**Crypt-DAC Cryptographically Enforced Dynamic Access Control in the Cloud**

Alternative Title: Attribute based data management in crypt cloud

**Aim:**

The main aim of this project is to provide integrity of an organization data which is in public cloud.

**Synopsis:**

Data owners will store their data in public cloud along with encryption and particular set of attributes to access control on the cloud data. While uploading the data into public cloud they will assign some attribute set to their data. If any authorized cloud user wants to download their data they should enter that particular attribute set to perform further actions on data owner’s data. A cloud user wants to register their details under cloud organization to access the data owner’s data. Users want to submit their details as attributes along with their designation. Based on the user details Semi-Trusted Authority generates decryption keys to get control on owner’s data. An user can perform a lot of operations over the cloud data. If the user wants to read the cloud data he needs to be entering some read related attributes, and if he wants to write the data he needs to be entering write related attributes. Foe each and every action user in an organization would be verified with their unique attribute set. These attributes would be shared by the admins to the authorized users in cloud organization Crypt-DAC enforces dynamic access control that provides efficiency, as it does not require expensive decryption, re -encryption and uploading/re-uploading of large data at the administrator side, and security, as it immediately revokes access permissions.

**Existing System:**

In existing system the considerable advancements in cloud computing, users and organizations are finding it increasingly appealing to store and share data through cloud services. Cloud service providers (such as Amazon, Microsoft, Apple, etc.) provide abundant cloud based services, ranging from small-scale personal services to large-scale industrial services. However, recent data breaches, such as releases of private photos, have raised concerns regarding the privacy of cloud-managed data. Actually, a cloud service provider is usually not secure due to design drawbacks of software and system vulnerability. Then the crypt-DAC proposes three key techniques. 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. This method is called onion encryption.

**Problem statement**

Crypt-DAC proposes adjustable onion encryption strategy to delegate the cloud to update file data. For a file, the administrator requests the cloud to encrypt the file with a new layer of encryption.

**Proposed System:**

To overcome these problems, we present Crypt-DAC, a cryptographically enforced dynamic access control system on un-trusted cloud. To overcome the onion encryption we propose Tuple for security purpose. Every time user should upload the tuple file while accessing the cloud files. If the tuple verification is success you can access the files otherwise admin sent you a warning message three times and then admin will block you at the same time camera will capture your face and sent to admin.

**Modules:**

* **Role Creation**
* **Admin File Upload**
* **Tuple Generation**
* **User File Access**

**1. Role Creation**

The roles will be created for employee and the cloud authority. The roles will be created based on their designation. The employee and the cloud authority will get added based on their designation and roles.

**2. Admin File Upload**

The admin will upload the file which is of two types. They are public and private files. The admin will add the news. If the file is public, it does not contain any access permission. If the file is private, then the tuples will get generated.

**3. Tuple Generation**

Here file permission keys are issued to the employees in the organization based on their experience and position to their registered. Senior Employees have all the permission to access the files (read, write, delete, & download). Freshers or trainee only having the permission to read the files. Some Employees have the permission to read and write. And some employees have all the permissions except deleting the data. If any Senior Employee leaks or shares their secret permission keys to their junior employees they will request to download or delete the Data Owners Data. Tuples are the encrypted PDF files which will be generated while the employee logs in. These tuples will get generated based on the roles of employee and the cloud authority.

**4. User File Access**

Authorized DUs are able to access (e.g. read, write, download, delete and decrypt) the outsourced data. While entering the password for re-encryption system, it will generate attribute set for their role in background validate that the user has all rights to access the data. If the attributes set is not matched to the Data Owners policy files they will be claimed as guilty. If we ask them we will find who leaked the key to the junior employees. If any employee does an illegal access of files without any permission, they will be warned for 3 times. If they continues the access, they will get captured by the camera and send as a notification to the admin.

**Software Requirements**

* Windows 7 and above
* JDK 1.8
* J2EE
* Tomcat 7.0
* MySQL

**Hardware Requirements**

* Hard Disk : 80GB and Above
* RAM : 4GB and Above
* Processor : P IV and Above

**Technology Used**

* + - J2EE (JSTL, Springboot), JavaScript, HTML, CSS, AJAX.

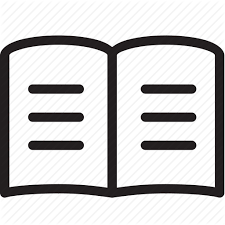
**Algorithm**

* AES
* RSA

**Conclusion:**

Thus to provide integrity of an organization data which is in public cloud is achieved successfully.

**Architecture:**



File Upload

Data Owners

Public Cloud

Cloud Users

Tuple File Generation

Encrypt Files

Various Types of File upload uploading

Login

File Read, Write, Download, Delete

File Accessing Page

Upload Tuple File

True User

Key Leakage

Account Blocked

Informs to Data Owners

Data owners have all rights to delete and edit their data

Take a Picture of the user