II. ACCESS CONTROL AND DATA ENCRYPTION

Access control and data encryption are critical components of ensuring security in cloud-based data management.

1. Access control mechanisms manage who can access and manipulate data by enforcing authentication and authorization procedures.
2. Users must first log intocloud, undergo authority checks,and be granted appropriate permissions based on their roles.
3. Data encryption secures the data by converting it into a format that is unreadable without the correct decryption key
4. Files uploaded by the data owner are encrypted to protect against unauthorized access.
5. This process ensures that only authorized users can view or download the data, enhancing the overall security of the cloud storage system.
6. These techniques are essential for maintaining data confidentiality, integrity, and availability, and for protecting against threats such as unauthorized access , data breaches.
7. **Authentication**: This is the initial step where users provide credentials (such as usernames and passwords) to verify their identity. Multi-factor authentication (MFA) can further enhance security by requiring additional verification methods.
8. **Authorization**: After successful authentication, the system checks the user's permissions to determine what actions they are allowed to perform. Role-based accesscontrol (RBAC) or attribute-based access control (ABAC) can be used to assign different levels of access based on userroles or attributes.




## III.SYSTEM ARCHITECTURE

The nodes involved are admin and clients which stands as UI for the system. The deployment is performed as per the requirements of Hardware and software specified in the requirements phase.Key generation center is a key authority that generates public and secret parameters for CPABE. . It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights toindividual users based on their attributes. . Data storing center is an entity that provides a data sharing service.

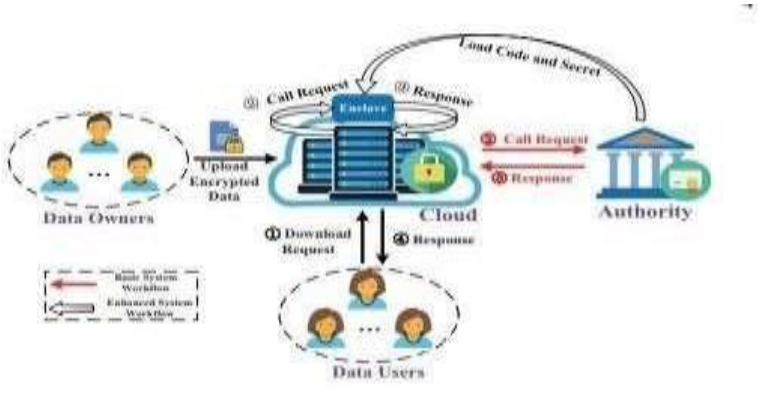



*Fig.1: Spira Change Request Work Flow*

## IV.INPUT DESIGN

The input design is the interface between the user and the cloud-based information system. It involves developing specifications and procedures for data preparation to ensure that transaction data is converted into a usable form for processing. This can be achieved by instructing the system to read data from various sources or by having users directly input the data. The design of the input focuses on minimizing the amount of input required, controlling errors, avoiding delays, eliminating unnecessary steps, and maintaining simplicity. For our project, the input design emphasizes both security and ease of use while retaining privacy. The input process ensures that data is encrypted before being uploaded to the cloud and that only authenticated and authorized users can access and manipulate the data. This design is crucial to prevent errors in data input, ensure data integrity, and guide management in obtaining accurate information from the cloud-based system.

## V.OUTPUT DESIGN

A quality output meets the requirements of the end user and presents the information clearly. In any system, the results ofprocessing are communicated to the users and other systems through outputs. In output design, it is determined how the information is to be displayed for immediate need and also inhard copy form. It is the most important and direct source of information to the user. Efficient and intelligent output design enhances the system's relationship with the user, aiding in decision-making.

1. Designing computer output should proceed in an organized, well-thought-out manner; the right output mustbe developed while ensuring that each output element is designed for ease of use and effectiveness. When analyzing and designing computer output, the specific output needed to meet the requirements should be identified. Methods for presenting information should be selected, and documents, reports, or other formats containing the information produced by the system should be created.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

For our project, "Dual Security Control for Cloud Storage and Data Sharing, ", the output form should accomplish one or more of the following objectives:

1.Convey information about past activities, current status, or
projections of future data access and sharing events.
2.Signal important events, such as unauthorized accessattempts, successful authentications, and data sharingactivities.
3.Trigger an action.
4.Confirm an action.

**Modules**

1. User Authentication and Authorization
2. Read &split Dataset To Train & Test Data Encryption and
3. Execute SVM Algorithms Access Control Management
4. Execute K-Means Algorithm Cloud Storage Integration
5. Economic Denial of Sustainability (EDoS) Mitigation
6. Data Sharing and Collaboration

## VI.RESULT

In Fig(a), after logging into the cloud and passing throughauthority checks, the data owner uploads and encrypts files

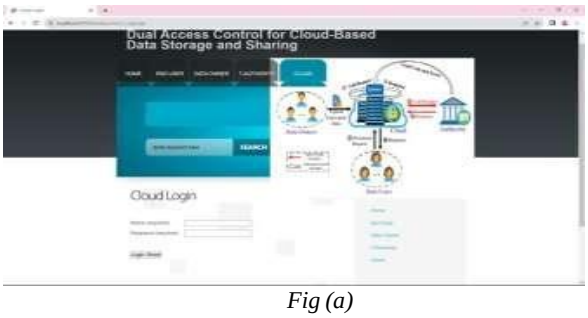



*Fig (a)*

Below screen Fig(b) is T-authority login page


*Fig (b)*

**Acknowledgement**

- We are extremely grateful to **Dr. A. Srinivasula Reddy**, Principal and **Dr. Madhavi Pingili,** HOD, **Department of IT, CMR Engineering College** fortheir constant support.
- We are extremelythankful **to Dr. X.S. Asha Shiny**,Associate Professor, Internal Guide, Department of IT, for her constant guidance, encouragement and moral support throughout the project.
- We express our thanks to all staff members and friends for all the help and co-ordination extended in bringing out this project successfully in time

## References

1. *Jianting Ning,Xinyi Huang,willy Susilo Secureand Efficient Dual Security Control Scheme inCloud Computing", 2024 5th International Conference on Mobile Computing SustainableInformatics (ICMCSI), pp.766-773, 2024.*
2. *Kaitai ,"Dual KeyAttribute-Based incloud Encryption with Outsource Revocation in Cloud Computing",202320th ACS/IEEE InternationalConference on ComputerSystems and Applications.*
3. *Ximeng Liu,Yinghui Zhang "A Review ofAccess Control Mechanisms for CloudComputing"2023 Third International Conference on Secure Cyber Computing andCommunication (ICSCCC), pp.337-343, 2023.*
4. *J. Ning, X. Huang, W. Susilo, K. Liang, X. Liu and Y. Zhang, "Dual Security Control for Cloud-Based Data Storage and Sharing," in IEEE Transactions on Dependable and SecureComputing, vol. 19, no. 2, pp. 1036-1048, 1 MarchApril 2022, doi: 10.1109/TDSC.2020.3011525.*
5. *Y. -H. Chen and P. -C. Huang, "Collaborative access control of cloud storage systems" 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 2018, pp.1063-1064, doi:10.1109/ICASI.2018.8394460.*
6. *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.*
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. *Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rashaan, Matthew Green, and Ariel D Rubin. Charm: a framework for rapidly prototyping cryptosystems. Journal ofCryptographic Engineering, 3(2):111–128, 2013.*
9. *Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, Hyesoon Kim, and Marcus Peinado.Inferring fine-grained control flow inside sgx enclaves with branch shadowing.In 26th USENIX Security Symposium, USENIX Security, pages 16–18, 2017.*
10. *Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rashaan, Matthew Green, and Ariel D Rubin. Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2):111–128, 2013.*
11. *AttainAmati, Shay Gueron, Simon Johnson, and VincentScarlata. Innovative technology for cpu based attestation and sealing. In Workshop on hardware and architectural support for security and privacy (HASP), volume 13, page . ACM New York, NY, USA, 2013.*
12. *Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.*
13. *John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.*
14. *Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1– 118, 2016.*
15. *Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.*