**A Data Sharing with Policy Authorization in Database**

**ABSTRACT**:

Cloud storage services allow data owners to outsource their potentially sensitive data (e.g., private genome data) to remote cloud servers in a ciphertext form. To enable data owners to further share the data encrypted in ciphertexts, many proxy re-encryption (PRE) schemes are proposed. However, most schemes only support single-recipient or coarse-grained re-encryption, which may limit the flexibility for data sharing. To address this issue, we propose a Policy-based Broadcast Access Authorization (PBAA) scheme by introducing the well-established identity-based broadcast encryption (IBBE) and key-policy attribute-based encryption into PRE. In our PBAA scheme, a data owner can apply IBBE to encrypt his data to a group of recipients. More importantly, the data owner can generate a delegation key with an access policy, and send this key to the cloud such that it can convert any initial ciphertext satisfying the access policy into a new ciphertext for a new group of recipients. With these features, cloud users can share their remote data in a secure and flexible way. Security analysis and performance evaluation show that the PBAA scheme is secure and efficient, respectively

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * The privacy of outsourced data is well protected by the PBAA scheme. Specifically, any user without the correct private key cannot access encrypted data; and even having the delegation key, the cloud cannot access encrypted data, nor deduce a valid delegation key to re-encrypt the ciphertext that is not specified by the data owner. * We also conduct theoretical and experimental analyses on the PBAA scheme and make comparisons with some related schemes. * The results show that the PBAA scheme achieves an efficient and flexible access authorization for data sharing, without incurring significant computational costs to data users or cloud servers | * . However, most schemes only support single-recipient or coarse-grained re-encryption, which may limit the flexibility for data sharing. * To address this issue, we propose a Policy-based Broadcast Access Authorization (PBAA) scheme by introducing the well-established identity-based broadcast encryption (IBBE) and key-policy attribute-based encryption into PRE. * In our PBAA scheme, a data owner can apply IBBE to encrypt his data to a group of recipients. More importantly, the data owner can generate a delegation key with an access policy, and send this key to the cloud such that it can convert any initial ciphertext satisfying the access policy into a new ciphertext for a new group of recipients. |
| **EXISTING ALGORITHM**  Policy-based Re-encryption | **PROPOSED ALGORITHM: -**  Policy-based Broadcast Access Authorization (PBAA) |
| **ALGORITHM DEFINITION: -**  If deciding to share data encrypted in the broadcast ciphertexts with a new group of users, the data owner can formulate an access policy to generate a delegation key. Given this key, the cloud can convert any initial ciphertext satisfying the access policy into a new ciphertext such that the underlying data can be accessed by the new group of users. | **ALGORITHM DEFINITION: -**  A PBAA system confronts several types of active attacks. First, malicious CSP or hackers intruding the cloud storage system would search and access the data outsourced by data owners. Second, unauthorized users would impersonate data owners or authorized users to access the outsourced data; even worse, they may collude with CSP to download and read the data. Third, CSP may abuse the delegation keys to try to re-encrypt the ciphertexts beyond the scope of the delegations. Considering these realistic attacks, we identify the security goals of PBAA as follows. Privacy of outsourced data. If the data outsourced to CSP has been encrypted, then only the data users having the correct private keys can access. Also, the data that has been re-encrypted can only be accessed by the data users having the correct private keys. In other words, any encrypted data is unreadable to CSP and unauthorized data users (who do not have correct private keys). Specificity of delegation key. A delegation key issued by a data owner can only be used to convert the specified ciphertexts (i.e., the ciphertexts with conditions satisfying the access structure). Even CSP or authorized data users cannot abuse the delegation key to re-encrypt unspecified ciphertexts, nor can they deduce a valid delegation key to re-encrypt unspecified ciphertexts |
| **DRAWBACKS: -**   * We have several types of active attacks. * These identities could be hashes of some secret information (e.g., passwords) of data users | **ADVANTAGES: -**   * secure and flexible data sharing in cloud computing * Broadcast encryption achieves a secure multi-recipient data sharing |

**MINIMUMSYSTEM 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 : Eclipse

Database : MYSQL