International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Cloud-Based Data Storage and Sharing with Dual Access Control

N. Sai Varsha, B. Triveni

MCA, Associate Professor DVR and Dr HS Mic College of Technology, Andhra Pradesh, India

ARTICLEINFO

Article History:

Accepted: 10 June 2023
Published: 29 June 2023

Publication Issue
Volume 10, Issue 3
May-June-2023

Page Number
1126-1134

ABSTRACT

In recent years, the cost-effective management of cloud-based data storage has piqued the interest of both businesses and educational institutions alike. Service providers must implement secure data storage and sharing mechanisms to protect data confidentiality and service user privacy because they provide their services over an open network. Encryption is the most well-known strategy for shielding delicate information against splitting the difference. The down-to-earth need for information the executives can't, notwithstanding, be completely met simply by scrambling information. To stop A robust access control system for download requests and economic denial of sustainability attacks that would prevent users from using the service should also be taken into consideration. In this arrangement, we consider cloud-based capacity double access control as in we make a control component for both download solicitations and information access without forfeiting security or viability. Every one of the two double access control frameworks proposed in this study is custom fitted to a particular arranged climate.

Keywords: Access Control, Cloud Storage Service, Cloud-Based Data Storage, Intel SGX, and Attribute-Based Encryption.

I. INTRODUCTION

The on-request accessibility of PC framework assets, specifically information capacity and handling power, without direct dynamic oversight by the client, is known as distributed computing. The expression is regularly used to depict server farms that are available to a few groups on the web. Capabilities from focal servers are oftentimes spread across a few areas by huge mists, which is normal these days. It very well may be alluded to as an edge server on the off chance that the association with the client is sensibly close.

Both scholarly communities and businesses have offered cloud-based capacity benefits a ton of consideration. Because of its broad rundown of benefits, which incorporates access opportunities and the absence of neighborhood information organization, it could be generally utilized in numerous Web-based business applications. These days, a developing number of individuals and organizations like to re-appropriate their information to distant mists to try not to need to update their neighborhood information in the executive's offices or gadgets. However, The security vulnerability is raised because outsourced data may be one of the main obstacles preventing Internet users from widely utilizing cloud-based storage services. Reevaluated information might be viewed as information in numerous down-to-earth applications. At whatever point shared again with others. As a Dropbox client,

Alice could share photographs with her companions. Alice must first generate a sharing link before sharing the images with friends without using data encryption. Despite the fact that it guarantees some access control for unauthorized users (such as Alice's friends), the sharing link may be viewable at the Dropbox administrator levels. To resolve the two issues framed above, we propose a fresh plastic new strategy called double access control. One of the promising competitors for getting information in cloud-based capacity administrations is quality-based encryption (ABE), which enables the classification of reevaluated information and fine-grained command over the reappropriated information. Especially, Code text-Strategy ABE (CP-ABE) is a reliable method for encrypting data that lets you specify access rules over scrambled data, which determine who has access to intended recipients. Please be aware that this study may incorporate CP-ABE into our mechanism. In any case, using the CP-ABE system alone is lacking to make a refined part that ensures the control of the two data access and download requests. A misrepresentation strategy to control download demands is to use sham code texts to verify the information recipient's decoding freedoms. It explicitly requires Alice, the proprietor of the information, to transfer various testing figure texts to the cloud alongside the genuine encryption of the information. The testing figure messages are the encryptions of made-up messages with a similar access strategy as genuine information. Cloud asks Sway to haphazardly decode one of the testing figure texts after receiving a download request from a client, whom we should call Bounce. The weave is able to download the relevant scrambled text from the cloud if an appropriate outcome or decoding is provided (i.e., demonstrating that Sway has genuine unscrambling abilities). Alice has allowed Bounce access to genuine information.

We respond positively to the previous question by demonstrating two cloud-based dual access control systems that are both secure and efficient in different contexts1. The reason for this concise clarification of the innovation guide is to give a proficient double access control strategy. To ensure the classification of rethought information without forfeiting strategy-based admittance control, we start with a CP-ABE framework, which is viewed as one of the structure blocks. In addition to the CP-ABE system, we utilize powerful commands over client download demands for information. We plan to deal with not using the method of testing figure text in a different way. Specifically, we empower the client with the information to create a download demand. Upon receiving the download request, a cloud server can determine, with the assistance of Intel SGX's authority or enclave, whether the data user has permission to access the data. The user's authorization status is the only information the cloud server has about them. The cloud keeps control of the download demand thanks to the above instrument. We give the data owner the option to send a random copy of their private key in a download request. The download request keeps the secret key's "decryption capability" in order to test whether the owner of the underlying data can decipher the shared cipher text(s). Due to the random nature of the aforementioned component in the download request, it is impossible to identify who owns the secret key. This indicates that the download demand is unknown, allowing the cloud to determine whether the information owner is authorized without learning the basic information owner's name. The authority or Intel SGX enclave must be involved in the verification of download requests in order to further prevent the cloud from receiving sensitive data. Our first system is designed to handle situations in which the Intel SGX enclave is used to verify download requests, while our second system is designed to handle situations in which authority assistance is required to verify download requests. The approach that we just talked about is compatible with the majority of the CP-ABE constructs that are currently in use, all of which are based on bilinear maps.

II. RELATED WORKS

Alexandros Baka's and Antonis Michalis. Modern family: Both businesses and end users consider the most crucial aspect before migrating their private data to the cloud: safe storage that is distributed. SSE is an intriguing idea of ongoing times, and characteristic-based encryption (ABE) is a deeply grounded field. We propose a creamer encryption strategy that exploits the upsides of SSE and ABE. Instead of relying on the ABE plot, we intend to use a repudiation tool that is completely independent of it.

Antonis Michalis. The lord of the shares: combining attribute based encryption and searchable encryption for flexible data sharing: Before moving their private information to the cloud, both businesses and end users are considering the most pressing issue: secure distributed storage. Attribute-Based Encryption (ABE) and SSE have recently emerged as intriguing concepts. First, analysts are attempting to establish conventions that safeguard customers' information from both internal and external threats without taking into account the issue of client repudiation. ABE plans and cipher text sizes are still utilized to determine suggested conventions, so denial is a problem that can be addressed using current methods. SSE and ABE are consolidated in this article so the significant advantages of every procedure might be taken advantage of. Clients can easily see encoded data with an SSE scheme, and a Cipher text-Policy Attribute-Based Encryption scheme guarantees the symmetric key needed for decoding.

G. Wang, C. Liu, Y. Dong, P. Han, H. Pan, and B. Fang, "Decrypt: A multi-user searchable symmetric encryption scheme for cloud applications," : Available Encryption (SE) has been broadly examined by both insightful and industry-trained professionals. While various academic SE plans show provable security, they by and large reveal some request information (e.g., search and access plans) to achieve high adequacy. However, some induction attacks have utilized this spillage, such as a question recuperation attack, which can change obscure inquiry secret entryways into their comparing catchphrases based on some prior information. On the other hand, many proposed SE plans require gigantic differences in existing applications, which makes them less sensible, weak in usability, and difficult to send. Available Encryption (SE) has been broadly examined by both insightful and industry-trained professionals. While various academic SE plans show provable security, they by and large reveal some request information (e.g., search and access plans) to achieve high adequacy. However, some induction attacks have utilized this spillage, such as a question recuperation attack, which can change obscure inquiry secret entryways into their comparing catchphrases based on some prior information. On the other hand, many proposed SE plans require gigantic differences in existing applications, which makes them less sensible, weak in usability, and difficult to send.

Keeping Xue, Weicheng Chen, Wei Li, Jinan Hong, and Pelini Hong. Consolidating information proprietor side and cloud-side access control for scrambled distributed storage: Despite the promise of distributed computing, people do not completely trust cloud providers to protect important information due to the lack of client-cloud controllability. Information proprietors utilize mixed data rather than plaintexts so they might be ensured that their information is fittingly classified. When encoded records are exchanged with multiple clients, code-based ciphertext cryptography can be used to protect them. However, it is difficult to defend against a wide range of attacks. A side-effect of this was that large numbers of the prior thoughts didn't permit the cloud supplier to assess whether a downloader was equipped for disentangling. Anyone who has access to the distributed storage should have access to these papers. Refusal of administration (DoS) assaults can be sent off by somebody with a pernicious goal who downloads immense informational collections to overpower the cloud's assets. As a result, the payer will bear any costs associated with cloud management. Besides that, cloud suppliers proceed as both the bookkeeper and the installment of resource usage expenses, leaving data proprietors in obscurity. These issues ought to be resolved by developing the ssa public, verifiable, sharable storage system. We suggest a way to protect cloud storage from EDoS attacks and make the most of the assets on this page. In the absence of predetermined plans, the CP-self-assertive access method of ABE is utilized to determine access. Two conventions for various scenarios follow the execution and security investigation.

Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Mama, and Lifei Wei. Auditable σ-time rethought property-based encryption for access control in distributed computing: With its intricate way to deal with access command over scrambled information, strategy trait-based encryption (CP-ABE) is a fascinating decision for distributed computing applications that require elevated degrees of safety. Nonetheless, there are two primary issues with CP-ABE that should be tended to before it very well may be generally utilized in business applications. First and foremost, decryption results in significant pairing costs, which typically increase in proportion to the size of the underlying access policy. Your characteristics put should match the strategy together to have limitless admittance to encode text.

CP-strength With ABE's entrance freedoms (such as pay-as-you-use), you probably won't be able to use real-world applications. This article addresses these issues by recommending a reevaluated, continuous-examination cloud-based ABE. We accept that decoding's tedious matching cycle can be effectively confirmed while its precision can be offloaded to the cloud. Control over who can access information is additionally given. Cloud service providers may impose time restrictions on the access privileges that users have to cloud services. A different worry in forestalling key spillage is integrated into the thought too. The disclosure of a user's decryption key does not make it any easier for a third party to gain access to the cipher texts of a victim. On a key epitome system setting, Rousakis and Waters CP-ABE is used. We use security and rigorous experimental analysis to improve efficiency and scalability.

III. Methodology

Proposed system:

To shield delicate information from being compromised, the most broadly utilized strategy is encryption. Nonetheless, the genuine prerequisite for information the executives can't be completely met by simply encoding information, for example, with AES. In addition, in order to prevent Economic Denial of Sustainability attacks from preventing users from using the service, effective access control over download requests needs to be taken into consideration. In this application, we consider the twofold access control, concerning cloud-based limit, as in we plan a control framework over the two-data access and download request without loss of security and efficiency.

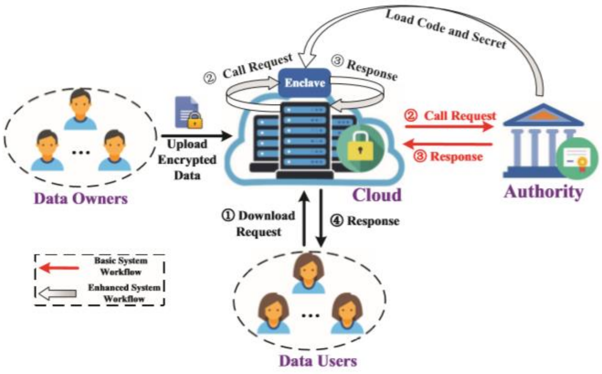


Figure 1: Block diagram of proposed method

IV. Implementation

The project has been implemented using the algorithm listed below.

AES Algorithm: Data is encrypted with round keys. The data to be encrypted, which is stored in an array of data, is the subject of these and other processes. This array is given the name "State." Using AES, you can encrypt a block with 128 bits using the following steps:

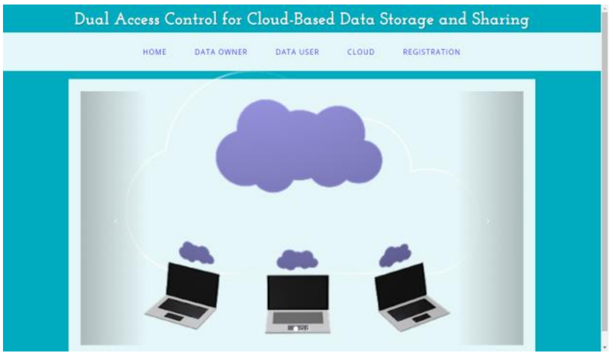
- Derivation of a collection of round keys from a cypher key is required.
- Block data is used to initialize the state array (plaintext).
- Create a new beginning state array with the initial round key.
- It is recommended to do nine rounds of state modification.
- Last but not least, do the eleventh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

A 128-bit sequence is all that is required to encrypt a block. Before we can use AES, we must first convert the 128 bits into 16 bytes. However, in reality, it has probably already been saved in this manner, so "converting" is unnecessary. RSN/AES operations are carried out using a two-dimensional byte array with four rows and four columns. When you start the encryption.

V. Results and Discussion

Home page:

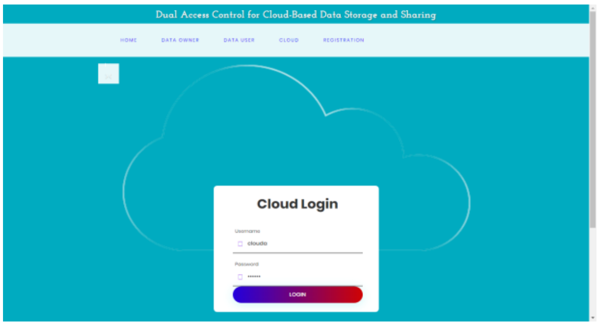
Dual Access for Cloud Based Data Storage has a home page that gives potential customers an overview of the service and its features.


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
DATA OWNER
DATA USER
CLOUD
REGISTRATION

Cloud A

login page:

Cloud A can login with their valid credentials.

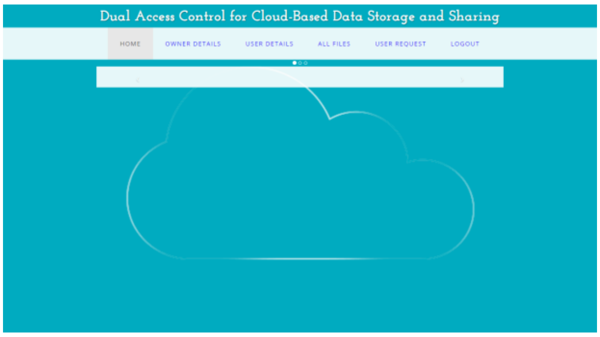

Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
DATA OWNER
DATA USER
CLOUD
REGISTRATION
Cloud Login
LOGIN

Username: cloudo

Password: ******

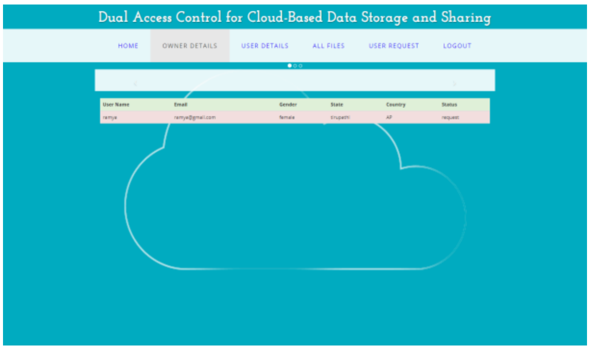
Cloud A

home page:


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
OWNER DETAILS
USER DETAILS
ALL FILES
USER REQUEST
LOGOUT

Owner Details:

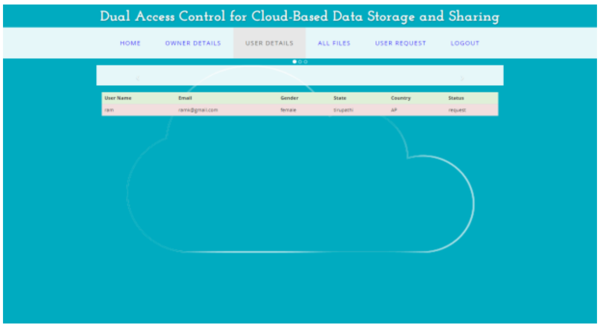
Cloud A can view all the data owner details.


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
OWNER DETAILS
USER DETAILS
ALL FILES
USER REQUEST
LOGOUT

User Name	Email	Gender	State	Country	Status
ramya	ramya@gmail.com	female	tirupathi	AP	request

User Details:

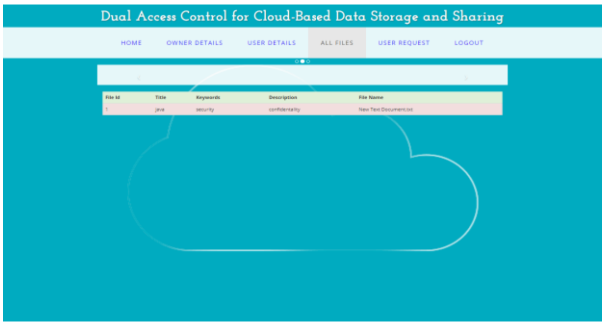
Cloud A can view all the User details.


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
OWNER DETAILS
USER DETAILS
ALL FILES
USER REQUEST
LOGOUT

User Name	Email	Gender	State	Country	Status
ram	ramk@gmail.com	female	tirupathi	AP	request

All Files:

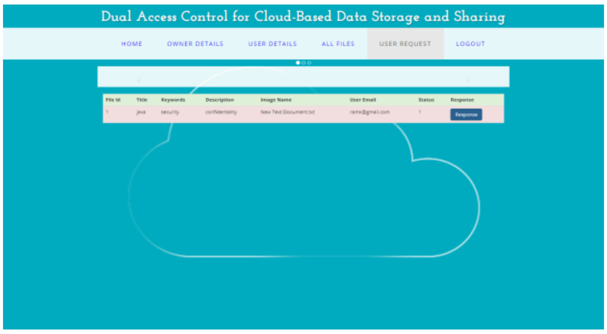
Cloud A can view all the files uploaded by owner.


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
OWNER DETAILS
USER DETAILS
ALL FILES
USER REQUEST
LOGOUT

File Id	Title	Keywords	Description	File Name
1	java	security	confidentality	New Text Document.txt

User Request:

Cloud A can view the user request and can give response to them.

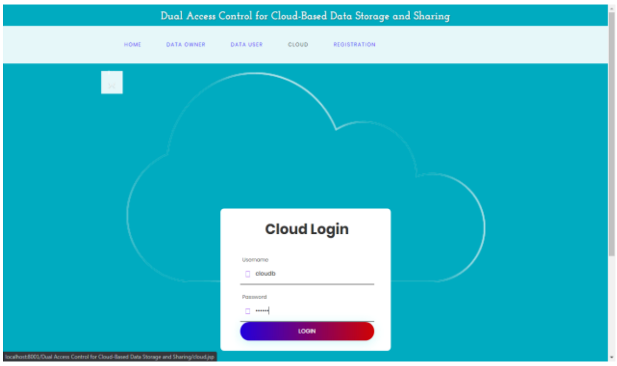

Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
OWNER DETAILS
USER DETAILS
ALL FILES
USER REQUEST
LOGOUT

File Id	Title	Keywords	Description	Image Name	User Email	Status	Response
1	java	security	confidentality	New Text Document.txt	ramk@gmail.com	1	Response

Cloud B

login page:

Cloud B can login with their valid credentials.


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
DATA OWNER
DATA USER
CLOUD
REGISTRATION
Cloud Login
LOGIN

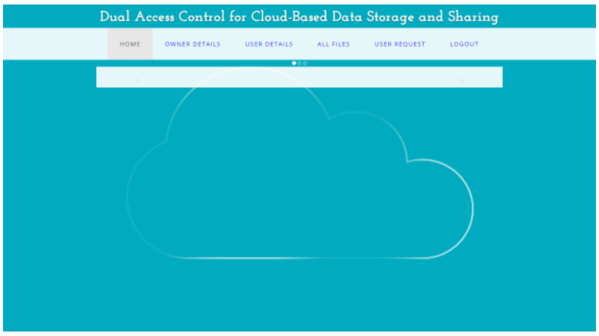
Username
cloudb

Password
••••••

localhost:8001/Dual Access Control for Cloud-Based Data Storage and Sharing/cloud.jsp

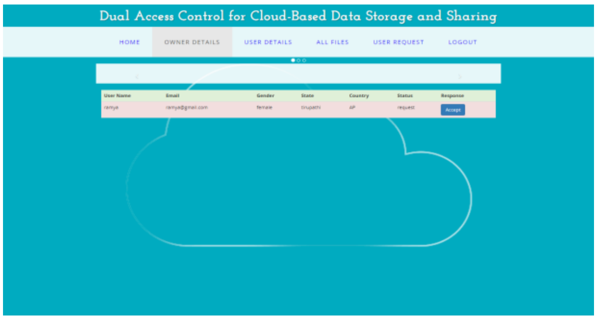
Cloud B home page:

A security of dual access for cloud-based data storage with B cloud.


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
OWNER DETAILS
USER DETAILS
ALL FILES
USER REQUEST
LOGOUT

Owner details:

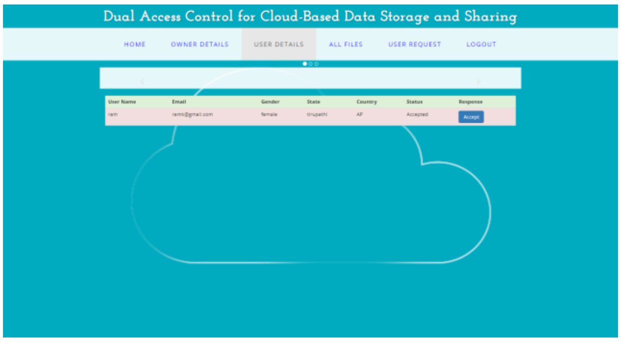
Cloud B can view all the data owner details and they can accept such that data owner can only login.


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
OWNER DETAILS
USER DETAILS
ALL FILES
USER REQUEST
LOGOUT

User Name	Email	Gender	State	Country	Status	Response
ramya	ramya@gmail.com	female	tirupathi	AP	request	Accept

User details:

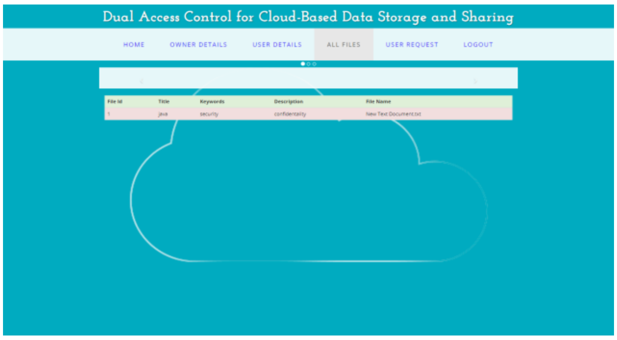
Cloud B can view all the User details and they can accept such that data user can only login.


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
OWNER DETAILS
USER DETAILS
ALL FILES
USER REQUEST
LOGOUT

User Name	Email	Gender	State	Country	Status	Response
ram	ramk@gmail.com	female	tirupathi	AP	Accepted	Accept

All files:

Cloud B can view all the files uploaded by owner.

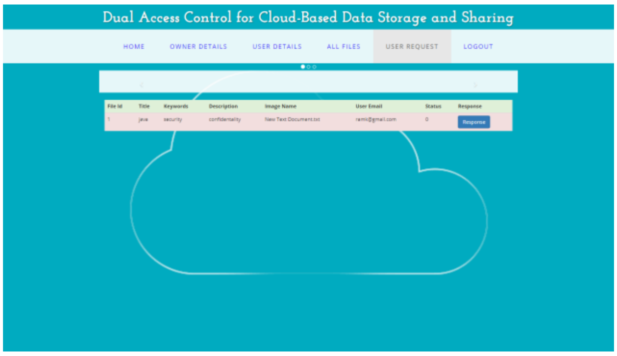


Dual Access Control for Cloud-Based Data Storage and Sharing

File Id	Title	Keywords	Description	File Name
1	java	security	confidentality	New Text Document.txt

User request:

Cloud B can view the user request and can give response to them.

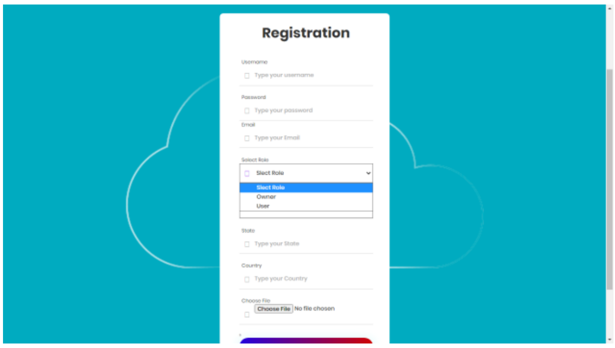


Dual Access Control for Cloud-Based Data Storage and Sharing

File Id	Title	Keywords	Description	Image Name	User Email	Status	Response
1	java	security	confidentality	New Text Document.txt	ramk@gmail.com	0	Response

Registration page:

Data user can register by entering valid details.



Registration

Usernome
□ Type your username

Password
□ Type your password

Email
□ Type your Email

Select Role
□ Slect Role
Slect Role
Owner
User

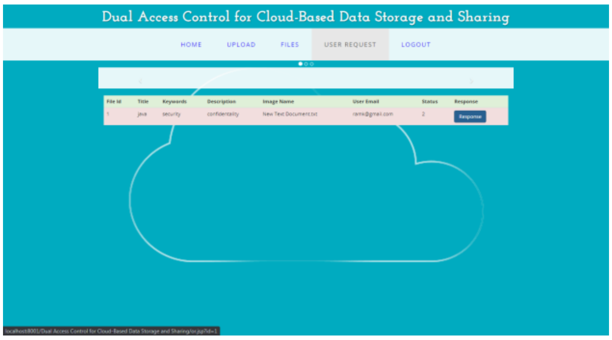
State
□ Type your State

Country
□ Type your Country

Choose File
□ Choose File No file chosen

Data owner login page:

Data user can login with their valid credentials.



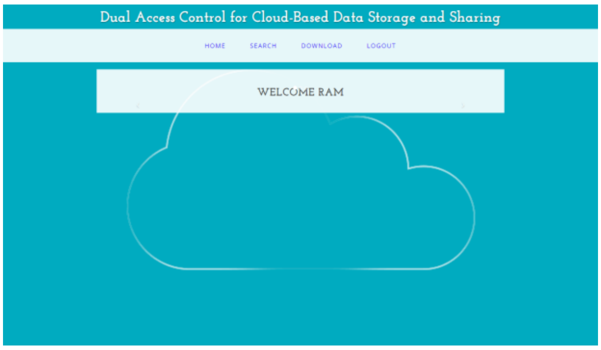
Dual Access Control for Cloud-Based Data Storage and Sharing

File Id	Title	Keywords	Description	Image Name	User Email	Status	Response
1	java	security	confidentality	New Text Document.txt	ramk@gmail.com	2	Response

localhost:8001/Dual Access Control for Cloud-Based Data Storage and Sharing/or.jsp?id=1

User home page:

A home page for Dual Access, a cloud-based data storage service designed for users like you

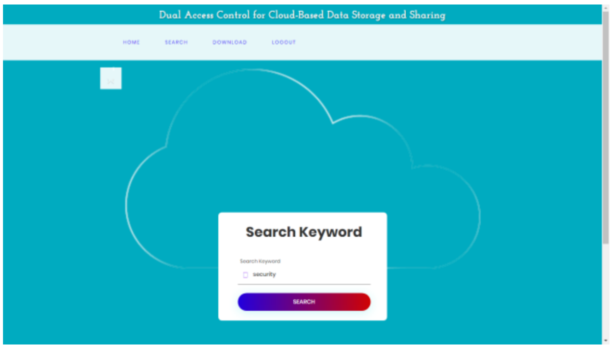


Dual Access Control for Cloud-Based Data Storage and Sharing

WELCOME RAM

Search:

By entering a keyword, the data user can search for a file and send a request to the owner to download it.



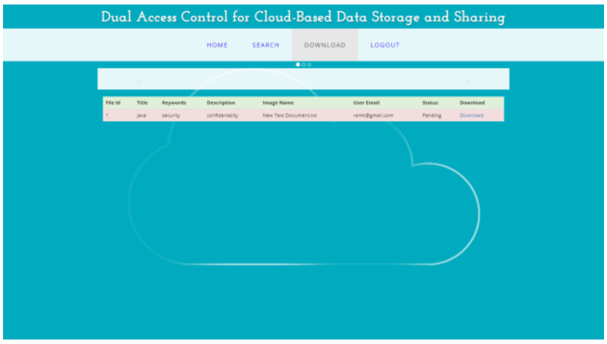
Dual Access Control for Cloud-Based Data Storage and Sharing

Search Keyword

Search Keyword
□ security

Download: pending

A connection to double access for cloud-based information capacity, commonly implies that the download demand is in the works but has not yet begun or is sitting tight for accessible assets.

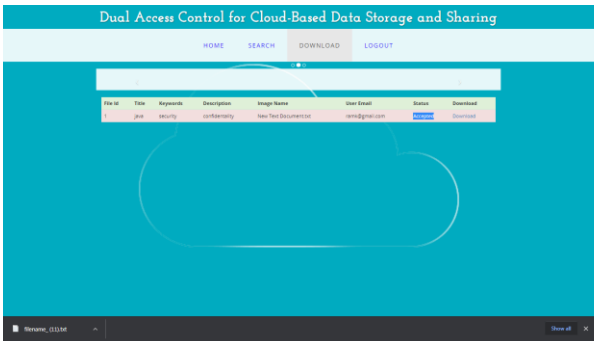


Dual Access Control for Cloud-Based Data Storage and Sharing

File Id	Title	Keywords	Description	Image Name	User Email	Status	Download
1	java	security	confidentiality	New Text Document.txt	ramk@gmail.com	Pending	Download

Download file:

If data owner accepted the request, data user can download that particular file.


Dual Access Control for Cloud-Based Data Storage and Sharing
HOME
SEARCH
DOWNLOAD
LOGOUT
filename_(11).txt
Show all

File Id	Title	Keywords	Description	Image Name	User Email	Status	Download
1	java	security	confidentiality	New Text Document.txt	ramk@gmail.com	Accepted	Download

VI. CONCLUSION

Here, We discussed an intriguing and common problem with cloud-based data sharing and demonstrated two dual access control systems. DDoS/EDoS attacks can't be utilized against the proposed frameworks. We assert that the approach used to provide control over the download request feature is "transplantable" to different CP-ABE designs. Based on our experiments, we can conclude that neither the computational nor communication overhead of the suggested methods significantly affects the control of the download request. No huge computational and correspondence above was found in our trials (contrasted with its fundamental CP-ABE building block). Our system makes use of enclaves, which are used to keep secret information from being accessed. Territories might uncover part of their mysteries to a threatening host through memory access designs or other comparable side-channel attacks, as indicated by new examination. It is consequently important to propose the idea of straightforward territory execution (TEE). This is a fascinating issue: developing a transparent enclave-based dual access control mechanism for AWS cloud data sharing In the future, we will investigate the problem's solution.

VII. REFERENCES

[1]. Matthew W Pagano, Michael Rushanan, Aviel D Rubin, Christina Garman, Ian Miers, Joseph A Akinyele, and Matthew Green Charm: a method for quickly creating prototypes of cryptosystems, Diary of Cryptographic Designing, 3(2), pp. 111-118, 2013.

[2]. A cutting-edge method of CPU-based attestation and sealing is presented by Shay Gueron, Simon Johnson, Vincent Scarlata, and Ittai Anati in Volume 13, page 7 of the Workshop on Hardware and Architectural Support for Security and Privacy (HASP) 2013: New York, NY, USA: ACM

[3]. The current family of Antonis Michalas and Alexandros Bakas: A quality-based, symmetric accessible, and SGX-based crossover encryption strategy that can be changed. In the 2019 edition of Secure COMM, pages 472-486.

[4]. Srinivas Devadas and Victor Costain Intel sgx got a handle on it. IACR Cryptology ePrint Archive, 2016(086):1–118

[5]. Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov IRON: SGX-based encryption that works with Intel. CCS 2017, pages 765-782, in Procedures of the 2017 ACM SIGSAC Gathering on PC and Correspondences Security.

[6]. Tatsuaki Okamoto and Eiichiro Fujisaki Secure blend of hilter kilter and symmetric encryption plans. Advances in Cryptology-CRYPTO 1999, pages 537–554. 1999, Springer.

[7]. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. attribute-based encryption for fine-grained control over data access. ACM, 2006, pages 89-98 of ACM CCS 2006.

[8]. Enhancing the privacy and security of decentralized ciphertext-policy attribute-based encryption with Willy Susilo, Yi Mu, Jianying Zhou, Man Ho Allen Au, and Jinguang Han. Pages 665–678 of Volume 10, Issue 3 of IEEE Transactions on Information Forensics and Security, 2015.

[9]. Imprint Tannian, Joseph Idziorek, and Doug Jacobson's fraudulent attribution of cloud

resource consumption. IEEE, 2012, pages 99-106 of IEEE CLOUD 2012.

[10]. Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksfoabe: for cloud storage, outsourced attribute-based encryption with a keyword search function. 10(5):715–725, IEEE Transactions on Services Computing, 2017.

Cite this article as :

N. Sai Varsha, B. Triveni, "Cloud-Based Data Storage and Sharing with Dual Access Control", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 3, pp. 1126-1134, May-June 2023.
Journal URL : https://ijsrst.com/IJSRST523103186