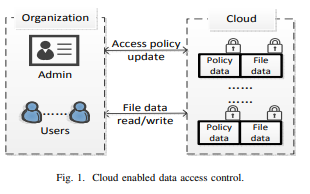
**CRYPT-DAC: CRYPTOGRAPHICALLY ENFORCED DYNAMIC ACCESS CONTROL IN THE CLOUD**

**ABSTRACT**:

Enabling cryptographically enforced access controls for data hosted in untrusted cloud is attractive for many users and organizations. However, designing efficient cryptographically enforced dynamic access control system in the cloud is still challenging. In this paper, we propose Crypt-DAC, a system that provides practical cryptographic enforcement of dynamic access control. Crypt-DAC revokes access permissions by delegating the cloud to update encrypted data. In Crypt-DAC, a file is encrypted by a symmetric key list which records a file key and a sequence of revocation keys. In each revocation, a dedicated administrator uploads a new revocation key to the cloud and requests it to encrypt the file with a new layer of encryption and update the encrypted key list accordingly. Crypt-DAC proposes three key techniques to constrain the size of key list and encryption layers. As a result, Crypt-DAC enforces dynamic access control that provides efficiency, as it does not require expensive decryption/reencryption and uploading/re-uploading of large data at the administrator side, and security, as it immediately revokes access permissions. We use formalization framework and system implementation to demonstrate the security and efficiency of our construction.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * The first scheme requires an administrator to re-encrypt file with new keys as discussed above. * Instead, the second scheme delegates users to re-encrypt the file when they need to modify the file, relieving the administrator from re-encrypting file data by itself. * In which the symmetric homomorphic encryption scheme is used to encrypt the file. * Such a design enables the cloud to directly re-encrypt file without decryption. | * In this paper, we propose Crypt-DAC, a system that provides practical cryptographic enforcement of dynamic access control. Crypt-DAC revokes access permissions by delegating the cloud to update encrypted data. * In Crypt-DAC, a file is encrypted by a symmetric key list which records a file key and a sequence of revocation keys. * In each revocation, a dedicated administrator uploads a new revocation key to the cloud and requests it to encrypt the file with a new layer of encryption and update the encrypted key list accordingly. * Crypt-DAC proposes three key techniques to constrain the size of key list and encryption layers. * As a result, Crypt-DAC enforces dynamic access control that provides efficiency, as it does not require expensive decryption/reencryption and uploading/re-uploading of large data at the administrator side, and security, |
| **EXISTING ALGORITHM**  FK tuples | **PROPOSED ALGORITHM:-**  Crypt-DAC |
| **ALGORITHM DEFINITION:-**  To alleviate the overhead, u delegates the administrator to do so. Assume that there are m roles having permissions to fn. u uploads the new key list (k) to the administrator and delegates it to update the key in the FK tuples of the m roles. For each of the m roles r, the administrator encrypts k by the encryption key of r, and uploads the encryption for the cloud provider to update | **ALGORITHM DEFINITION:-**  First, Crypt-DAC proposes delegation-aware encryption strategy to delegate the cloud to update policy data. For a file, the administrator appends a new revocation key at the end of its key list and requests the cloud to update this key list in the policy data. The size of the key list however increases with the revocation operations, and a user has to download and decrypt a large key list in each file access. To overcome this problem, we adopt the key rotation technique to compactly encrypt the key list in the policy data. As a result, the size of the key list remains constant regardless of revocation operations.. |
| **DRAWBACKS:-**   * This scheme incurs a considerable communication overhead. * This scheme, however, comes with a security penalty as the revocation operation is delayed to the next user’s modification to the file. | **ADVANTAGES:-**   * For revocation efficiency, Crypt-DAC incurs lightweight communication overhead at the administrator side as it does not need to download and re-upload file data. * For immediate revocation, the permissions of users are immediately revoked as the files are re-encrypted |

**System Arichture**

****

**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 7.

Coding Language : Java.

Tool : Eclipse

Database : MYSQL