IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 7, July 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307046|

Enhanced Access Control for Cloud Data Storage and Sharing

Neha D K

PG Student, Department of Master of Computer Applications, PES Institute of Technology and Management, Shivamogga, India

ABSTRACT: In recent years, both academia and industry have become increasingly interested in the cost-effective and efficient management of cloud-based data storage services. Service providers must instantly adopt secure data exchange and storage procedures because they operate in an open network in order to safeguard data confidentiality and privacy of service users. The method most frequently employed to stop sensitive data from being hacked is encryption. However, the real-world demand for data management cannot be met by data encryption alone (using AES, for example). A robust download request access control system is also necessary to guard against attacks such as Economic Denial of Sustainability (EDoS), which try to stop users from accessing the service. In this study, we investigate dual access control in the context of cloud-based storage, making sure that efficiency and security are upheld while creating a control system for requests for both downloads and data access. Two dual access control systems are constructed in this study, one for a specific designed setting. The security and experimental analysis of the systems are also offered.

KEYWORDS: Encryption, Decryption, Database, Security and Authentication.

I. INTRODUCTION

Our project, "Enhanced Access Control for Cloud Data Storage and Sharing," was introduced with the goal of addressing the urgent demand for the safe and effective administration of sensitive data kept in cloud environments. Our project focuses on putting in place a strong system that guarantees data security, integrity, and availability in the current digital environment, where data breaches and unauthorized access pose serious concerns. The main goal is to create a system that allows for dual access control, in which authorization policies and different authentication factors are used to determine who can access stored data.

Although cloud computing provides unmatched accessibility and scalability, security issues continue to be of utmost importance. Our project encrypts data before storing it using cutting-edge encryption techniques like RSA (Rivest-Shamir-Adleman) and AES (Advanced Encryption Standard). This ensures that only authorized users with the right decryption keys may access crucial files. To further enforce granular permissions based on user roles and particular data attributes, the system integrates advanced access control techniques including Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).

To sum up, our research implements dual access control mechanisms that integrate authentication, access control, and encryption techniques to satisfy the urgent need for secure cloud-based data storage solutions. By doing this, we hope to offer a dependable and scalable platform that satisfies the dynamic security demands of contemporary businesses and promotes easy data management and regulatory compliance.

II. RELATED WORK

[1] Charm is a framework that has been developed by Joseph A. Akinyele, Christina Garman, et al. for rapidly prototyping cryptosystems. It provides a modular method for building cryptographic primitives, making it simple for researchers to test out various parts. Charm offers implementations for identity-based encryption, pairing-based cryptography, and attribute-based encryption, among other cryptographic algorithms. Its goal is to make it easier for academics to create and test new cryptographic algorithms by giving them a productive and adaptable environment.

[2] Innovative technology for CPU-based attestation and sealing is presented by Ittai Anati, Shay Gueron, Simon

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307046|

Johnson, and Vincent Scarlata. Hardware and architectural support for security and privacy are the main points of emphasis. It covers methods for securing sensitive data on CPU platforms and safely verifying the integrity of software. In order to improve the security of the attestation and sealing procedures and defend against different types of attacks including tampering and illegal access, the suggested solutions make use of hardware features.

[3]A revocable hybrid encryption method based on attribute-based encryption (ABE), symmetric searchable encryption (SSE), and Intel Software Guard Extensions (SGX) is introduced by Alexandros Bakas and Antonis Michalas. The approach allows for fine-grained access control and search capabilities, while offering a flexible and effective method of encrypting data. The system provides strong security assurances and dynamic access right revocation by integrating ABE and SSE with SGX, which makes it appropriate for contemporary data protection standards.

[4]Amos Beimel's thesis, which focuses on cryptographic protocols for safely transferring secret information among several participants, offers secure systems for key distribution and secret sharing. The thesis examines several methods of key distribution and secret sharing and evaluates their effectiveness and security. It advances secure multi-party computing and key management protocols by putting out innovative schemes to meet various security and usability needs.

[5]Ciphertext-policy attribute-based encryption (CP-ABE), a cryptographic primitive introduced by John Bethencourt, Amit Sahai, and Brent Waters, enables data owners to define access policies based on user attributes. Fine-grained access control over encrypted data is made feasible by CP-ABE, where users whose attributes meet the access policy are the only ones who can decode the data. In addition to effective building techniques and security evaluations, the study provides a formal description of CP-ABE and illustrates its applicability in a number of contexts, including data sharing and cloud computing.

[6]An extensive explanation of Intel Software Guard Extensions (SGX), a technology intended to improve the security of data and application code on Intel CPU systems, is given by Victor Costan and Srinivas Devadas. It talks about SGX's architectural characteristics, such as memory encryption and secure enclaves, and how it can shield critical computations from manipulation and unwanted access. The study offers insights into the practical usage and limitations of SGX by examining potential security concerns and mitigating strategies.

[7]Ben Fisch, Dhinakaran Vinayagamurthy et al. introduces IRON, a functional encryption scheme that leverages Intel SGX to provide fine-grained access control over encrypted data. IRON allows data owners to specify access policies as functions, enabling selective decryption based on the inputs provided by users.

III. PROBLEM STATEMENT

Conventional cloud storage solutions frequently use weak access control and single-layer encryption, which exposes data to a variety of risks including insider threats, unauthorized access, and hacking.

User confidence in cloud storage services is undermined by the exposure of sensitive information to potential exploitation and compromise due to a lack of strong security safeguards. In order to overcome these problems, our solution introduces a two-tier access control system that offers multiple security levels to protect cloud-stored data. We aim to reduce the risks associated with unwanted data access and improve the overall security posture of cloud-based data storage systems by putting robust authentication procedures, dynamic access controls, and advanced encryption techniques into practice.

IV. DESIGN AND IMPLEMENTATION

In order to secure data stored in the cloud, this project entails developing a complete enhanced access control system that incorporates authentication, access control, and encryption techniques. Data owners will be able to precisely manage who can access their files and under what circumstances by defining fine-grained access rights and encryption keys within the system. Users will be able to safely upload, read, and manage their files using an intuitive interface, reducing the possibility of illegal data access and guaranteeing adherence to data privacy laws. Because of its scalable architecture, the system can be easily integrated with current cloud storage platforms and expanded to meet changing

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307046|

user and organizational needs.

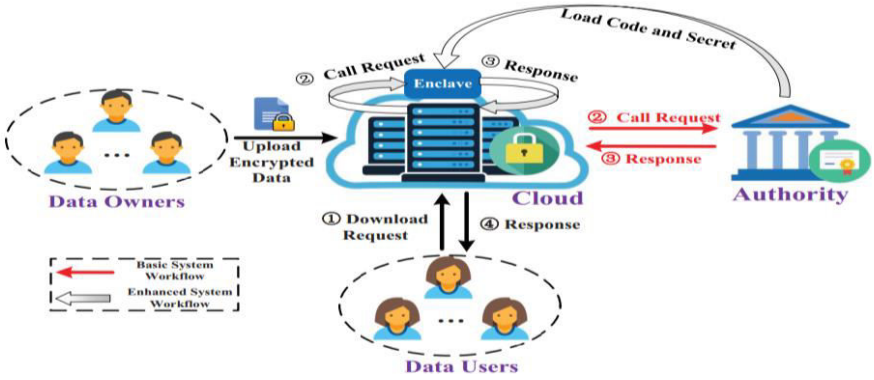

Figure 1 : System Architecture

Our project, "Enhanced Access Control for Cloud Data Storage and Sharing," has a system architecture that is made to offer a stable and expandable foundation for protecting data that is kept on the cloud. The architecture is made up of a few essential parts, each of which is vital to maintaining the availability, confidentiality, and integrity of the data. The design is based on the client-server paradigm, in which servers manage data processing, storage, and security while clients communicate with the system via an intuitive user interface. .. Users may upload, view, and manage their files safely via the client-side interface, which also offers tools for setting encryption keys and access controls. Several security layers are put in place on the server side to safeguard data while it's in transit and at rest. These consist of authentication procedures, access control guidelines, and encryption algorithms that cooperate to verify user identities, grant access to information, and uphold security regulations. A centralized database is also included in the architecture to store user credentials, access logs, and other system-related data, making authentication and auditing procedures easier. All things considered, the system architecture is made to be both extendable and adaptable, making it simple to integrate with current cloud storage platforms and to meet future scalability and enhancement needs.

V. RESULTS AND DISCUSSION

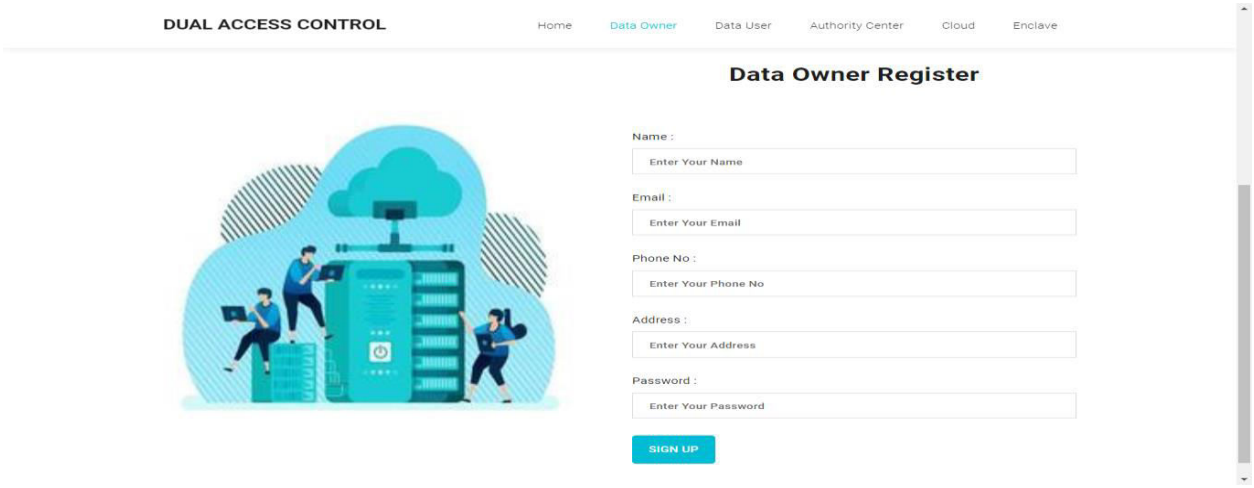

Figure 2: Data owner register page

The data owner is the one who saves the info in the cloud in the encrypted way and shares the data to users by creating the access to limited or authorized users.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307046|

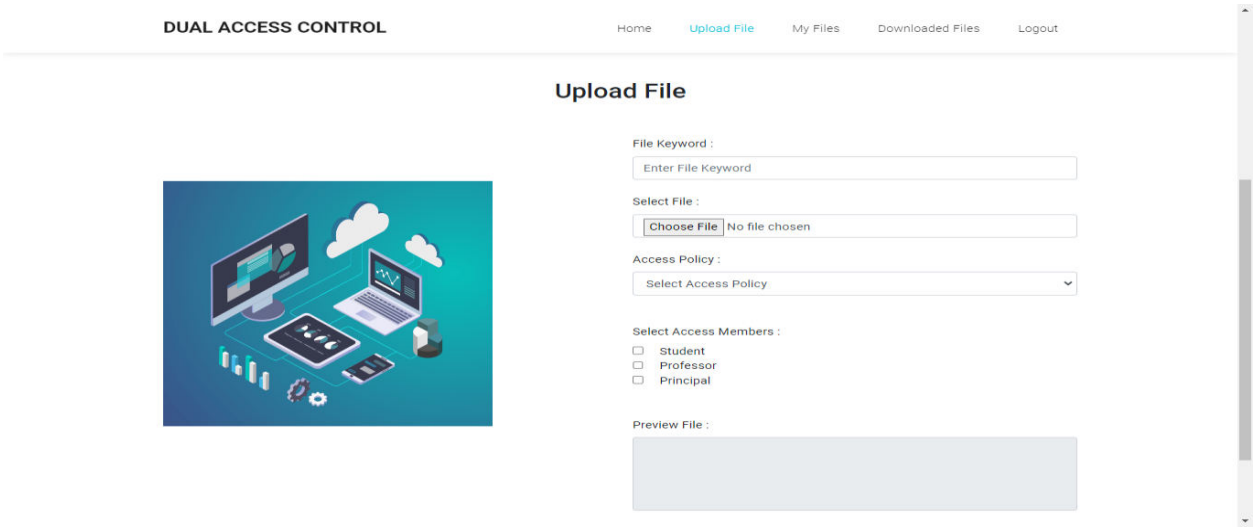

Figure 3: Upload file

The above figure shows the uploading a file to the cloud with the access privacy like read and download option or access members like student, professor, principal.

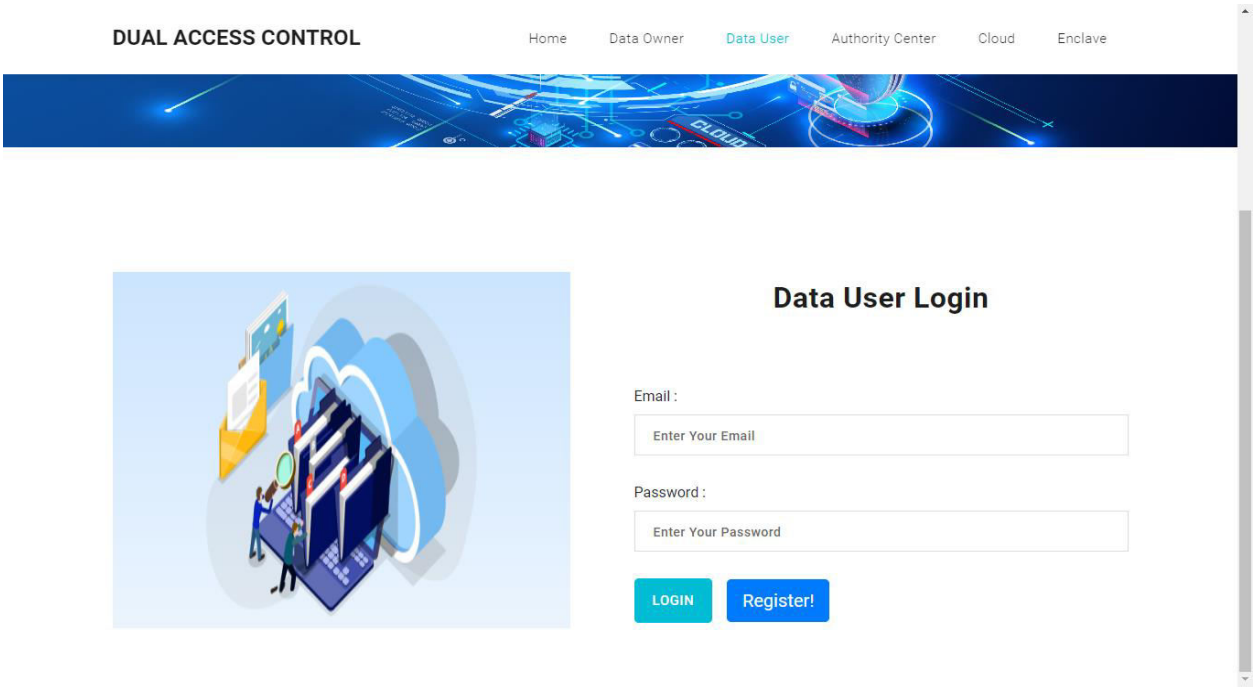

Figure 4: Data User login page

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307046|

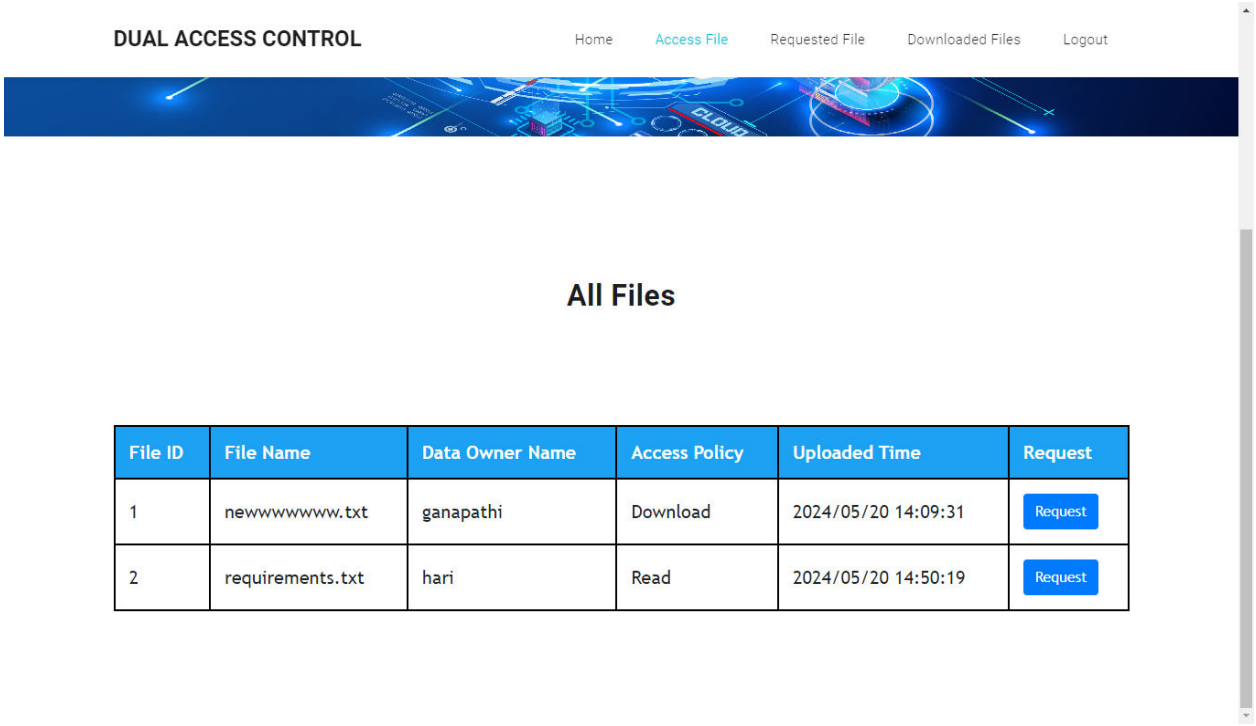

Figure 5: All files

The above fig shows the all files which are shared data owners so that the user can request to read or download the files.

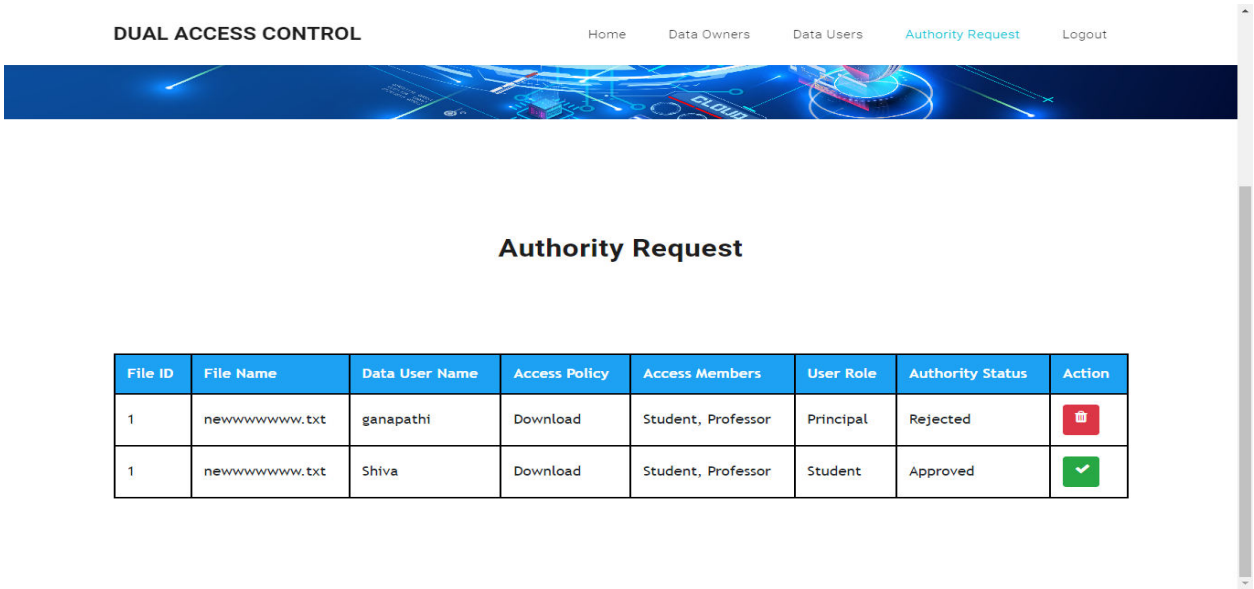

Figure 6: Authority Request

The fig shows the approved and rejected Data users.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307046|

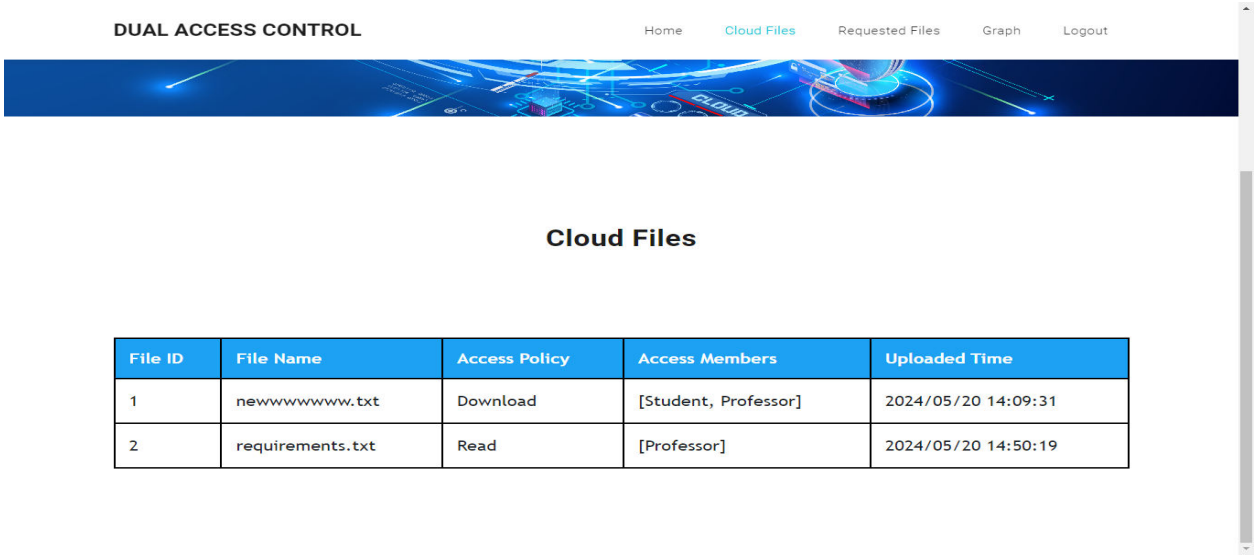

Figure 7: Cloud files

The above fig shows the list of Files which are uploaded by the data owners with access policy and access members.

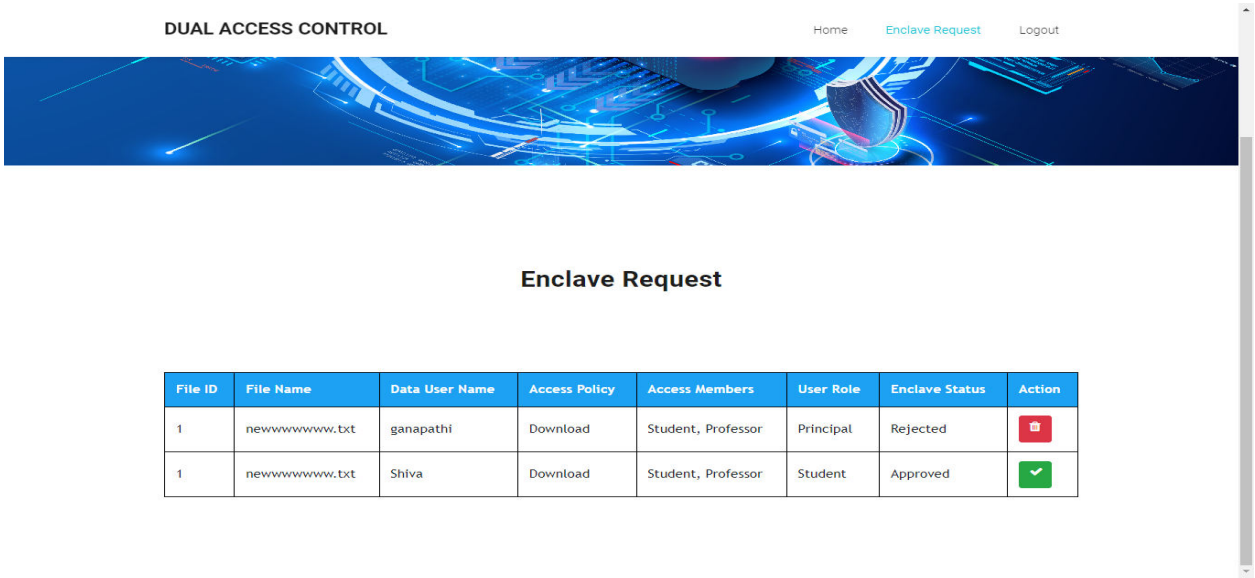

Figure 8: Enclave Request

The above file shows the list of files which are requested by the data users.

VI. CONCLUSION AND FUTURE WORK

By putting in place two dual access control systems designed to survive DDoS/EDoS attacks, we were able to handle a serious and long-lasting issue: cloud-based data sharing. We assert that the download request management method is modifiable by different CP-ABE architectures. Our experimental results demonstrate that the proposed systems impose negligible computational or communication overhead as compared to the underlying CP-ABE paradigm. We take use of the fact that private information kept in an enclave cannot be deleted in our improved system. According to recent research, an enclave may be able to divulge some of its secrets to a malicious host through side-channel attacks or other

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753; p-ISSN: 2347-6710|

Volume 13, Issue 7, July 2024

|DOI: 10.15680/IJIRSET.2024.1307046|

memory access patterns. As a result, the transparent enclave execution model was presented. Using transparent enclave execution to offer a dual access control strategy for cloud data sharing is one intriguing challenge. In future study, we will investigate possible solutions to this problem.

REFERENCES

[1] Joseeph Akiinyele, Christina Garman, Matthew W, Michael Rusihianan, Mattheew Green, and l D Rubiin. Charm: a framework rapidly prototype cryptosystems. Journal of Cryptographic Engiineering, 3(2):111–128, 2013.
[2] Ittai Simon Johson, and Vincent Sciarlata. Innovatiive technology for cpu based atteistation and sealing. Inn Workshop on hardware and arcohitectural support for security and privacy (HASP), volume 13, page 7. ACM New York, NY, USA, 2013.
[3] Alexandros and Antionis Michalas. family: A revocable hybriid encrypted scheme based on attribute-based encrCyption, symmetric searchable encryption and SGX. In SecureeComm 2019, pages 472–486, 2019.
[4] Amos Beiimel. Secure schemes secret sharing and key distribiution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
[5] John Bethencouriit, A Saihai, and Waters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.
[6] Victor Costain and Srinivas Devaidas. Inteil sgxi explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.
[7] Ben Fiisch, Dhinakaran Vinayagamurthy, Dan, and Gorbiunov. IRON: functional encryptiion using intel SGX. In Proceediings of the 2017 ACM SIGSAC Conference on Computer and Communicatiions Security, CCS 2017, pages 765–782, 2017.
[8] Eiichioro Fujisiaki and Tatsuaki Okamoito. Secure integratiion and symmetriic encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–554. Springer, 1999.
[9] Viipul Goyali, Pandey, Amit Sahai, and Brent s. Attribute-based encryption for fiine-grained access control of data. In ACM CCS 2006, pages 89–98. ACM, 2006.
[10] Jiinguang Han,Yii Mu, and Man Ho Alleno Au. Improving privacy to security in decentraliized ciphertext-policy attriibute-based encryption. IEEE transactions on information forensics and securitys, 10(3):665–678, 2015.
[11] Christofer Hofif. Cloud computiing security: From ddos (distriibuted denial of service) edos (economic denial of sustainability). http://www.. rationalsuarvivability.com/blog/?p=66.
[12] Joseph Idziorek, Mrark Tanniian, and Jacoibson. Attributiion of frauduleent resource consumption to cloud. In IEEE CLOUD 2012, pages 99–106. IEEE, 2012.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details