Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

Attribute-Based Storage in the Cloud Enables Secure Deduplication of Encrypted Data

Mrs MARESWARAMMA P Assistant Professor in the DVR & Dr HS MIC college of Technology kanchikacherla NTR District.

Mr.Seelam Gopi Narendar Reddy MCA student in the Department of Computer Applications at DVR & Dr HS MIC College of Technology(Autonomous), Kanchikacherla, NTR District.

ABSTRACT_ Cloud is an important source of data storage that can be maintained, managed and backed up via remotely anytime. These cloud services not only provide easy access but also protects user's data to a greater extent from the third party. Due to rise of 'Big Data', Cloud computing has become one of the most significant and essential rising application platforms to solve the expanding of data exchange. Cloud networks are not so secure, to protect data from exposure, users need to encrypt their data before sharing it to other users. So, to achieve this few terms Attribute-based encryption (ABE) has been widely used in cloud computing where data providers outsource data in encrypted format to cloud and can share the encrypted data with different users possessing specific attributes which will indeed get decrypted using security measures. It allows a user with limited computational resources to outsource their large data processing workloads to the cloud, and economically enjoy the better power, computational bandwidth, storage, and even appropriate software that can be shared in a pay|per|use manner. To the other side, the outsourced computation workloads often contain highly-confidential and sensitive data, such as the proprietary research data, business statistics, or personally identifiable information, university student data records, stock market data etc. To combat against unauthorized data leakage and exposure, this sensitive and confidential data have to be encrypted before outsourcing so as to provide end-to-end data confidentiality assurance in the cloud and beyond that. However, ordinary data encryption techniques, in essence, prevent the cloud from performing any meaningful operation of the underlying ciphertext policy, making the computation over encrypted data a very hard problem for the system. The proposed system achieves scalability due to its hierarchical structure as well as efficiency and easiness of data flow in cloud computing.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

1.INTRODUCTION

Cloud computing greatly facilitates data providers who want to outsource their data to the cloud without disclosing their sensitive data to external parties and would like users with certain credentials to be able to access the data. This requires data to be stored in encrypted forms with access control policies such that no one except users with attributes (or credentials) of specific forms can decrypt the encrypted data. An encryption technique that meets this requirement is called attribute-based encryption (ABE), where a user's private key is associated with an attribute set, a message is encrypted under an access policy (or access structure) over a set of attributes, and a user can decrypt a ciphertext with his/her private key if his/her set of attributes satisfies the access policy associated with this ciphertext. However, the standard ABE system fails to achieve secure deduplication, which is a technique to save storage space and network bandwidth by eliminating redundant copies of the encrypted data stored in the cloud. On the other hand, to the best of our knowledge, existing constructions for secure deduplication are not built on attribute-based encryption. Nevertheless, since ABE and secure deduplication have been widely applied in cloud computing, it would be desirable to design a cloud storage system possessing both properties. We consider the following scenario in the design of an attribute-based storage system supporting secure deduplication of encrypted data in the cloud, in which the cloud will not store a file more than once even though it may receive multiple copies of the same file encrypted under different access policies. A data provider, Bob, intends to upload a file M to the cloud, and share M with users having certain credentials. In order to do so, Bob encrypts M under an access policy over a set of attributes, and uploads the corresponding ciphertext to the cloud, such that only users whose sets of attributes satisfying the access policy can decrypt the ciphertext. Later, another data provider, Alice, uploads a ciphertext for the same underlying file M but ascribed to a different access policy ` . Since the file is uploaded in an encrypted form, the cloud is not able to discern that the plaintext corresponding to Alice's ciphertext is the same as that corresponding to Bob's, and will store M twice. Obviously, such duplicated storage wastes storage space and communication bandwidth. We present an attribute-based storage system which employs ciphertextpolicy attribute-based encryption (CP-ABE) and supports

secure deduplication. Our main contributions can be summarized as follows. • Firstly, the system is the first that achieves the standard notion of semantic security for data confidentiality in attribute-based deduplication systems by resorting to the hybrid cloud architecture. • Secondly, we put forth a methodology to modify a ciphertext over one access policy into ciphertexts of the same plaintext but under any other access policies without revealing the underlying plaintext. Thistechnique might be of independent interest in addition to the application in the proposed storage system. • Thirdly, we propose an approach based on two cryptographic primitives, including a zero-knowledge proof of knowledge and a commitment scheme, to achieve data consistency in the system.

2.LITERATURE SURVEY

2.1) 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 use of cloud that assuages the clients from zeroing in on information capacity framework. However, there are serious security concerns associated with outsourcing data to a third-party administrative control. Information spillage might happen because of assaults by different clients and machines in the cloud. Discount of information by cloud specialist organization is one more issue that is looked in the cloud climate. Therefore, elevated degree of safety efforts is required. Data Security for Cloud Environment with Semi-Trusted Third Party (DaSCE) is a data security system we propose in this paper that offers file assured deletion, key management, and access control. To manage the keys, the DaSCE employs Shamir's (k, n) threshold scheme, in which k shares out of n are required to generate the key. We use multiple key managers, each of which stores a single key share. Multiple key managers keep the cryptographic keys safe from a single point of failure. We (a) use the Satisfiability Modulo Theories Library (SMT-Lib) and the Z3 solver to verify the operation of DaSCE, (b) formally model and analyze the working of DaSCE using High Level Petri nets (HLPN), and (c) evaluate its performance based on the amount of time consumed by various operations. Key management, access control, and file assured deletion are all features of DaSCE that can be used

effectively to protect outsourced data, as demonstrated by the findings.

2. 2) Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption

AUTHORS: Jung, T., Li, X. Y., Wan, Z. and Wan, M

Although some cloud servers store data, which raises a number of privacy concerns, cloud computing is a revolutionary computing paradigm that enables flexible, on-demand, and low-cost resource utilization. To protect cloud storage, a number of approaches based on attribute-based encryption have been proposed. However, identity privacy and privilege control receive less attention than data content privacy and access control in most projects. AnonyControl, a semi-anonymous privilege control method, is presented in this paper to address the data privacy and user identity privacy concerns of existing access control methods. To prevent identity leaks, AnonyControl decentralizes authority, resulting in semi-anonymity. In addition, it extends file access control to privilege control, making it possible to fine-tune privilege management for all cloud data operations. Then, we present the AnonyControlF, which achieves complete anonymity and completely prevents identity leakage. Our performance evaluation demonstrates the viability of our schemes, and our security analysis demonstrates that, under the DBDH assumption, both AnonyControl and AnonyControl-F are secure.

3.PROPOSED SYSTEM

This project uses secure deduplication to save storage space for cloud storage services as well. However, several processes have used the same idea for deduplication. However, there are various modules incorporated into this project. In this scenario, the cloud server is able to distinguish the identical ciphertexts and store the file if two users upload the same file. just a single duplicate of them. For security reasons, this procedure has some authentication options available in some issues. through this interaction for guarantee got deduplication. A business owner wishes to transfer data to the cloud and share it with authorized users. The Property Authority gives each client a decoding key related with clients set of qualities. which is thought to be the most significant obstacle for effective and safe cloud storage services in a dynamic ownership environment. Each time a data provider uploads a file checking from the cloud for the purpose of saving space. The

majority of the plans have been proposed to give information encryption, while as yet profiting from a deduplication procedure. each client get gotten key structure administrator for security reason .client might not take at any point any key he can not download chipertext document .they can download just encoded information. Each and every detail is managed and kept up by the attribute authority. Along these lines, any client who downloads the record, after unscrambling, can really look at the rightness of the decoded plaintext by matching it to the comparing tag. To keep the documentation brief, we utilize c to mean the mix of the encoded information and the relating access structure.

3.1 IMPLEMENTATION

DATA OWNER:

In this module, initially the data owner has to register to the cloud server and get authorized. After the authorization from cloud data owner will encrypt and add file to the cloud server where in after the addition of file data owner requests the content key and the master secret key to the authority for the file he uploaded and finds Find deduplication ,only after the keys generated the file is uploaded to the cloud server. After the uploading of the file the data owner will have to provide download and the search permission for individual file for the users to perform search and download.

CLOUD SERVER

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with cloud End users. To access the shared data files users will request the permission of content key and the MSK master secret key. And the cloud will provide the permission .and also views all the transactions and attackers related to the files.

AUTHORITY

Authority generates the content key and the secret key requested by the end user.

Authority can view all files with the content key and master secret key generated with the corresponding data owner details of the particular file.

END USER

User has to register and login for accessing the files in the cloud. User is authorized by the cloud to verify the registration. User has to request for the MSK master secret key and content key to download the file. User can only download and serach the file if the data owner of the particular file has provided the permissions.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

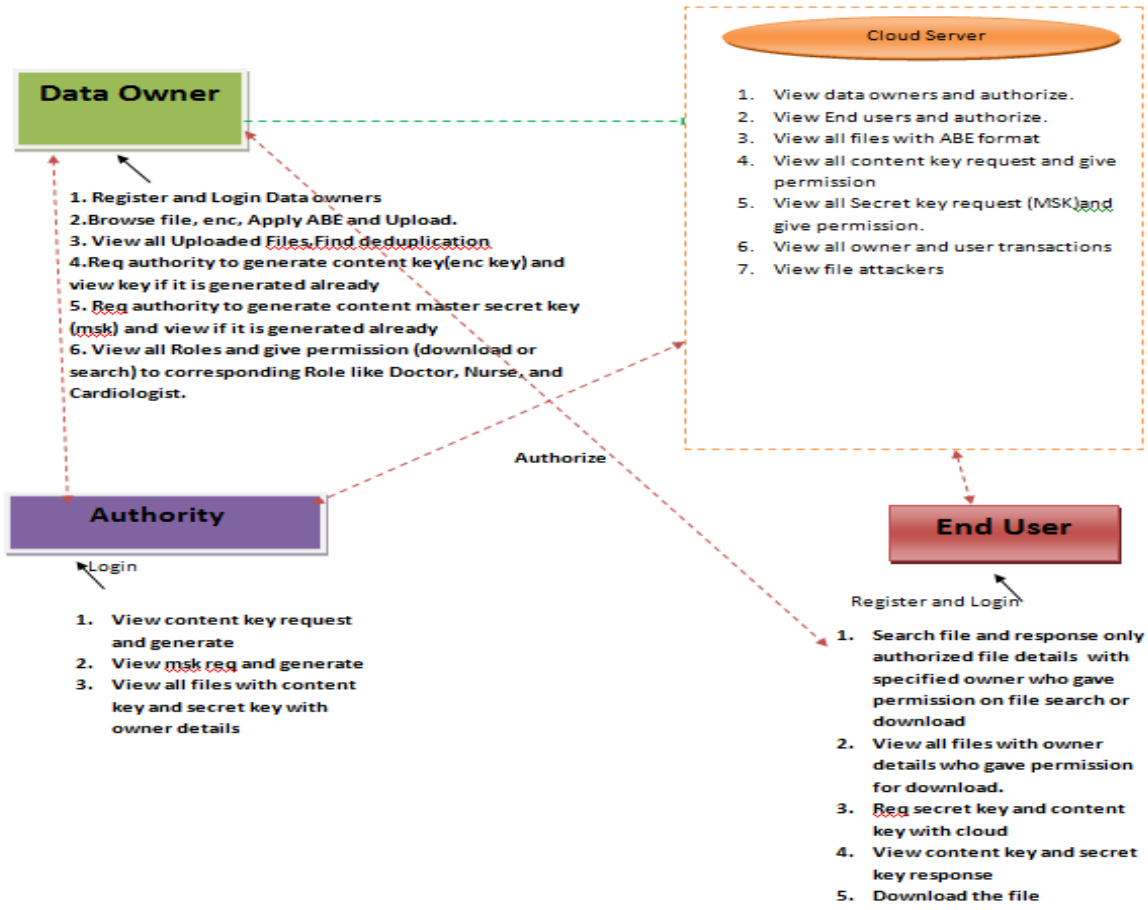

Fig 1: Architecture

4.RESULTS AND DISCUSSION

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

Fig 2: Cloud Main Page

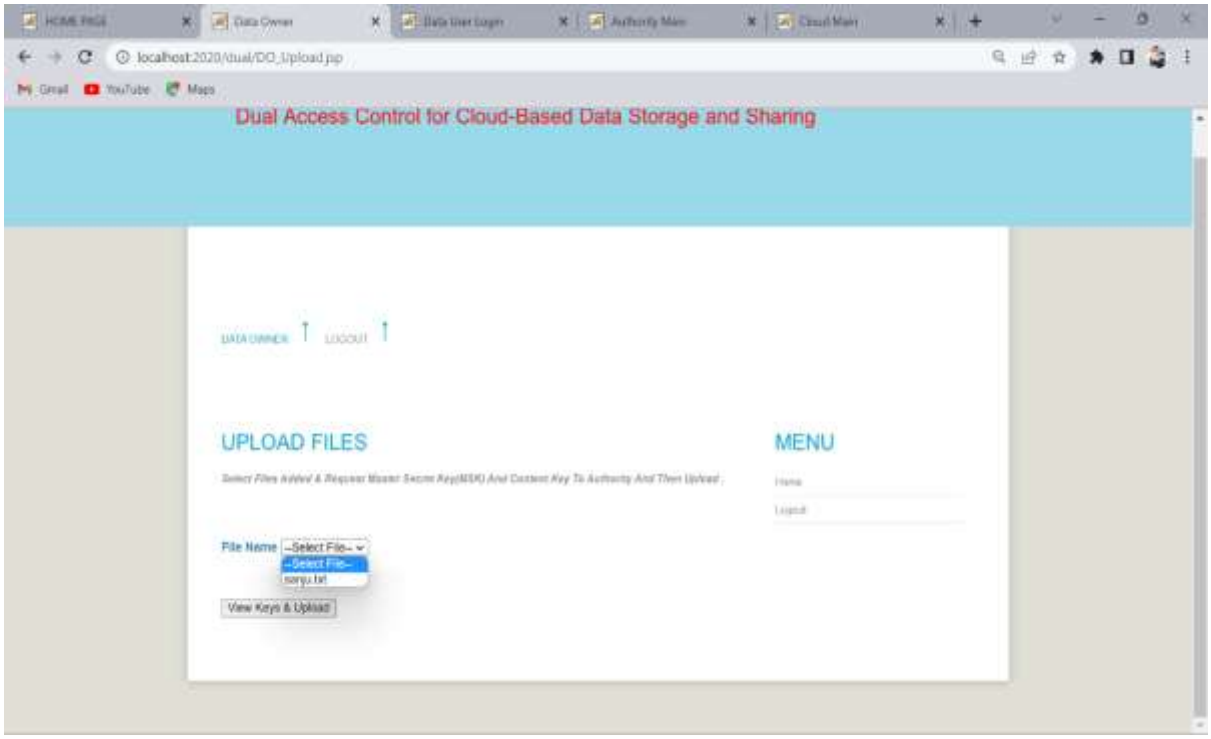

Fig 3: Uploading file to cloud

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

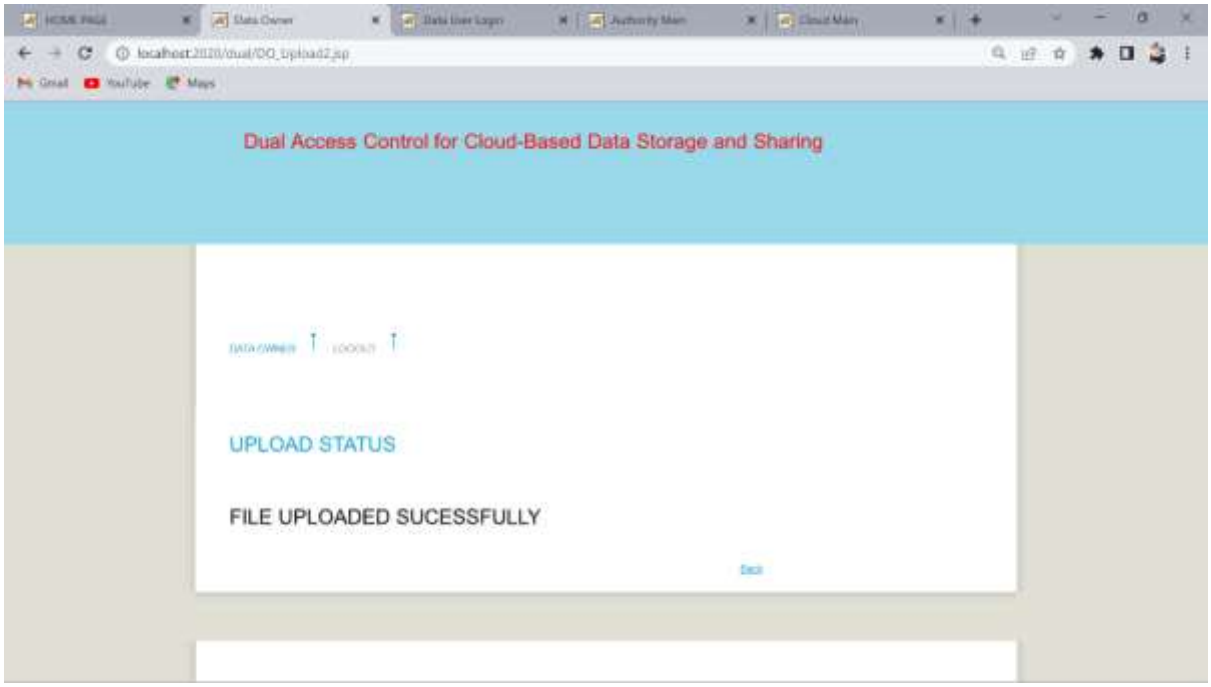

Fig 4: File uploaded successfully

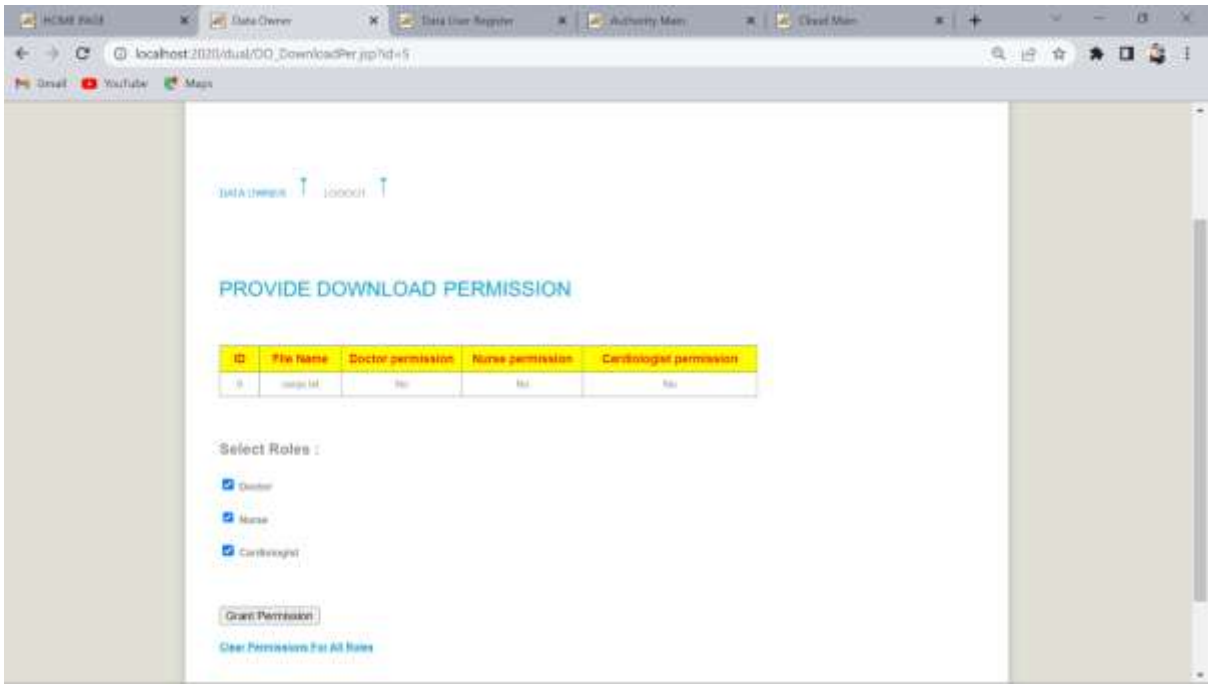

Fig 6: Giving permission to end users

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

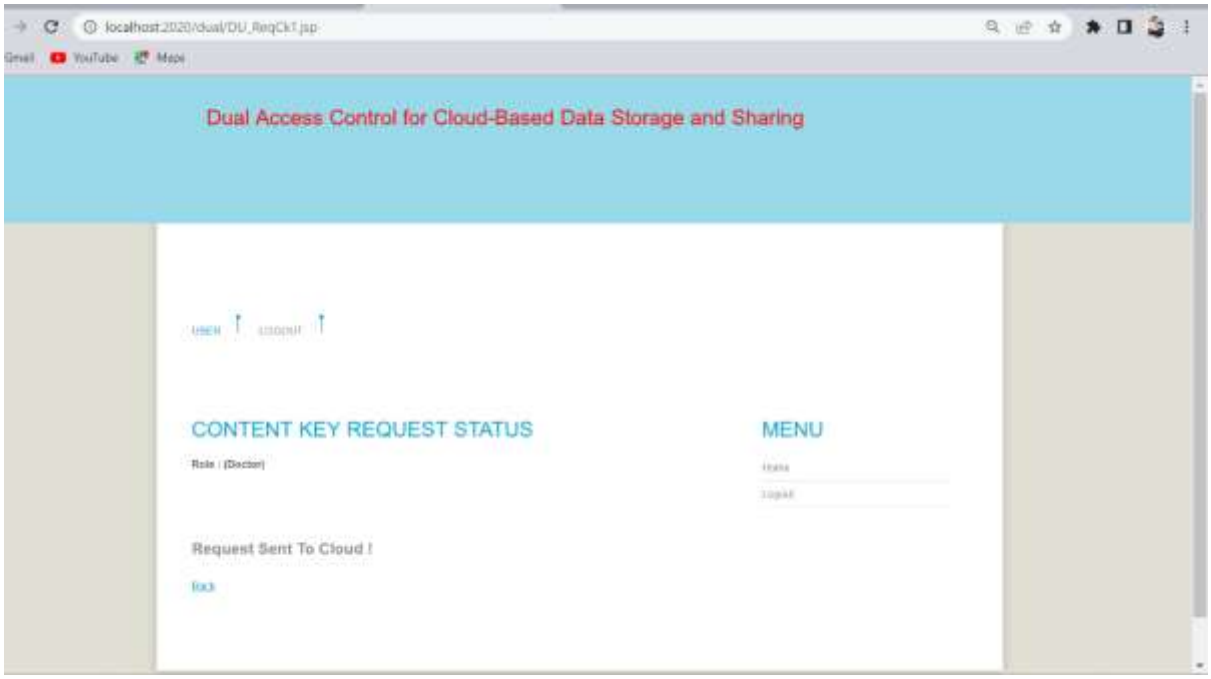

Fig 7: User requesting MSK and Content key

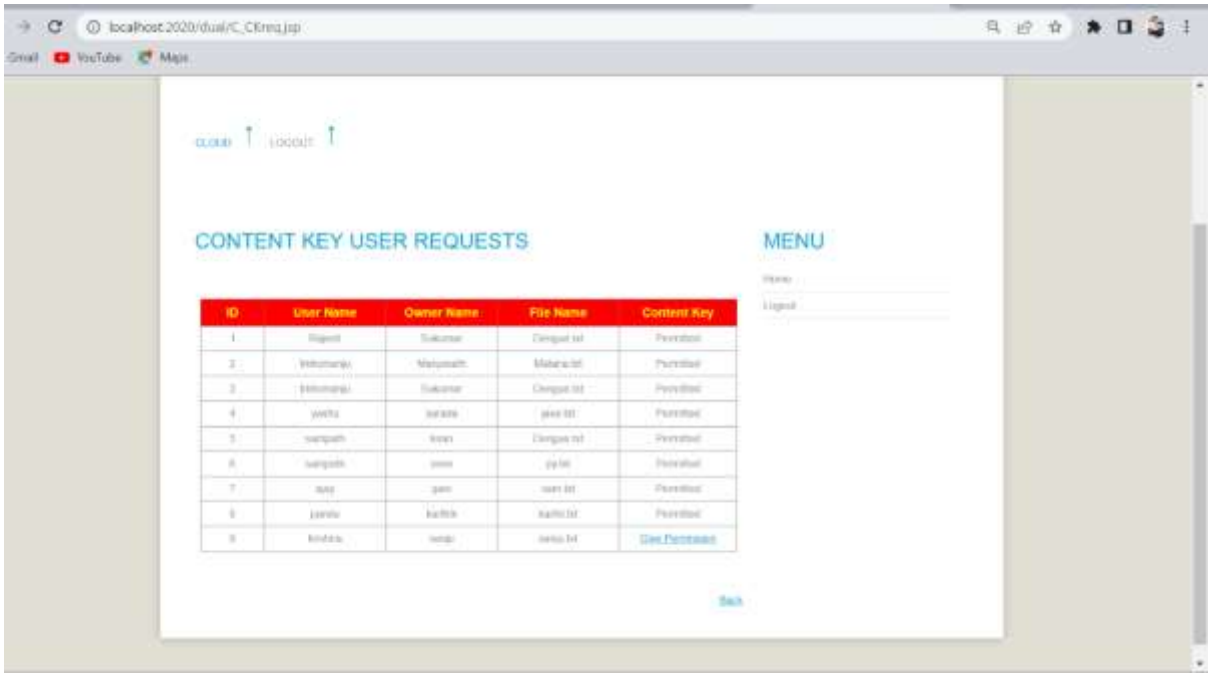

Fig 8: Cloud giving response to request for keys by the users

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

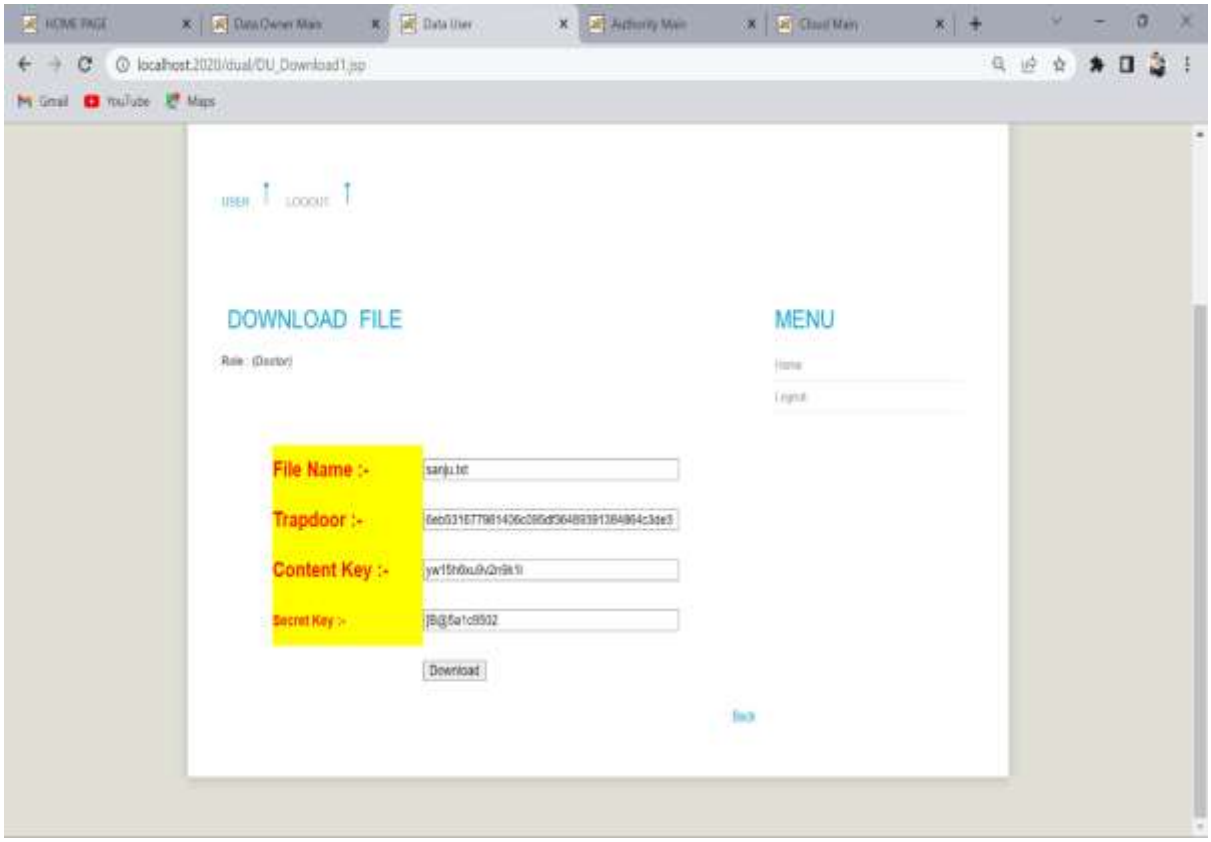

Fig 9: user downloading the file

5.CONCLUSION

When data providers outsource their encrypted data to the cloud and can share the data with users possessing specified credentials, attribute-based encryption (ABE) has been widely used in cloud computing. On t he o ther hand, deduplication is a significant strategy to save the extra room and organization data transfer capacity, which wipes out copy duplicates of indistinguishable information. However, the standard ABE systems are too expensive to use in some commercial storage services because they do not support secure deduplication. An innovative strategy for creating a storage system based on attributes that allows for secure deduplication was presented by us. A hybrid cloud architecture governs our storage system, with a private cloud handling computation and a public cloud handling storage. The confidential cloud is furnished with a hidden entryway key related with the comparing ciphertext, with which it can move the ciphertext more than one access strategy into ciphertexts of the equivalent plaintext under some other access strategies without monitoring the

basic plaintext. The private cloud first checks the integrity of the uploaded item using the attached proof after receiving a storage request. The private cloud runs a tag matching algorithm to determine whether the same data that underlies the ciphertext has been stored if the proof is valid. If this is the case, it will regenerate the ciphertext into a ciphertext that is identical to the plaintext whenever it is required over an access policy that is the union set of both access policies. There are two primary benefits to the proposed storage system. First, rather than sharing the decryption key, it can be used to share confidential data with other users by specifying an access policy. Second, it achieves semantic security in the traditional sense, whereas other deduplication schemes only do so under a weaker security concept..

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.

[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 Fujisaki and Tatsuaki Okamoto. Secure 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 and security, 10(3):665–678, 2015.

.