WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

CRYPTCLOUD+ Attribute Based Secure Data Access Control Storage in Cloud

D.Deepika[1], M. V. Disali[2], I. Raihana[3],

[1,2,3,]Department of Computer Science, R.B. Gothi Jain College for Women, Redhills, Chennai- 600052

A B S T R A C T

Information sharing in the cloud, technology, is rising as a guaranteeing procedure for permitting users to access information. However, the data owner who stores their information in cloud servers is progressively challenging data privacy and the security of information that are stored in the cloud. This paper concentrates on providing a security for the cloud information sharing services that permits users dynamic access to their information. In order to achieve this, we propose an effective and flexible privacy preserving information policy by using Cipher text Policy Attribute Based Encryption (CP-ABE) system. To ensure strong information sharing security, the policy succeeds in protecting the privacy of cloud data owners

Keywords: cloud computing, Storage, file permission, extraction

1. Introduction

Cloud computing gives us the ability to use apps as utilities over the Internet. It enables us to design, configure, and personalise programmes online. A network or the Internet is referred to as a cloud. In other terms, the Cloud is something that exists in distant regions. Cloud services can be delivered across public and private networks, such as WAN, LAN, and VPN. Cloud-based applications include e-mail, conferencing, and customer relationship management (CRM). Cloud computing refers to the ability to remotely manipulate, configure, and access hardware and software resources. It provides data storage, infrastructure, and applications all across the internet.

CLOUD STORAGE

Cloud storage allows organisations and individuals to preserve data securely online so that it may be accessed at any time and shared with those who have been granted permission. Cloud storage also allows you to back up your data and recover it off-site. Individuals now have access to a variety of free cloud computing platforms, including Google Drive, Dropbox, and Box, all of which offer enhanced subscription packages with higher storage sizes and extra cloud services.

2. Main Goal

The goal is to propose an authority and revocable Crypt Cloud with white-box traceability and auditing to achieve the following requirements:

1) Security guarantees should be provided –to protect the integrity of the data and the flexibility of access control over encrypted data.

2) Computation should be cost-effective - computation cost spent on trace and revocability are minimized.

3) Audit, trace and revoke procedures should be efficient - system betrayers are easily pointed out in a short period of time.

3. Crypto+ Cloud

Data owners will keep their data in the public cloud, which will be encrypted and have a certain set of features for access control. Cloud owners have complete control of their data and can download and erase it whenever they wish. They will assign some attribute set to their data while uploading it to the public cloud. A cloud user wishes to register their information with a cloud organisation so that they can access the data owner's information. Along with their designation, users desire to provide their personal information as characteristics. To get control over the data of the owner, the Semi-Trusted Authority creates decryption keys. A user can manipulate cloud data in a variety of ways. Users in an organization's unique attribute set would be validated for each and every action. The admin would share these attributes with the cloud organization's permitted users. These characteristics will be saved in cloud-based policy files. If a user spills their unique decryption key to a malevolent user, data owners can track them down by submitting an audit request to an auditor, who will assess the request and determine who is responsible. By planning a responsible expert and revocable Crypt Cloud that supports white-box identifying and inspecting (referred to as Crypt Cloud+), we have tended to the test of certification spillage in a CP-ABE based distributed storage architecture. Crypt Cloud+, in particular, allows us to track and avoid malicious cloud clients (spilling certifications).

4. Framework

. • Data owners (DOs) encrypt their data under the relevant access policies prior to outsourcing the (encrypted) data to a public cloud (PC).

• PC stores the outsourced (encrypted) data from DOs and handles data access requests from data users (DUs)

• Authorized DUs are able to access (e.g. download and decrypt) the outsourced data.

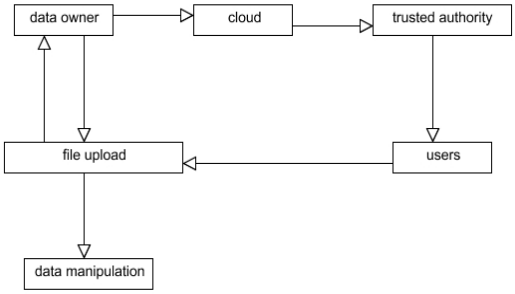
4.1 SYSTEM FEATURES:

1) The capacity to track and identify malevolent cloud users: Users who leak their login credentials can be tracked and recognised.

2) Accountable authority: A semi-trusted authority that generates and distributes access credentials to unauthorised users (without proper authorisation) can be discovered. This allows for additional actions to be conducted (e.g. criminal investigation or civil litigation for damages and breach of contract).

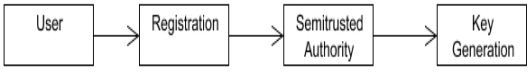
3) Auditing: An auditor can determine whether or not a (suspected) cloud user has leaked his or her login credentials.

4) Tracing requires "almost" zero storage. Paillier-style encryption as an extractable commitment in tracing malevolent cloud users and, more realistically, no need to keep a user identity table for tracing (unlike the approach used in [27]).



4.2 ORGANIZATION PROFILE CREATION AND KEY GENERATION:

User has abeginning degree Registration Process on the internet end. The customers offer their very own private facts for this manner and it's miles saved withinside the server because the database. Now the Accountable STA (semi-relied on Authority) generates decryption keys to the customers primarily based totally on their Attributes Set (e.g. name, mail-id, touch range etc..,). User receives the supply to get entry to the Organization records after you have decryption keys from Accountable STA.

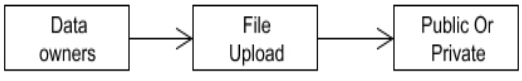


4.3 DATA OWNERS FILE UPLOADS:

Owners of data create accounts in the public cloud and upload their stuff there. Data owners will encrypt their data using the RSA Encryption technique and produce public and secret keys while uploading files to the public cloud. Additionally, it generates a single unique file access permission key for the organization's users to access their data.

4.4 FILE PERMISSION AND POLICY FILE CREATION:

Different data owners will generate different file permission keys to their files and issues those keys to users under the organization to access their files. And also generates policy files to their data that who can access their data. Policy File will split the key for read the file, write the file, download the file and delete the file.



4.5 TRACING WHO IS GUILTY:

Authorized data users have access to outsourced data stored in the cloud (e.g. read, write, download, delete, and encrypted). Employees in the organisation are given file authorization keys depending on their experience and position to access the file that the data owner has saved. Senior employees have complete access to all of the files (read, write, delete, & download). Fresher has only read-only access to the files. Some employees have been granted the ability to read and write. Some employees have all permissions except the ability to delete data. If a senior employee leaks or reveals their secret permission keys with their subordinate employees, the Data Owners Data will be requested to be downloaded or deleted.

Conclusion

We have designed an accountable authority and revocable CryptCloud that provides white-box traceability and auditing (referred to as CryptCloud+) to address the challenge of credential leakage in CP-ABE based cloud storage systems. This is the first cloud storage system based on CP-ABE that offers white-box traceability, responsible authority, auditing, and effective revocation all at the same time. CryptCloud+, in particular, allows us to track down and block rogue cloud users (leaking credentials). Our method can also be employed in the event where the semi-trusted authority redistributes the users' credentials.

REFERENCES

1) https://jespublication.com/upload/2020-110716.pdf
2) https://jpinfotech.org/cryptcloud-secure-and-expressive-data-access-control-for-cloud-storage/
3) Dorothy Elizabeth Robling Denning, *Cryptography and Data Security.* Addison-Wesley, Reading Mass. 1982, ISBN 0-201-10150-5.
4) Mihir Bellare and Oded Goldreich.On defining proofs of knowledge. In Advances in CryptologyCRYPTO'92, pages 390–420. Springer, 1993.
5) Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015
6) M Praneesh and Jaya R Kumar. Article: Novel Approach for Color based Comic Image Segmentation for Extraction of Text using Modify Fuzzy Possiblistic C-Means Clustering Algorithm. IJCA Special Issue on Information Processing and Remote Computing IPRC(1):16-18, August 2012. Published by Foundation of Computer Science, New York, USA.
7) J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-strategy quality based encryption, in IEEE S&P, 2007
8) J. Wang, X. Chen, X. Huang, I. You, and Y. Xiang, Verifiable Auditing for Outsourcedinformationin Cloud Computing, IEEE Transactions on Computers, vol. 64, no. 11, 2015.