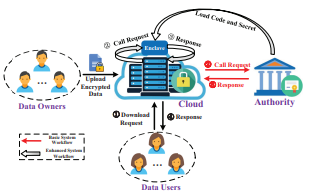
**Efficient Access Control for Cloud-Based User Data Storage and Sharing**

**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. However, simply encrypting data (e.g., via AES) cannot fully address the practical need of data management. Besides, an effective access control over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, we consider the dual access control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security 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.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * In this paper, This has been known as Economic Denial of Sustainability (EDoS) attack which targets to the cloud adopter’s economic resources. * in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. * In a cloud-based storage service, there exists a common attack that is well-known as resource-exhaustion attack. | * we propose a new mechanism, dubbed dual access control, to tackle the above aforementioned two problems. * To secure data in cloud-based storage service, attribute-based encryption is one of the promising candidates that enables the confidentiality of outsourced data as well as fine-grained control over the outsourced data. * In particular, Cipher text-Policy ABE (CP-ABE) provides an effective way of data encryption such that access policies, defining the access privilege of potential data receivers, can be specified over encrypted data |
| **EXISTING ALGORITHM**  EDoS attack | **PROPOSED ALGORITHM:-**  proxy re encryption(PRE) |
| **ALGORITHM DEFINITION:-**  Any unauthorized data user cannot download the shared file(s) (i.e., resistant to data user’s EDoS attacks. Any unauthorized data user cannot decrypt the shared file if the data user obtains the file. A data user is defined to be unauthorized if his/her attribute set does not satisfy the access policy of shared file. | **ALGORITHM DEFINITION:-**  Cipher text-Policy Attribute-based-Encryption (CP-ABE) is a versatile encryption supporting fine-grained access control over encrypted data. In a CP-ABE system, each data user is issued with a secret key according to his attributes. A data owner can choose an access structure A and encrypt his data under A. The encrypted file can be decrypted by any data user whose attribute set satisfies A. CP-ABE systems proposed in recent years usually make essential use of linear secret-sharing schemes |
| **DRAWBACKS:-**   * Data owner is honest in the sense that she/he encrypts the outsourced data and uploads the encrypted data to the cloud honestly. * Data user is malicious in the sense that she/he may try to download the shared file which is not authorized for her/him and launch the EDoS attacks. * Cloud is honest-but-curious in the sense that it may gather sensitive information curiously by observing the transcript but will not deviate from the specification | **ADVANTAGES:-**   * we allow data user to generate a download request. * Upon receiving the download request, with help of the authority or the enclave of Intel SGX, a cloud server is able to check if the data user is authorized to gain access to the data. * No other information is revealed to the cloud server except the knowledge of whether the user is authorized |

**System Architure**

****

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS**:

System : Pentium i3 Processor

Hard Disk : 500 GB.

Monitor : 15’’ LED

Input Devices : Keyboard, Mouse

RAM : 2 GB

**SOFTWARE REQUIREMENTS:**

Operating system : Windows 10.

Coding Language : Java.

Tool : Netbeans7.2.1

Database : MYSQL

**REFERENCE**:

Jianting Ning, Xinyi Huang, Willy Susilo, Senior Member, IEEE, Kaitai Liang, Member, IEEE, Ximeng Liu Member, IEEE, and Yinghui Zhang, Member, IEEE, “Dual Access Control for Cloud-Based Data Storage and Sharing”, IEEE Transactions on Dependable and Secure Computing ( Early Access ), 2021.