ZKG INTERNATIONAL ISSN: 2366-1313

DUAL ACCESS CONTROL MECHANISM FOR SECURE DATA STORAGE AND SHARING IN THE CLOUD

[#1]KOMIRE SANJANA,
[#2]GANDRA VISHWANTH,
[#3]V. MAMATHA, *Assistant Professor,*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Cloud-based data storage has recently gotten a lot of attention from both businesses and academics. This is because it is easy to handle and doesn't cost much. Service providers need to make sure they share and store data in a way that doesn't compromise user privacy or data security because their services are delivered over an open network. Encryption is the most common way to keep private information safe from being stolen. On the other hand, data protection (like using AES) is not enough to meet all the needs of data management. To stop Economic Denial of Sustainability (EDoS) tactics that make it hard for users to use the service, it is also important to have tight access control over download requests. In this piece of writing.In the setting of cloud-based storage, dual access control is used to make sure that download requests and data access are controlled in a way that ensures the best performance and security. A single dual access control system is the subject of this study. It is meant for two different areas. It also talks about a security and experimental check of the devices. Two-level access control keeps cloud storage and exchange of data safe.

KEYWORDS: Dual access, Data Sharing, Storage, Data management

1.INTRODUCTION

Cloud-based storage systems have piqued the curiosity of corporate and educational leaders in recent decades. Because it has so many advantages, such as flexible access and no need for local data management, it may be found in a variety of Internet-based business solutions, such as Apple iCloud. Nowadays, an increasing number of individuals and businesses prefer to transfer their data to a remote cloud rather than update their personal information governance infrastructure and technology.

However, the biggest barrier to using cloud-based storage services for Internet users may be their concerns about potential security flaws involved with transmitting data to an external source. Information that was outsourced may need to be discussed with others in a number of real-world situations. In this case, Alice, a Dropbox user, might email images to her friends. To share the images with her friends without encrypting the data, Alice must generate a sharing link and send it to them. At the Dropbox organizational level, the sharing link may be visible, even if it claims to give you some control over unwanted users (for example, those who aren't Alice's friends).

Because it is based on an open network, the cloud is not entirely secure. Encrypting data before sending it to the cloud is generally recommended to ensure data security and privacy.

One solution to this problem is to secure the outsourced data directly (with AES, for example) before sending it to the cloud. In this way, the data can only be decrypted by a specific cloud user with a valid decryption key. One simple method for preventing "insiders" from viewing shared photographs is to provide access to the material before posting it for the set of people who have permission to see it. Alice may not always know who

will see or use the photographs. Alice may only be aware of credits for picture readers. Paillier Encryption and other basic public key encryption cannot be utilized in this case since the person encrypting the content must know who will get it beforehand. As a result, having a policy-based encryption solution for outsourced images would be advantageous. In this way, Alice can use the system to restrict who can view the encrypted photos—only approved users. Resource fatigue is a well-known problem that regularly affects cloud-based storage services. Malicious users may use denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks to overload the cloud storage service server with requests, preventing it from responding to valid service requests. This is due to the risk that a public cloud will be unable to restrict download requests, allowing a service user to submit an infinite number of download requests to the cloud server. Under the "pay-as-you-go" method, rising resource use may lead to financial troubles. Clients of cloud management will pay much more as the attacks worsen. Economic Denial of Sustainability (EDoS) attacks target cloud users' financial resources. To begin with, downloading anything endlessly could be costly for you. Furthermore, it may allow network attackers to examine corrupted download data, resulting in data loss (for example, file sizes). In this regard, it is vital to efficiently manage the demand for downloading stolen or encoded data. In this paper, we propose a unique solution called dual access control to overcome the two difficulties described earlier. Attribute-based encryption (ABE) is one method for protecting data in a cloud storage service.

It allows you to have fine-grained control on leased data while maintaining its secrecy. Ciphertext-Policy ABE (CP-ABE) [5] is a useful way of encrypting data since it allows access policies to be established over encrypted data and notifies possible data recipients of their rights of access. Remember that the technique used in this paper takes CP-ABE into account. For example, creating a terrific tool that can control both download demand and data access involves more than simply the CP-ABE technique.

A hypothetical solution to the download control problem would be to validate the data receiver's decoding privileges with bogus ciphertexts. Alice, the data owner, must upload multiple "testing" ciphertexts to the cloud alongside the "real" encryption of the data. "Testing" ciphertexts are encrypted copies of fictitious messages that can be accessed in the same way that "real" data is. An ISSN:0377-9254 user, Bob, makes Cloud a download request, and Cloud demands that Bob randomly decrypt one of the "testing" ciphertexts. Bob has the right to analyze the "real" data because Alice gave him permission to do so.

If he decrypts the data or receives the correct answer, he can retrieve the ciphertext from the cloud. However, there are certain drawbacks with this approach: Alice, the data owner, must first encrypt a few false ciphertexts with the same method as the "real" ciphertext. This may make Alice's computations significantly more complicated, which could be a problem in the real world. If Alice just wants to transfer one photo from her phone to iCloud, she will need to generate several ciphertexts. Second, all ciphertexts, even bogus ones, are sent to the cloud simultaneously. However, some people may be unaffected if their mobile network uses a pay-as-you-go plan or an earlier kind of internet technology (such as 3G). Furthermore, this slows data transfers and increases the bandwidth that the network must use. Third, to ensure that his download request is valid, Bob, as a user and data recipient, must decipher a random "testing" ciphertext from the cloud. Therefore, in order to access the "real" information, Sway must "pay" twice as much (the decoder cost), which may not be practical in a circumstance where assets are required. This leads to the following question being asked in this paper: Is it possible to use cloud computing in a way that maximizes efficiency and security while restricting download requests and data access?

2. LITERATURE SURVEY

DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party
AUTHORS: Ali, M., Malik, S. and Khan, S.,

Off-site information capacity is a cloud-based service that manages information capacity configurations for clients. However, sharing routine data with a third party significantly increases security risks. Attacks by various clients and systems in the cloud could result in information leaks. Another issue being addressed in the cloud environment is the discounting of information by cloud-specialized firms. As a result, additional safety measures must be implemented. The study recommends a data security method called Data Security for Cloud Environments with Semi-Trusted Third Parties (DaSCE). It can securely delete data, manage keys, and regulate who has access to them. The DaSCE handles keys using Shamir's (k, n) threshold technique. To create a key, k shares out of n are required. We employ numerous key managers, each with a single key share. Having more than one key manager protects encryption keys from a single point of failure. We (a) use the Satisfiability Modulo Theories Library (SMT-Lib) and the Z3 solver to ensure that DaSCE works; (b) codify and examine DaSCE's work using High Level Petri nets (HLPN); and (c) grade its performance by examining how long various procedures take. The results show that key management, access control, and file assured erasure are among the DaSCE features that can be utilized to protect outsourced data.

Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption
AUTHORS: Jung, T., Li, X. Y., Wan, Z. and Wan, M

Some cloud services keep data, causing privacy problems. However, cloud computing is a breakthrough approach to computer use that allows you to use resources in a flexible, on-demand, and cost-effective manner. Several solutions based on attribute-based encryption have been proposed to protect cloud storage. However, most initiatives prioritize privacy and control over access to data content over identity and privileges. AnonyControl is a semi-anonymous privilege control system presented in this paper to address the privacy concerns that current access control methods have with user identities and data. AnonyControl distributes authority so that names do not leak out, making things partially anonymous. It also incorporates privilege control with file access control, allowing you to manage privileges finely across all cloud data operations. Then we show you the AnonyControlF, which provides perfect privacy and prevents your name from being disclosed. Our performance analysis demonstrates that our schemes operate, and our security study reveals that AnonyControl and AnonyControl-F are secure under the DBDH assumption.

3.PROPOSED SYSTEM

In this paper, we propose a new mechanism known as "dual access control" to address the two concerns listed above. Attribute-based encryption (ABE) is an effective method for protecting data in cloud-based storage systems. This sort of encryption keeps data secure and allows you to manage it in a very specific way. Ciphertext-Policy ABE (CP-ABE) [5] is an excellent method for encrypting data because it allows you to specify access rules that instruct potential data receivers what they can and cannot do with the encrypted data. We discuss how CP-ABE is used in our mechanism in this paper. The CP-ABE approach, on the other hand, is insufficient to create a beautiful system that manages both data access and download requests.

IMPLEMENTATION

DATA OWNER:

In this case, getting permission and setting up an account with the cloud provider are the responsibilities of the data owner. Authorization from the cloud is a prerequisite for the data owner to upload a file to a cloud server. The master secret key and content key for the file must be obtained by the data owner before they can access

ISSN: 2366-1313

sensitive information. The owner will have access to compression once the file has been added. It is necessary to generate the keys before uploading the file to the cloud service. Every file that has been posted must have search and download privileges granted by the data owner in order for users to be able to access and download the data.

CLOUD SERVER

A server must be in control of the cloud for it to operate and store data. Data owners make sure their files are safe before uploading them to the cloud so that cloud users can access them. Users must create an MSK master secret key and a content key before being allowed to view shared data files. Permission will be granted by the cloud.It additionally shows each exchange and attack related to the files.

AUTHORITY

The authority creates both the secret key and the content key that the end user requires. The authority can view any file thanks to the content key and master secret key, which are created using the data owner's information.

END USER

The user needs to register and authenticate before they can access data that is saved on the cloud. The cloud has given the user authorization to confirm the registration. To access the file, one must request both the MSK master secret key and the content key. Any file can only be accessed and inspected with permission from the data owner.

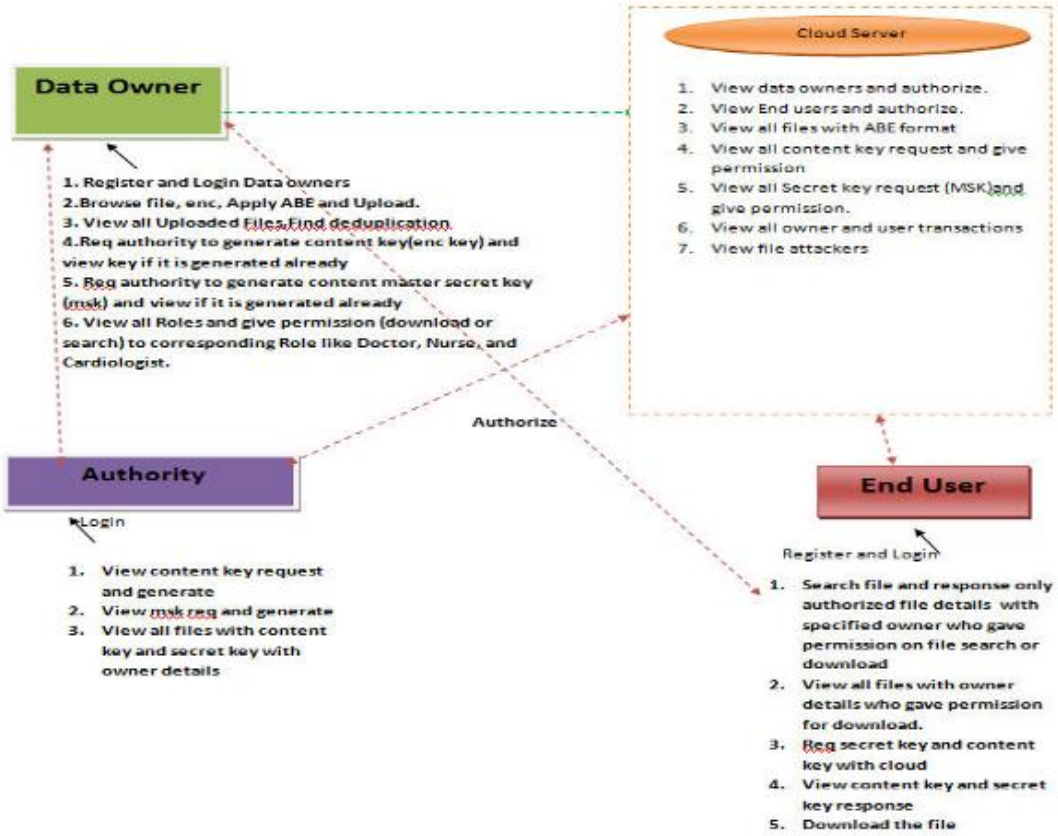

Fig 1: Architecture

4.RESULTS AND DISCUSSION

ISSN: 2366-1313

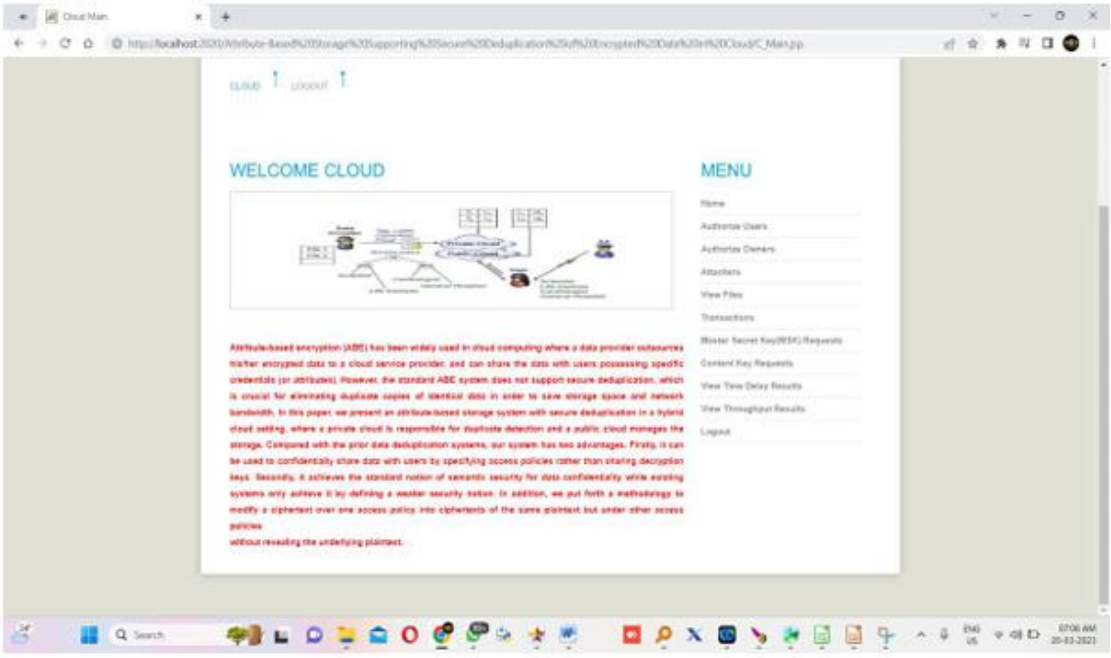

Fig 2: Cloud Main Page

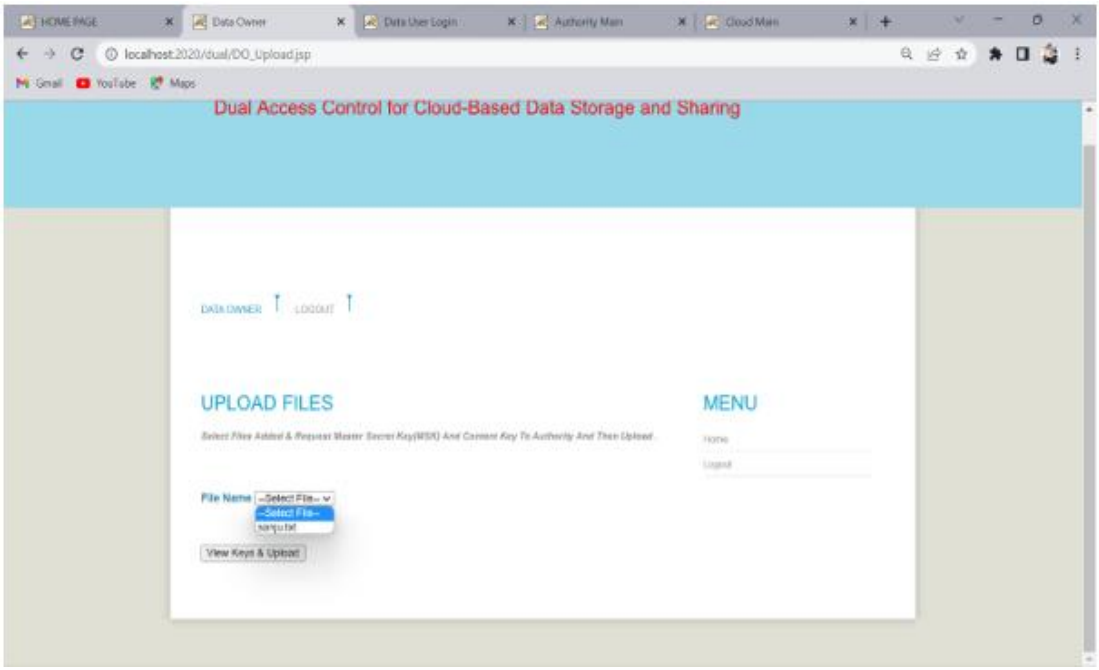

Fig 3: Uploading file to cloud

ISSN: 2366-1313

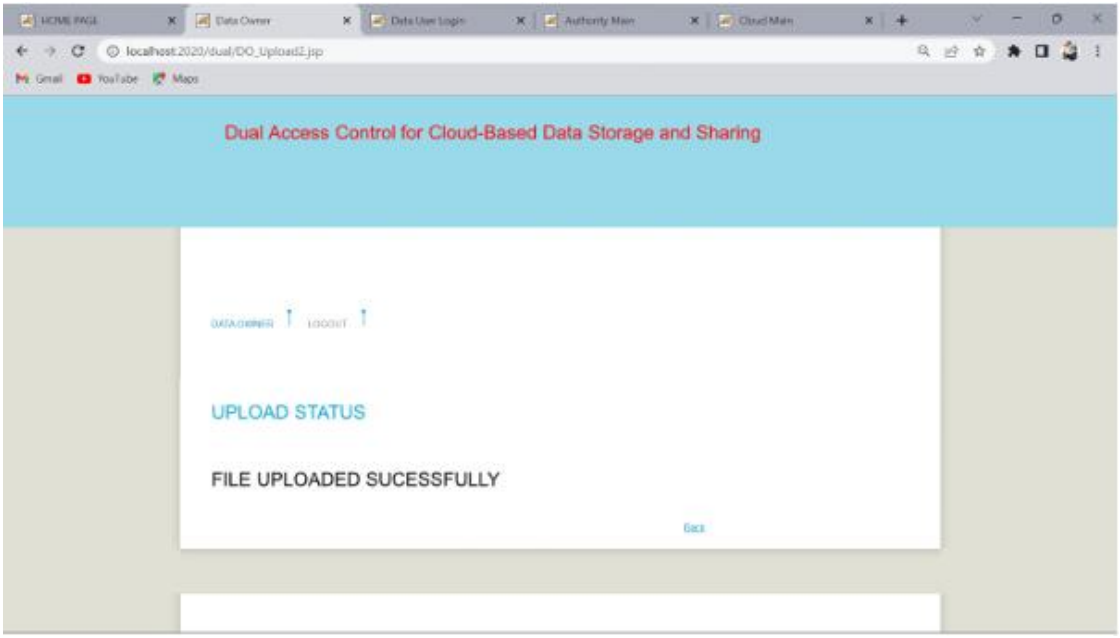

Fig 4: File uploaded successfully

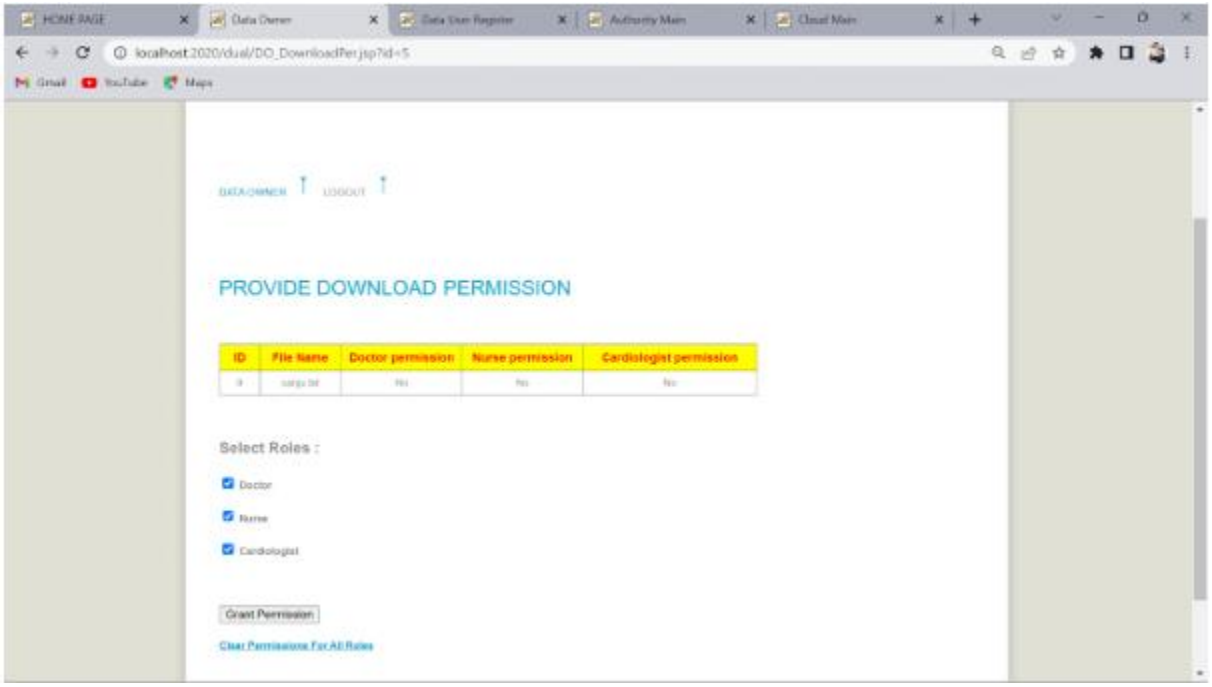

Fig 6: Giving permission to end users

ISSN: 2366-1313

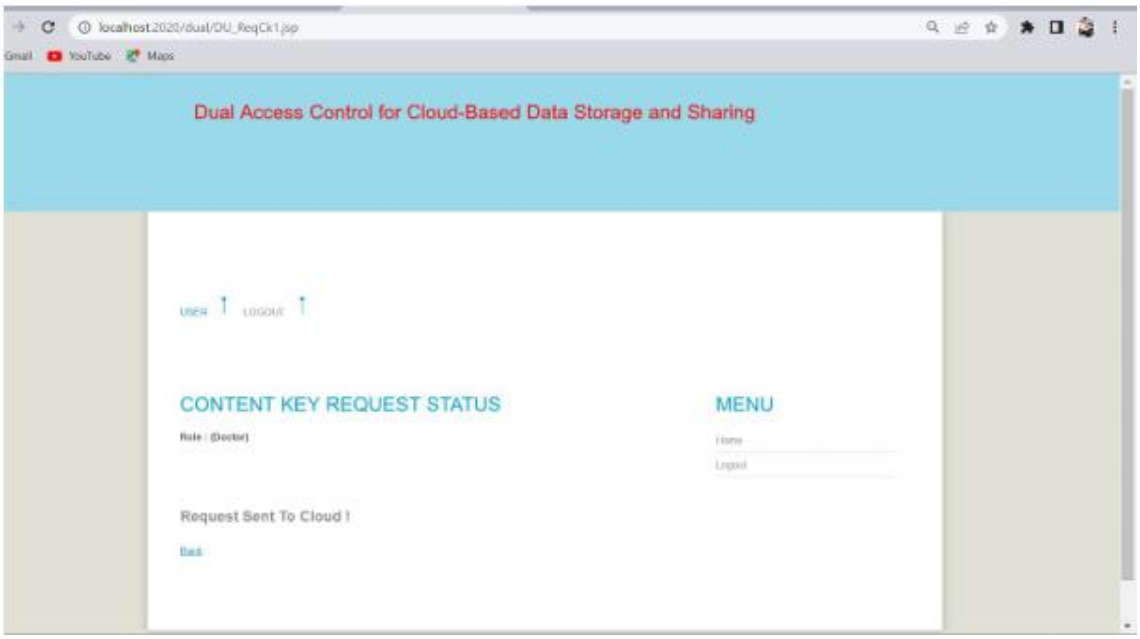

Fig 7: User requesting MSK and Content key

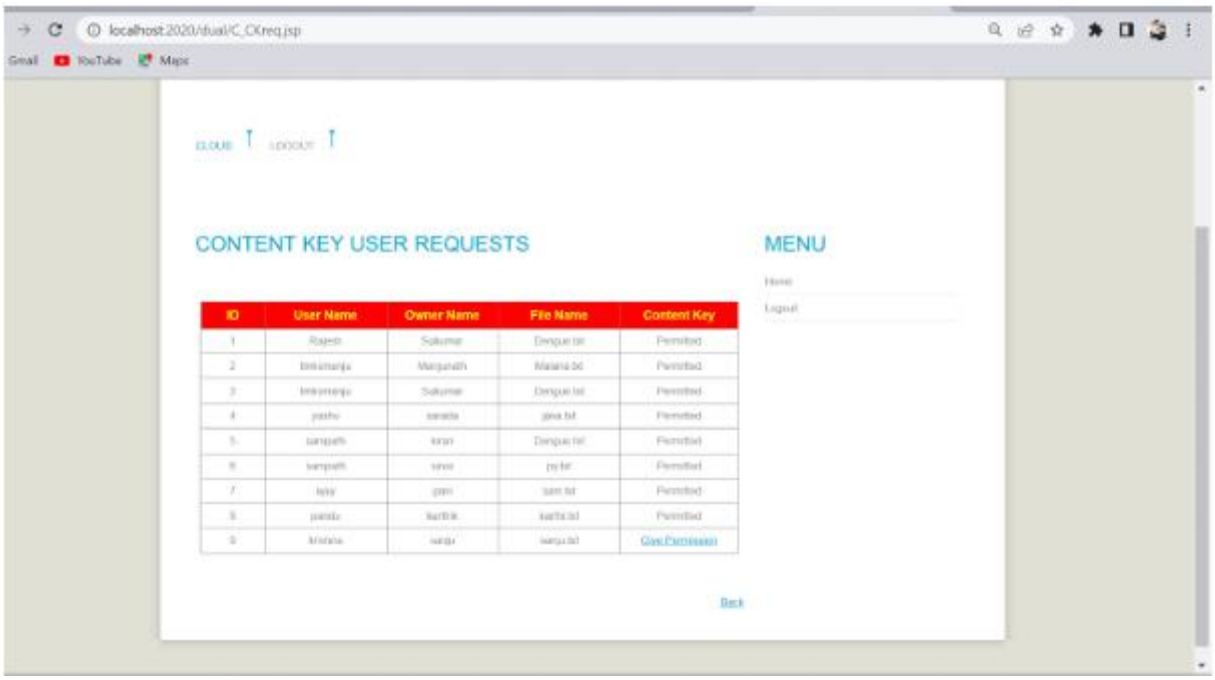

Fig 8: Cloud giving response to request for keys by the users

ISSN: 2366-1313

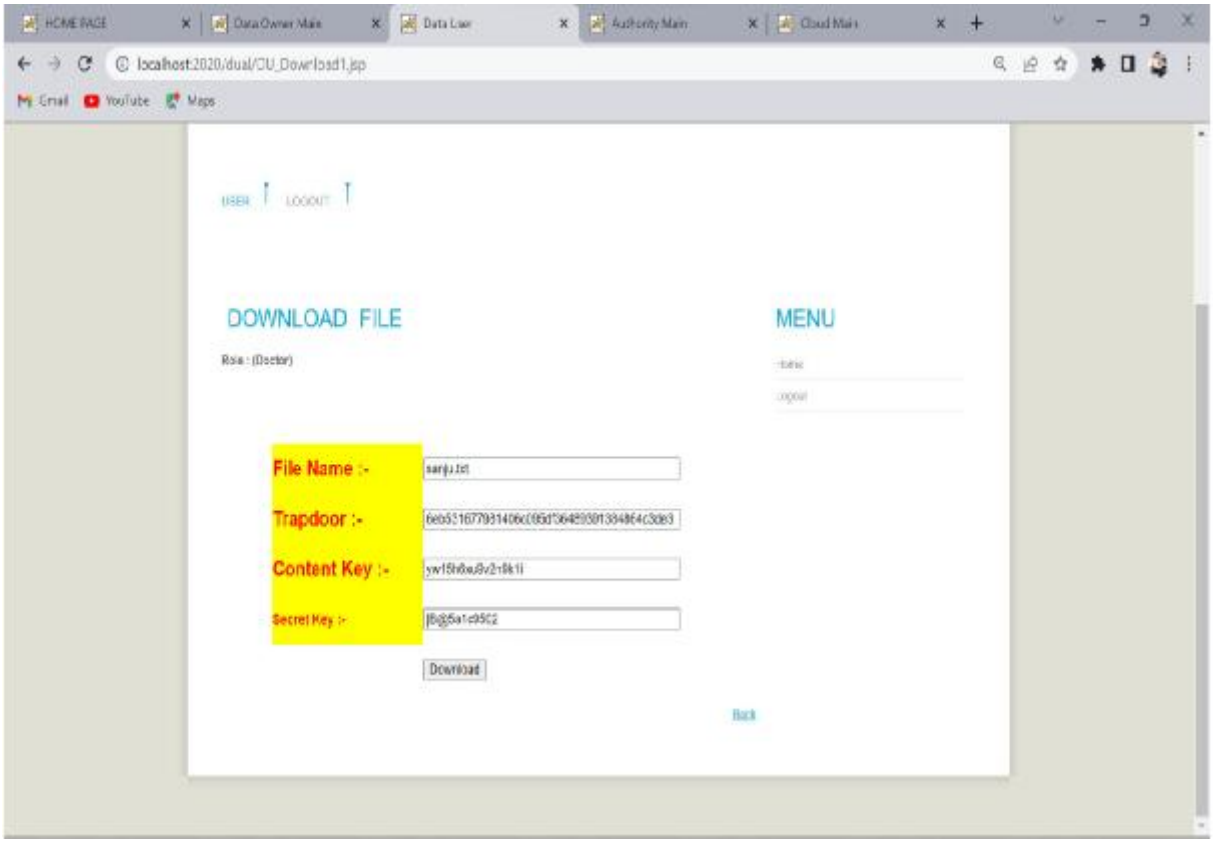

Fig 9: user downloading the file

5.CONCLUSION

Two different types of access control have been created to deal with an interesting problem that keeps coming up when people share data in the cloud. DDoS and EDoS attacks can't hurt the systems that were proposed. "Transplantable" to other CP-ABE architectures is what we say about the method used to make the download request control function. The results of the experiments show that the systems being studied don't have nearly as many problems with computation or transfer as the main CP-ABE component.

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. Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
5. JohnBethencourt,AmitSahai,andBrentWaters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE, 2007.

ISSN: 2366-1313

6. Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.
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. Eiichiro Okamoto. Fujisaki Secure and Tatsuaki integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology CRYPTO 1999, pages 537–554. Springer, 1999.
9. 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.
10. 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 10(3):665–678, 2015.