Applied Research Methods:

Crypto-DAC over encrypted data scheme

Version	Previous Modification was done on	Modification is done by	Brief description of document modification
1.1	12th July 2022	Veerabhadraswamy.NG	Document first created. Included basic content
1.2	7th August 2022	Veerabhadraswamy.NG	Submitted proposal for review
1.3	22nd August 2022	Veerabhadraswamy.NG	Final corrections done

Module Title:	Applied Research Methods
Module Code:	B9BA109
Module Leader:	Dr. Amir Esmaeily
Level:	9
Assessment Title:	**Crypto-DAC over encrypted data scheme**
Assessment Number:	1
Restrictions on Length:	2000 words
This document's word count excluding Index, Table of contents, and References	2292 words
Individual/Group:	Individual
Assessment Weighting:	100%
Hand In Date:	23rd August 2022
Mode of Submission:	Online via Moodle
Student ID/Student Name	**10603349/Veerabhadraswamy.NG**

Table of contents

Title Page.....1

Table of Contents.....3

Abstract.....4

Introduction.....4

Background.....4

Problem Statement.....5

Aims and objective.....5

Literature review.....6

Methodology.....7

Work Plan.....8

Conclusion.....11

References.....11

Abstract:

Many users and organizations using untrusted cloud services find it attractive to enable cryptographically enforced access controls for data. It is challenging to design an efficient cryptographically enforced dynamic access control system. In this paper, a proposal on Crypto-DAC is provided, which uses a system that provides practical cryptographic enforcement of dynamic access control. Here using the symmetric key list, the file is encrypted and this would further record a file key. Cloud service providers (such as Amazon, Microsoft, Apple, etc.) provide abundant cloud-based services, ranging from small-scale personal services or 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. As such, a critical issue is how to enforce data access control on the potentially untrusted cloud. To overcome the mentioned security issues, Crypto-DAC over encrypted data scheme is proposed through which access control on untrusted cloud services is performed to leverage cryptographic primitives.

Introduction:

Cloud computing has become appealing for users and organizations to store and further share data. Though there are abundant services provided by cloud service providers, there is always a risk of a data breach, which is observed in the recent past across these organizations. This has made to think that Cloud service provider is not secure with their software drawbacks and system vulnerability. Hence on a potentially untrusted cloud, it is a critical issue to enforce data access control. To overcome problems of communication overhead, on an untrusted cloud, a cryptographically enforced dynamic access control system is developed. This method of Crypto-DAC over encrypted data scheme uses a symmetric key list that records a file key. During revocation, a new key to the cloud is uploaded by an administrator that encrypts the file with a new layer of encryption and accordingly updates the encrypted key list. It can be noticed that the size of the key list and encryption layers would increase as the number of revocation operations, which incurs additional decryption overhead for users to access files.

Background:

In this section, system and threat models are defined first, then classes of cryptographic primitives are defined based on Crypto-DAC. A system model is depicted in the following figure

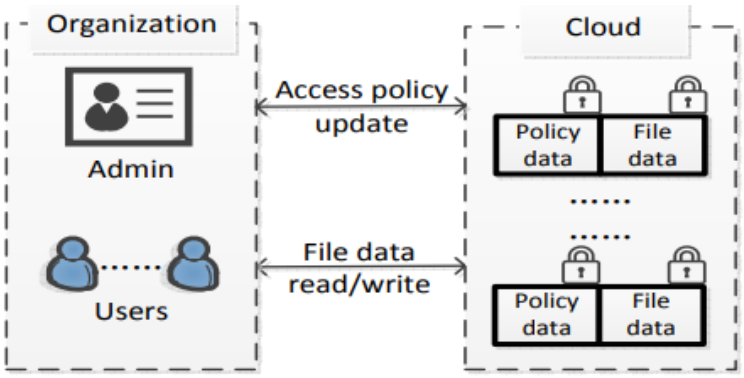


Figure: Cloud-enabled data access control

Taking a scenario where enterprise storage is commercially outsourced by companies through contract. There are three types of entities in our system model:

1. A cloud provider, which is responsible for the data storage and management

2. An access control administrator, which is responsible for managing access policies of the file data.

3. A large number of users who download any policy/file data from the cloud, but are only allowed to decrypt and read files according to their access permissions.

In a threat model, we consider that the administrator is honest. The users may try to access the file data out of their access permissions by compromising the cloud provider. The security goals are aimed to provide confidentiality and access control for the cloud-hosted file data with confidentiality and read and write access control.

Problem Statement:

Currently, only a few works investigated the problem of dynamic data access control. Of which presenting two revocation schemes. The first scheme requires an administrator to re-encrypt files with new keys as discussed above. This scheme incurs a considerable communication overhead. 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. This scheme, however, comes with a security penalty as the revocation operation is delayed to the next user's modification to the file. As a result, a newly revoked user can still access the file before the next writing operation.

As observed in the previous works static scenarios are considered in which access control policies rarely change. The previous works incur high overhead when access control policies need to be changed in practice. At a first glance, the revocation of a user's permission can be done by revoking his access to the keys with which the files are encrypted. This solution, however, is not secure as the user can keep a local copy of the keys before the revocation. To prevent such a problem, files have to be re-encrypted with new keys. This requires the file owner to download the file, re-encrypt the file, and upload it back to the cloud for updating the previously encrypted file, incurring prohibitive communication overhead at the file owner side.

Aim and objective:

The main aim is to propose Crypto-DAC, a system that provides practical cryptographic enforcement of dynamic access control. This also provides confidentiality and access control for the cloud-hosted file data. Confidentiality is taken care of through systems that store encrypted data on the cloud, but never reveal the decryption keys to the cloud. This protects the confidentiality of the file data. Read access control present in the system uses Cryptography [8] to enforce access control so that users can only read file data according to their access permissions. Write access control in the system with writing permission enforcement, on a system that relies on the cloud. Through this, we design and analyze Crypto-DAC based on the role-based access control model named, which is widely used in practical applications.

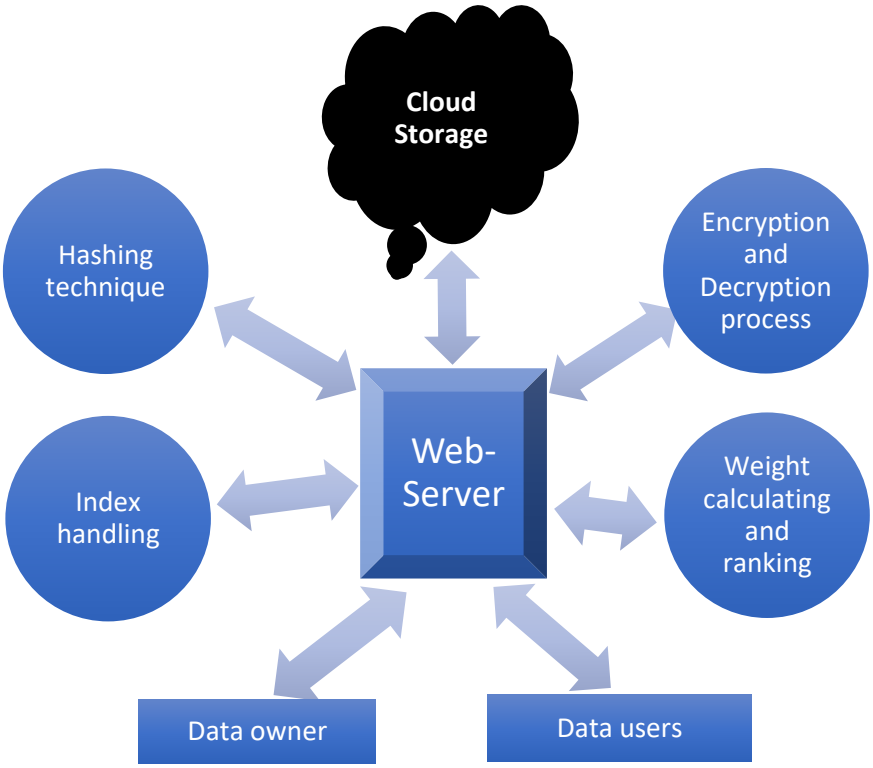
Literature review:

The present cryptographically enforced access control schemes can be classified as follows:

Hierarchy access control – "Ehud Gudes" [2] from "Ben-Gurion University of the Negev" has mentioned in his IEEE paper "The Design of a Cryptography Based Secure File System" that it is possible through Cryptography [8] to enforce hierarchy access control without considering dynamic policy scenarios. "S. G. Akl and P. D. Taylor" [3] from Queen's university Canada have mentioned in their IEEE paper "Cryptographic solution to a problem of access control in a hierarchy" that oppose a key assignment scheme to simplify key management in hierarchical access control policy. Also, this work does not consider policy update issues. Later, "M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken" [4] through their IEEE paper "Dynamic and efficient key management for access hierarchies" propose a method that allows policy updates, but in the case of revocation, all descendants of the affected node in the access hierarchy must be updated, which involves high computation and communication overhead.

Role-based access control [9]: "L.Ibraimi" [5] in his Ph.D. thesis "Cryptographically support role-based access control" has mentioned that structure using mediated public encryption. However, their revocation operation relies on additional trusted infrastructure and an active entity to re-encrypt all affected files under the new policy. Similarly, "A. L. Ferrara, G. Fuchsbauer, and B. Warinschi" [6] define a secure model to formally prove the security of a cryptographically enforced RBAC system. They further show that an ABE-based construction secures under such a model. However, their work focuses on theoretical analysis

Methodology:



Particularly in this proposal, we will make use of “Drive-HQ” as a cloud-storage option to furnishes FTP server hosting service. DriveHQ as a File-Manager can be used in an Android environment to provide enterprise file management, sharing, and backup tool. Here, it can manage local files, cloud files and folders shared with users. It is not just an application, but it is a part of DriveHQ's one-stop cloud IT solution.

A hash function will be used, which has an algorithm that takes an arbitrary amount of data input (can be called a credential) and it produces a fixed-size output of enciphered text called a hash value, or just “hash”. This particular enciphered text can further be stored instead of the password itself and can be used to verify the user Hashing is designed to solve the problem of needing to efficiently find or store an item in a collection. Generally, hashing means using some algorithm that is used to map object data to some representative integer value. This hash code can then be used as a way to narrow down the search when looking for the item in the map. These hash codes are further used to generate an index, at which the value is stored.

Cryptography [8] will be used here for secure communication from outside observers. To make this happen we make the use of Encryption [12], which is the process of translating the plain text into ciphertext, which is not understandable. Decryption is the process of converting ciphertext back to plaintext for which a key is used to decrypt the encrypted message. Through this, we achieve more robust connections to elevate one’s privacy. The goal here is to have every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key.

Through index, handling will be making the best use of Search-Index. As it is well known in Google whenever a word is typed within seconds search results are displayed. This is all possible because of the fast phased internet which is working as a backbone. In the traditional method, indexes are observed in books that are created by the author(s), and editors but also by professionals specialized in indexing, so-called indexers. To sum up, about Search-Index, it is to find information with little effort and fast using a keyword. A search index is critical in creating relevant search results.

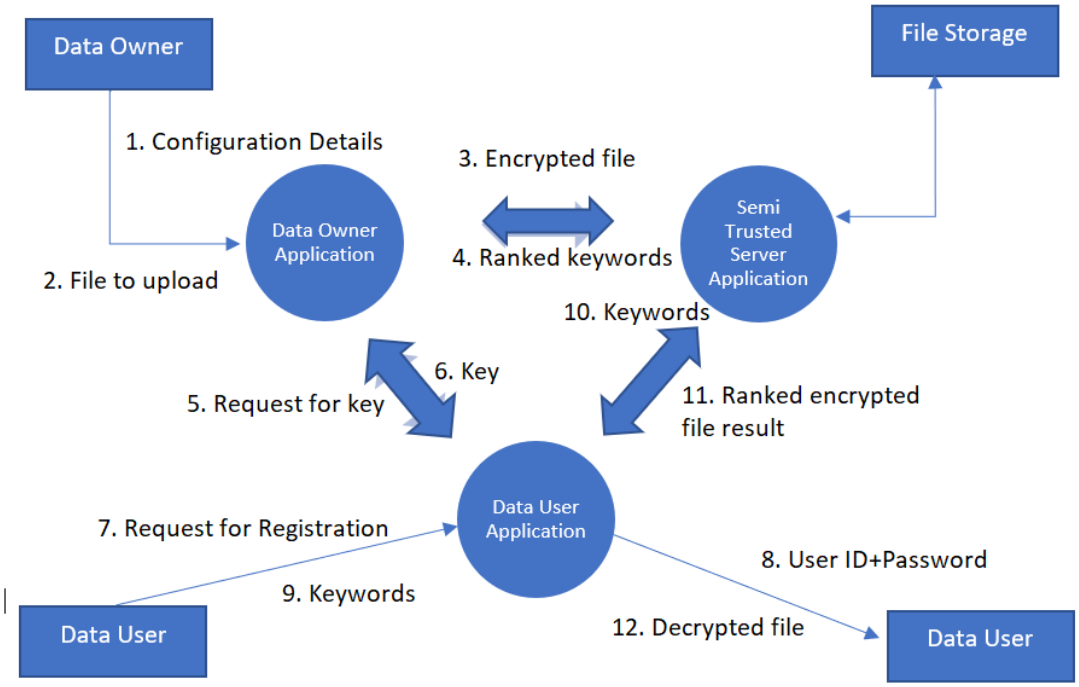
Natural Language Processing (NLP) search will be used. This method will strive to process and build a system that understands and respond to the text data in much of the same way as humans do. This also helps in identifying the particular keywords a user is trying to find in less time. This type of search combines the computational linguistics of rule-based modeling of human language having deep learning and machine learning models. With these technologies, the computer enables to process human language in the form of text or voice data.

To accomplish the mentioned proposal, following software requirements are proposed:

- Operating system: Windows 10/11
- Coding Language: Java (JDK 16)
- Web Server: TomCAT 8/9
- Database: My-SQL 7/8
- UGI for DB: SQLyog
- Cloud Storage: Drive-HQ

Work Plan:

The work plan is mentioned in the following graphical representation. This has a data flow depicting the "flow" of data through an information system, modeling its process aspects. This is used as a preliminary step to create an overview of the system and it also visualizes data processing.



Data Owner Session

- Login
- Category (View Only)
- Configuration
    - o File Storage Server Configuration
    - o Crypto Key Generation
    - o Hash Key Generation
- User Creation
    - o Each User come under a Category
- User Revocation
    - o Select the user
    - o Revocation is done for the user
- User Renewal
    - o Select the user
    - o Renew the user

- Upload a file
    - o Select the file from the system
    - o Provide Access Control
    - o Remove unnecessary words
    - o Find Keywords
    - o Calculate the Content Weightage of keywords
    - o Convert the Keywords into Hash-code
    - o Place the Hash-code in Index Array
    - o Encrypt the File using Crypto Key
    - o Upload the encrypted file into the file storage
- Keyword Ranking
    - o View keyword & weightage
    - o Calculate the Ranking for a keyword
    - o Store the keyword Ranking in a Table
    - o View keyword Ranking details
- View User Details
- Change Password

Data User Session

- Login
- User Profile
- Search with Keyword

    Input Search Keyword

    - o Convert the keyword into hash-code
    - o Generate Hash-codes.
    - o Send the Hash codes to the server
    - o Based on the Hash codes received server has to check the keyword index and if any matching files are available, list all the file names to the user.
    - o View the shortlisted files from Server
    - o Download the files
    - o Decrypt the file
- Change Password
- logout

a) Key Generation: In this module, Data Owner going to generate two keys for the encryption and decryption process. By using an Asymmetric algorithm, Data Owner going to generate a master secret key and public key.

b) Access Control: Here, the Data Owner is going to give access control for the files he will going to upload while uploading Data Owner going to encrypt the file with the help of a master secret key for the security purpose of the cloud.

c) Keyword Indexing: Remove unnecessary words from the file and finds the keywords. Calculate the Content Weightage of keywords Convert the Keywords into hash code by using hashing algorithm; place the hash code in Index Array.

d) Send Public Key: After the User requests data owner has to send the corresponding Public Key to the user's mail id.

e) Search with Keyword: The user has to Input the search keyword. Convert the keyword into hash-code. Send generated hash codes to the server, based on the Hash codes received server has to check the keyword index and if any matching files are available, list all the file names to the user. View the shortlisted files from the server, download the files and finally decrypt the file with the owner's public key.

f) User Renewal: Data Owner can able to renew the user who is removed from the file access earlier. Once the user is renewed then in the search options one can retrieve the files with corresponding keywords

Conclusion:

Through this proposal, the plan is to provide a system that practically enforces cryptography using dynamic access control in the potentially untrusted cloud provider. Considering the practical problem of a privacy-preserving data sharing system based on public cloud storage which requires a data owner to distribute a large number of keys to users for enabling them to access the documents, for the first time propose the concept of Crypto-DAC over encrypted data scheme. The performed analysis confirms that the work can provide an effective solution to building a practical data-sharing system based on public cloud storage.

References:

- [1] F. Wang, J. Mickens, N. Zeldovich, and V. Vaikuntanathan, Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Clouds, in NSDI, 2016.
- [2] E. Gudes, The Design of a Cryptography Based Secure File System, IEEE Transactions on Software Engineering, vol. 6, no. 5, 1980.
- [3] S. G. Akl and P. D. Taylor, Cryptographic solution to a problem of access control in a hierarchy, IEEE TOCS, vol. 1, no. 3, 1983.
- [4] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, Dynamic and efficient key management for access hierarchies, ACM TISSEC, vol. 12, no. 3, 2009

- [5] L. Ibraimi, Cryptographically enforced distributed data access control, Ph.D. dissertation, University of Twente, 2011.

- [6] A. L. Ferrara, G. Fuchsbauer, and B. Warinschi, Cryptographically enforced RBAC, in CSF, 2013.

- [7] IEEE document on "Crypt-DAC" https://eprint.iacr.org/2017/090.pdf (Accessed on 10th July 2022)

- [8] Wiki details on Cryptography, https://en.wikipedia.org/wiki/Cryptography (Accessed on 20th July 2022)

- [9] IEEE, "Role Based Access Control models", https://ieeexplore.ieee.org/document/6976127 (Accessed on 2nd August, 2022)

- [10] F. Wang, J. Mickens, N. Zeldovich, and V. Vaikuntanathan, Sieve:Cryptographically Enforced Access Control for User Data in Untrusted Clouds, in NSDI, 2016

- [11] IEEE, "Crypt-DAC: Cryptographically Enforced Dynamic Access Control in the Cloud" https://ieeexplore.ieee.org/document/8676350 (Accessed: 10th July 2022)

- [12] Wiki details on Encryption, https://en.wikipedia.org/wiki/Encryption (Accessed on 15 July)