International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228424

A Novel Approach for Providing Security to Data Using Dual Access Technique

N. Shanmuka Srinivas*[1], V K Venugopal[2]
[1,2]PG Scholar, Department of Computer Application, Madanapalle Institute of Technology and Science, India

Article Info

Publication Issue :

Volume 8, Issue 4
July-August-2022

Page Number : 308-315

Article History
Accepted: 10 August 2022
Published: 30 August 2022

ABSTRACT

Cloud-based data storage service has drawn increasing interests from both academic and industry in the recent years due to its efficient and low-cost management. Since it provides 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. merely encrypting data (e.g., via AES) cannot entirely satisfy the actual necessity of data management. Moreover. On the off chance that download demand can be effectively controlled, EDoS attacks can't be launched to prevent customers from receiving a charge out of administration. In this paper, we consider the double access control, with regards to AWS cloud-based capacity, as in we plan a control system over the two information get to and download demand without loss of safety and efficiency. Two dual access 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

Keywords : Cloud, Searchable Encryption, Multi-Keyword Search, Multi-User Access, Search Pattern, Access Pattern.

I. INTRODUCTION

Over the past few decades, AWS Cloud-based storage services have drawn the interest of both academics and industry. As a result of its broad list of benefits, including access flexibility and free local data management, it may be widely utilized in various Internet-based commercial applications (e.g., Apple I Could). Individuals and businesses are increasingly turning to the AWS Cloud to store and manage their data in order to avoid the expense of updating their local data management facilities and devices. Internet consumers may be deterred from adopting AWS Cloud-based storage services because of concerns about security breaches. There are a number of situations in which outsourced data may need to be shared with others in order to be used effectively. If you're a Dropbox user named Alice, you might be able to exchange photographs with your pals via the Dropbox application. It is necessary for Alice to

establish a sharing link and then share it with her friends in order to share photographs without data encryption. Even if the sharing link is hidden from unauthorized users (e.g., those who aren't Alice's friends), it is visible at the Dropbox management level (e.g., administrator could reach the link). To protect data security and privacy, it is typically advised to encrypt data before uploading it to the AWS Cloud.

In this case, one option is to encrypt the data before uploading it to the AWS Cloud, such that only a specific AWS Cloud user (with a valid decryption key) may decode the data. Encrypting the material before sharing it with others is an easy approach to prevent "insiders" from seeing shared photographs. It's possible that Alice has no idea who the photo recipients/users will be. Alice may only be aware of the properties of picture receivers, which is feasible. Because the encryption must know in advance who the data receiver is, standard public key encryption (e.g. Paillier encryption) is not an option here. To ensure that only authorized individuals may view the photographs, Alice should have access to a policy-based encryption mechanism over the outsourced photos.

Known as a resource-exhaustion attack, resource-exhaustion attacks are frequent in AWS Cloud-based storage services. A malicious service user may launch denial-of-service (DoS)/distributed denial-of-service (DDoS) attacks on a AWS Cloud storage service server to consume the server's resources so that the AWS Cloud service is unable to respond to honest users' service. Since a public AWS Cloud may not have any control over download requests(namely, a service user may send unlimited numbers of download requests to AWS Cloud server), Because of this, economic components of the "pay as you go" model might be affected owing to increased resource use. Users of AWS Cloud services will see their bills skyrocket.

As a solution to these two issues, we suggest in this work a novel method called dual access control. It's possible that attribute-based encryption (ABE) [9] might be a good option for securing data in a AWS Cloud-based storage service. ABE allows for the confidentiality of outsourced data as well as fine-grained management of the outsourced data. There are a number of data encryption methods available, including Ciphertext Policy ABE (CP-ABE) [5]. It should be noted that this article considers the usage of CP-ABE as part of our methodology. Although CP-ABE may be used to create a sophisticated system that ensures the control of both data access and download requests, it is not sufficient.

II. RELATED WORKS

Alexandros Bakas and Antonis Michalas. Modern family: Secure distributed storage is considered as quite possibly the main issue that the two organizations and end-clients consider prior to moving their private information to the cloud. Recently SSE is an intriguing notion, and Attribute-Based Encryption is a well-established area (ABE). Using the advantages of SSE and ABE, we suggest a half-and-half encryption scheme. Instead of relying on the ABE plot, we aim to utilise a repudiation instrument that is completely independent of it.

Antonis Michalas. The lord of the shares: combining attributebased encryption and searchable encryption for flexible data sharing: Secure distributed storage is viewed as quite possibly the main issue that the two organizations and end-clients are thinking about prior to moving their private information to the cloud. Recently SSE is an intriguing idea, as is Attribute-Based Encryption (ABE). First, analysts are trying to create conventions where customers' information is protected from both internal and outside attacks, without considering the issue of client repudiation. Denial is a problem that can be addressed by current techniques Not that it makes any difference because ABE plans and cypher text sizes are still used to determine suggested conventions. SSE and ABE are combined in this article so that the major benefits of each strategy may be exploited. By using an SSE

scheme, clients may easily see encoded data, while a Cipher text-Policy Attribute-Based Encryption scheme ensures the matching symmetric key necessary for decoding.

G. Wang, C. Liu, Y. Dong, P. Han, H. Pan, and B. Fang, "Idcrypt: A multi-user searchable symmetric encryption scheme for cloud applications," : Accessible Encryption (SE) has been widely analyzed by both scholarly and industry specialists. While numerous scholarly SE plans show provable security, they generally uncover some inquiry data (e.g., search and access designs) to accomplish high effectiveness. In any case, a few induction assaults have taken advantage of such spillage, e.g., a question recuperation assault can change over obscure inquiry secret entryways to their comparing catchphrases dependent on some earlier information. Then again, many proposed SE plans require huge change of existing applications, which makes them less reasonable, feeble in ease of use, and hard to send. Accessible Encryption (SE) has been widely analyzed by both scholarly and industry specialists. While numerous scholarly SE plans show provable security, they generally uncover some inquiry data (e.g., search and access designs) to accomplish high effectiveness. In any case, a few induction assaults have taken advantage of such spillage, e.g., a question recuperation assault can change over obscure inquiry secret entryways to their comparing catchphrases dependent on some earlier information. Then again, many proposed SE plans require huge change of existing applications, which makes them less reasonable, feeble in ease of use, and hard to send.

Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong. Combining data owner-side and cloud-side access control for encrypted cloud storage: People may believe in the promise of distributed computing, but owing to the absence of client-cloud controllability, they don't completely trust cloud providers to safeguard critical information. Data owners employ scrambled information instead of plaintexts so that they may be guaranteed that their data is appropriately categorized. Cryptography that uses code-based cipher-text can be used to safeguard encoded records when they are exchanged with numerous clients Difficult to defend against a wide range of attacks. A byproduct of this was that many of the earlier ideas did not allow the cloud provider to evaluate whether or not a downloader was capable of decoding. These papers should be available to anybody with access to the distributed storage. Denial-of-service (DoS) attacks can be launched by someone with malicious intent who downloads huge data sets to overwhelm the cloud's resources. It follows that costs associated with cloud management will be paid by the payer. Aside from that, cloud providers perform as both the accountant and the payment of asset utilization fees, leaving information owners in the dark. Developing ssa public, verifiable sharable storage system should clear these problems. On this page, we propose a solution for safeguarding cloud storage from EDoS assaults and maximizing the usage of assets. ABE's CP-self-assertive access technique is used to decide access, given there are no predetermined plans in place. The execution and security investigation are followed by two conventions for various scenarios.

Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma, and Lifei Wei. Auditable σ-time outsourced attribute-based encryption for access control in cloud computing: With its complex approach to access control over encrypted data, policy attribute-based encryption (CP-ABE) is an interesting choice for cloud computing applications that require high levels of security. However, there are two main problems with CP-ABE that need to be addressed before it can be widely used in commercial applications. In the first place, decryption leads in significant pairing costs, which tend to rise in proportion to the size of the access policy in question. Your attribute set must match the policy in order to have unlimited access to cipher-text. CP-strength You might not be able to utilise real-world apps with ABE's access rights (e.g., pay-as-you use). These problems are addressed in this

article by proposing an outsourced cloud-based ABE that can be audited in real time. It is our belief that decryption's costly pairing process can be offloaded to the cloud, while its accuracy can be verified efficiently. Control over access to data is also provided. Users' access privileges to cloud services may be restricted for a specified period of time by cloud service providers. A separate concern in preventing key leakage is incorporated into the idea as well. Having a third party get access to a victim's cipher texts is not aided by a user's decryption key being leaked. On a key encapsulation mechanism setting, Rousakis and Waters CP-ABE is utilized. When it comes to scalability and efficiency, we employ security and rigorous experimental analysis.

III. METHODS AND MATERIAL

Proposed system:

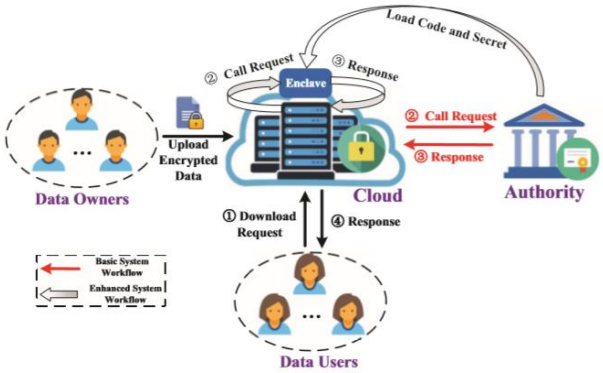


Figure 1: Block diagram of proposed method

Implementation:

The project has implemented by using below listed algorithm.

AES Algorithm:

To encrypt data, round keys are used. As well as other processes, they are performed on the data to be encrypted, which is stored in an array of data. 'State' is the name we give to this array. You encrypt a 128-bit block with AES using the following steps:

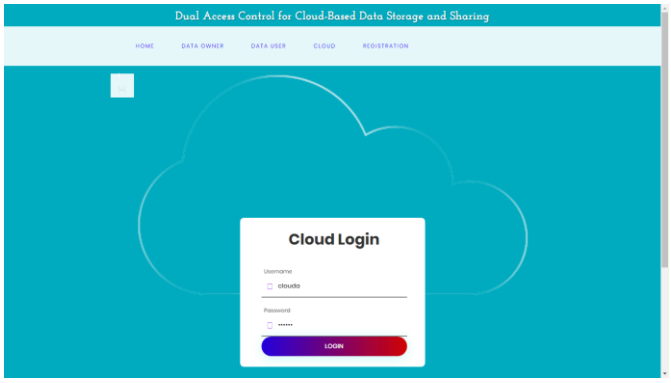
- Derivation of a collection of round keys from a cypher key is required.
- Block data is used to initialize the state array (plaintext).
- Create a new beginning state array with the initial round key.
- It is recommended to do nine rounds of state modification.
- Last but not least, do the eleventh round of state modification!
- Final state array as encrypted data copy out of final state array (cipher-text).
- The tenth round requires a somewhat different manipulation than the others, which is why the rounds are stated as "nine followed by a final tenth round."

To encrypt a block, all you need is a 128-bit sequence. To use AES, we must first transform the 128 bits into 16 bytes before we can use it. However, in actuality, it's very probably already saved this manner, so there's no need to "convert." A two-dimensional byte array with four rows and four columns is used for RSN/AES operations. As soon as you start the encryption.

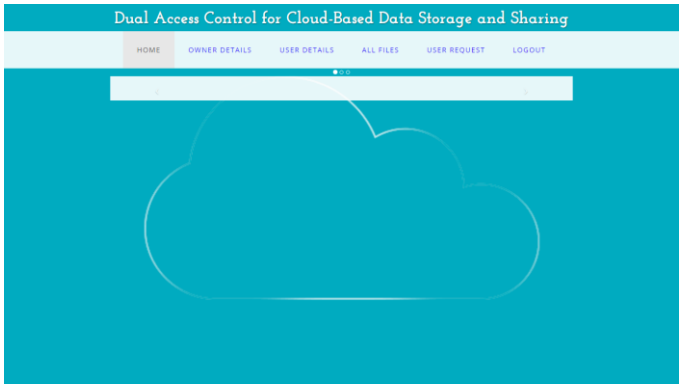
IV. RESULTS AND DISCUSSION

Home page:

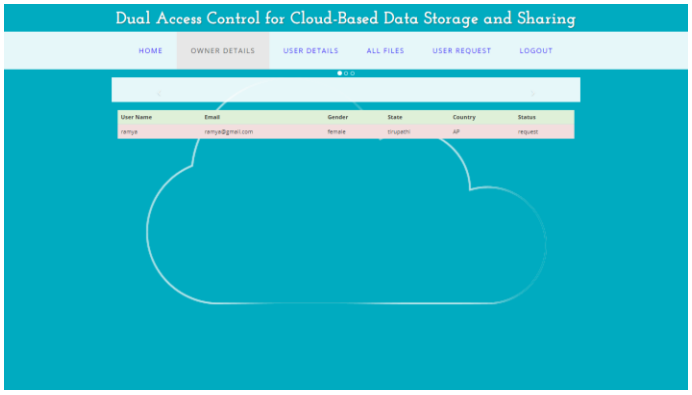
Cloud A login page:



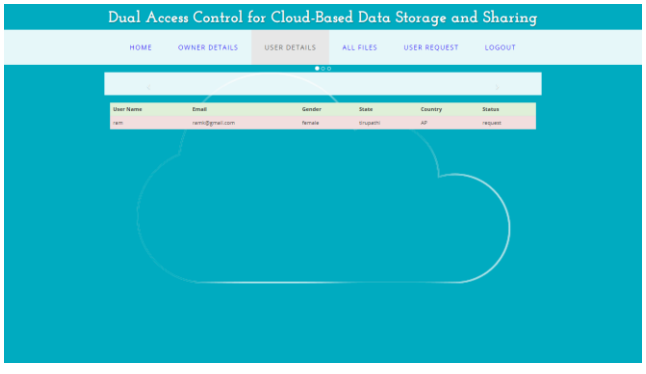
Cloud A home page:



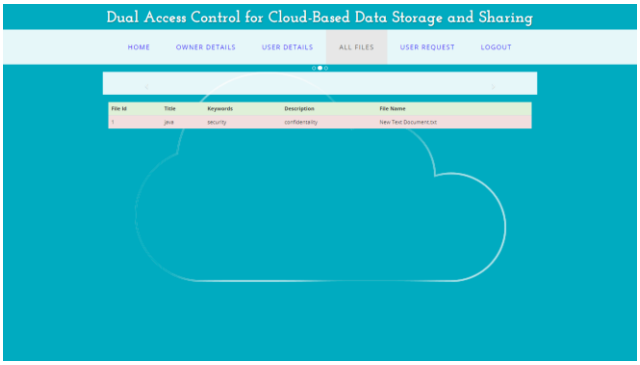
Owner Details:



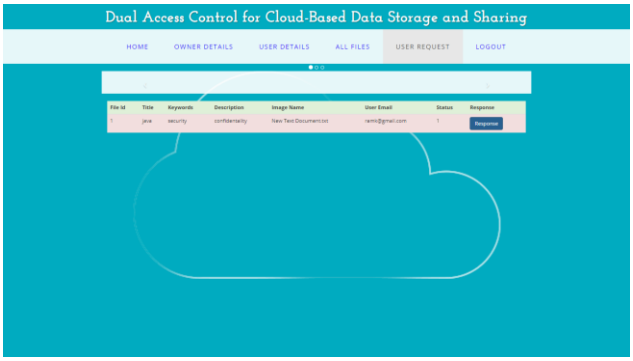
User Details:



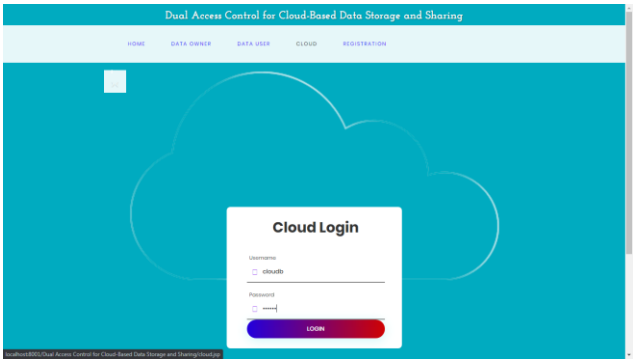
All Files:



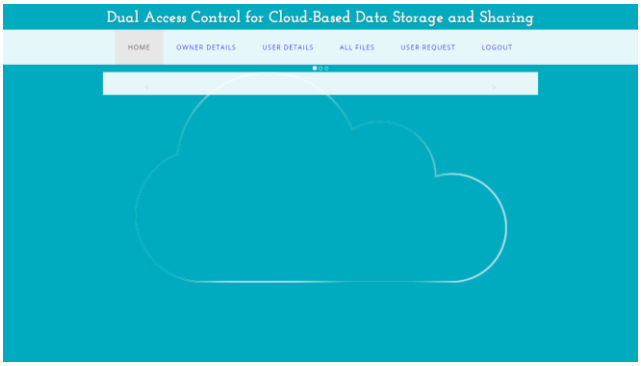
User Request:



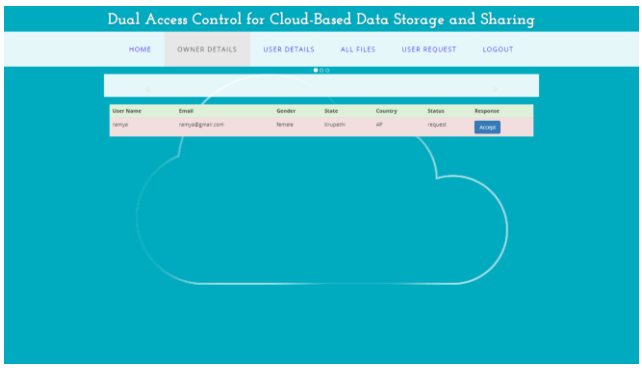
Cloud B login page:



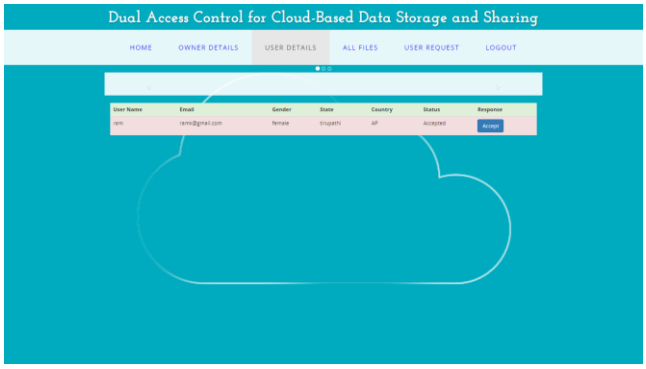
Cloud b home page:



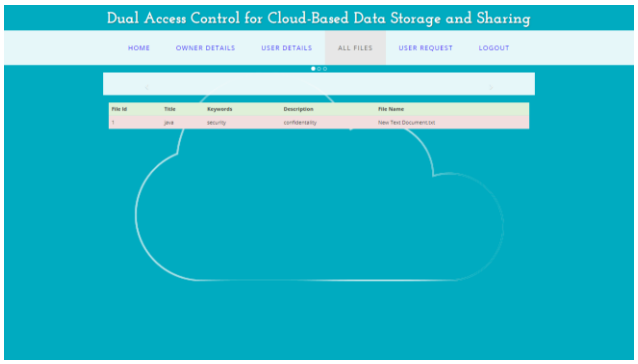
Owner details:



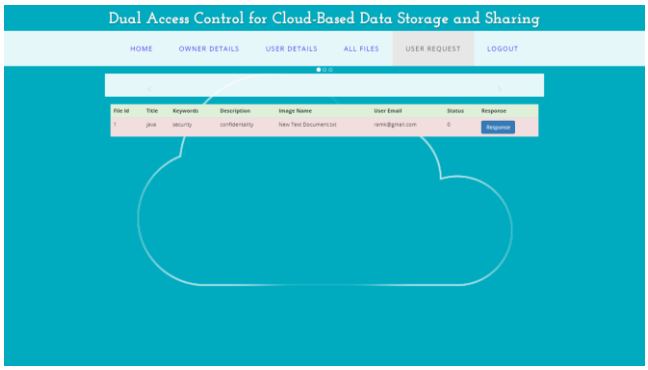
User details:



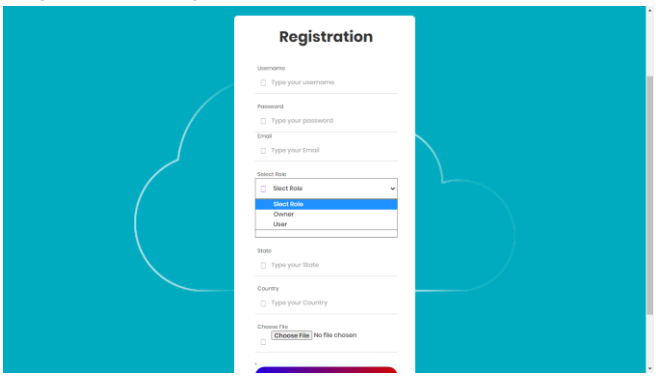
All files:



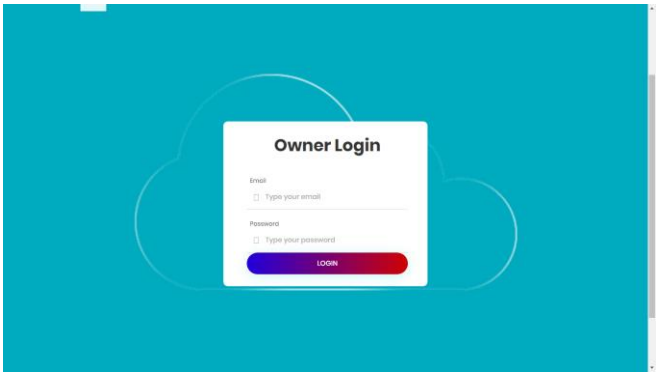
User request:



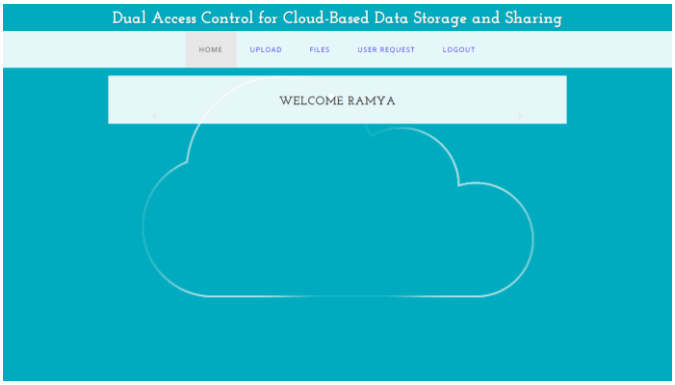
Registration page:



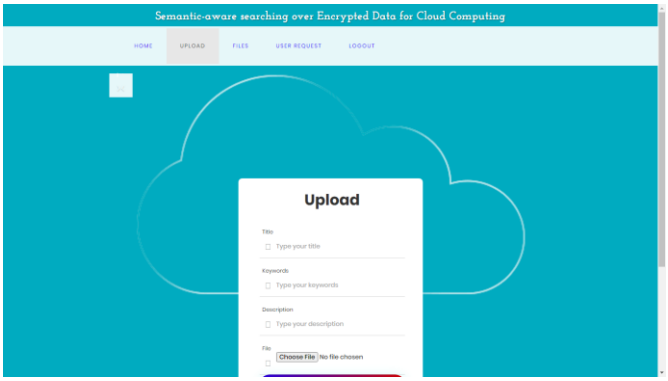
Data owner login page:



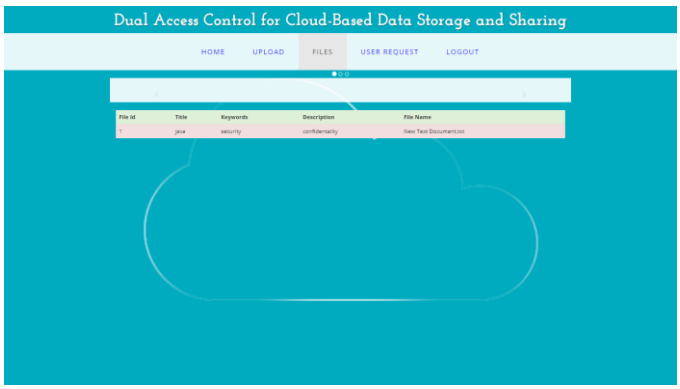
Owner home page:



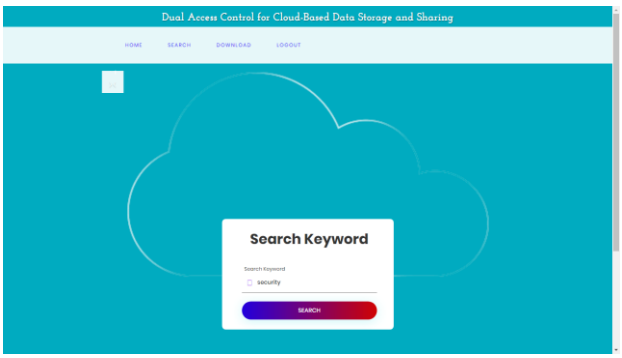
Upload:



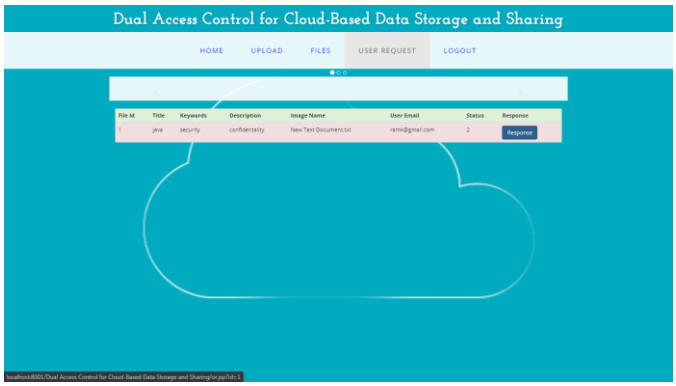
Files:

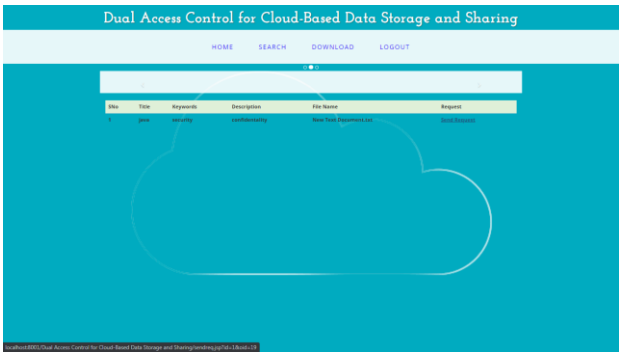


Search:

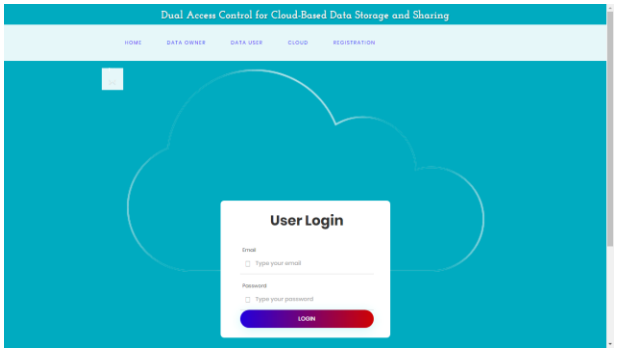


User request:

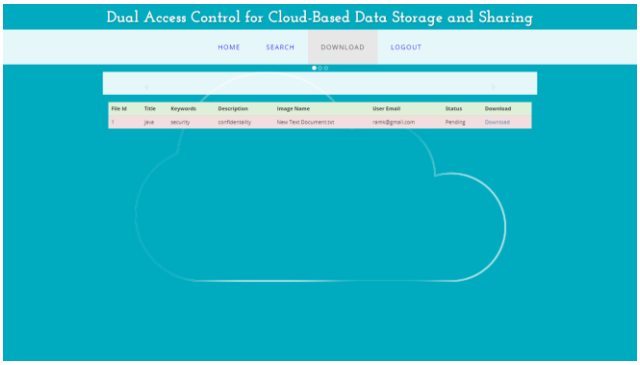




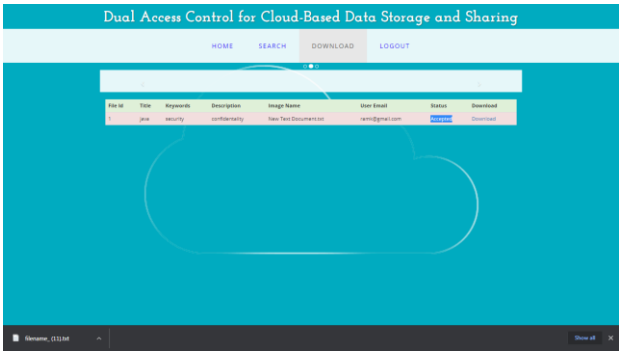
User login page:



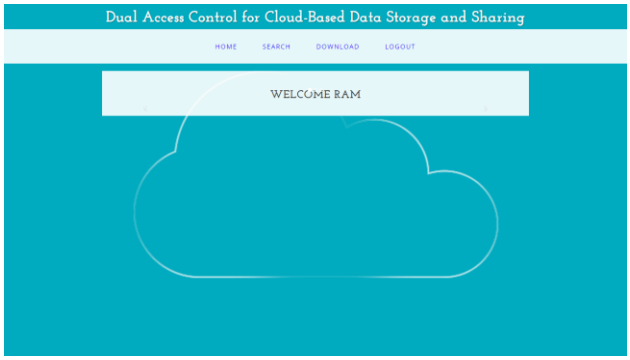
Download: pending



Download file:



User home page:



V. CONCLUSION

In this article. On the topic of cloud-based data sharing, we presented two dual access control solutions that solved an important and long-standing

challenge in cloud-based data sharing. DDoS/EDoS assaults are not a problem for the suggested solutions. However, we assert that it is "transplantable" to different CP-ABE structures the approach employed to obtain the characteristic of control on download request. No significant computational and communication overhead was seen in our experiments (compared to its underlying CP-ABE building block). Enclaves are used to protect secret information from being accessed, and our system takes use of this feature. Enclaves may disclose part of their secrets to a hostile host through memory access patterns or other similar side-channel assaults, according to new research. It is therefore necessary to propose the concept of transparent enclave execution (TEE). This is an intriguing problem: building a dual access control mechanism for AWS cloud data sharing from transparent enclave In the future, we'll look at the answer to the problem.

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

[5]. 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.

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

[7]. 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.

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

[9]. Joseph Idziorek, Mark Tannian, and Doug Jacobson. Attribution of fraudulent resource consumption in the cloud. In IEEE CLOUD 2012, pages 99–106. IEEE, 2012.

[10]. Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksfoabe: outsourced attribute-based encryption with keyword search functionforcloudstorage. IEEETransactionsonServicesComputing, 10(5):715–725, 2017.

Cite this article as :

N. Shanmuka Srinivas, V K Venugopal, "A Novel Approach for Providing Security to Data Using Dual Access Technique", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 4, pp. 308-315, July-August 2022.

Journal URL : https://ijsrcseit.com/CSEIT228464