ISSN: 2454-9940

# INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

# CRYPT CLOUD SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE

[1]MR.A N L KUMAR, [2]BORRA BHUVANA SRI GAYATHRI

[1](Head of the Department), MCA, Swarnandhra College

[2]MCA, scholar, Swarnandhra College

## ABSTRACT

Secure cloud storage is a service that keeps your data safe and allows you to access it from anywhere. One way to protect this data is through a method called Ciphertext-Policy Attribute-Based Encryption (CP-ABE). This method is promising but can have a security risk where someone might misuse their access rights to decrypt data. We looked at two main ways this misuse can happen: one is when the authority managing access is not completely trustworthy, and the other is when a cloud user abuses their access. To address this, we&#39;ve created a system called CryptCloud that can hold these authorities accountable and revoke access if needed. This system also has features for tracking and auditing access, which helps ensure its security. We&#39;ve tested our system to show that it works effectively.

## 1. INTRODUCTION

There are growing worries regarding the security and privacy of outsourced data due to the widespread use of cloud computing. Protecting sensitive information kept in the cloud against unauthorized access at any time and from any location is a major concern. Using encryption methods on the data before to transferring it to the cloud is one way to tackle this problem. Data confidentiality and access control in cloud computing settings may be effectively achieved using Ciphertext-Policy Attribute-Based Encryption (CP-ABE). With CP-ABE, organizations and individuals can specify access policies based on attributes, and authorized users are granted access credentials corresponding to their attributes. This allows them to access the data stored in the cloud.

While CP-ABE offers access control, existing systems often overlook the issue of access credential misuse. For example, in a university setting, sensitive student information stored in the cloud could be compromised if access credentials are misused. Additionally, there is a concern about the accountability of the authority issuing access credentials, as they could potentially distribute these credentials to unauthorized users.

We provide CryptCloud, a cloud storage solution based on responsible authority and revocable CP-ABE that includes white-box auditing and traceability, to solve these problems. To determine whether the file is in a protected condition or not is the primary responsibility of the auditor. An approach to traceability using white boxes The capacity of a system to track traitors or malevolent users who purposefully divulge incomplete or altered decryption keys is known as white box traceability. In the context of White Box Traceable Ciphertext-Policy Attribute-Based Encryption (ABE), this idea is vital for identifying individuals who breach security by disclosing sensitive information. Data saved in the cloud may be securely accessed by authorized users only using CryptCloud.

It also holds the authority issuing access credentials. CryptCloud is a sophisticated system that addresses critical security challenges in cloud computing. It ensures that data stored in the cloud remains confidential and accessible only to authorized users. This traceability enhances accountability and helps prevent unauthorized access. Additionally, This feature adds an extra layer of security, ensuring that access credentials are only granted to trustworthy entities.Another important aspect of CryptCloud is its efficient tracing mechanism, which uses encryption technique. This approach minimizes the storage requirements for tracing information, making it a practical solution for real-world cloud storage systems. Overall, CryptCloud+ provides a comprehensive and practical solution for securing cloud storage, offering fine-grained access control, accountability, and traceability of access credentials.

## 2.LITERATURE SURVEY

In the realm of secure and expressive data access control for cloud storage, several researchers have made significant contributions to enhancing security measures and access control mechanisms.

**Here is a literature survey based on the works of various scholars in this field:**

**Accountable CP-ABE Systems:**

● **Li et al.:** Presented the idea of responsible CP-ABE to forestall unapproved key dispersion among intriguing clients. They later proposed a client responsible multi-authority CP-ABE framework.

● **Liu et al.:** Created white-box and black-box detectability CP-ABE frameworks. The authors Ning et al. presented CP-ABE systems that are both practical and feature-rich, with an emphasis on traceability. These systems include both white-box and black-box traceability. A tracing technique for CP-ABE was developed by Deng et al. to detect compromised

login credentials in cloud storage systems.

● . **Revocable Storage and Attribute Updating:** Sahai et al.: The revocable storage issue was defined, and an ABE based on ciphertext that is completely secure was demonstrated. Yang and colleagues: Developed a CP-ABE system with revocable multiple- authority that achieves both forward and backward security They also introduced an attribute updating method for dynamic changes to attributes, including revoking and re-granting attributes.

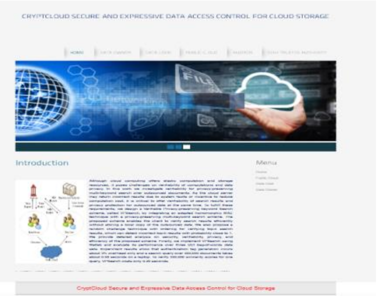
## 3. EXISTING SYSTEM

- Li et al. introduced the concept of accountable CP-ABE to prevent unauthorized key distribution among colluding users. In a subsequent work, they propose user accountable multi-authority CP-ABE system. Liu et al. also developed white-box and black-box traceability CP-ABE systems, supporting policy expressiveness in any monotone access structures.
- Ning et al. proposed several practical CP-ABE systems with white-box and black-box traceability. Deng et al. provided a tracing mechanism for CP-ABE to identify leaked access credentials in cloud storage systems.

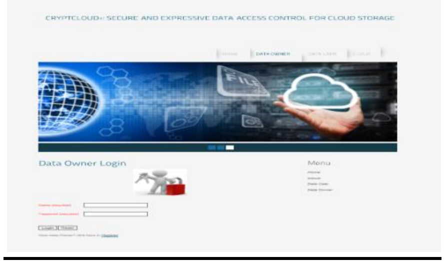
- Sahai et al. defined the problem of revocable storage and presented a fully secure construction for ABE based on ciphertext. Yang et al. proposed a revocable multi-authority CP-ABE system that achieves both forward and backward security. More recently, Yang et al. introduced an attribute updating method to enable dynamic changes to attributes, such as revoking previous attributes and re-granting previously revoked attributes.

## 4. RESULTS

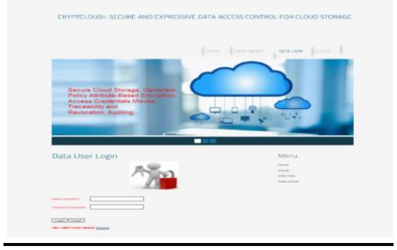
### Home Page:


CRYPTCLOUD SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE
HOME
Introduction
Menu
CryptCloud Secure and Expressive Data Access Control for Cloud Storage

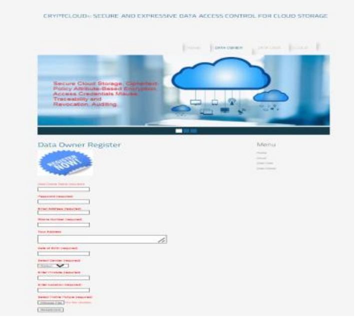
### DataOwner Login:


CRYPTCLOUD+: SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE
DATA OWNER
FILE
Data Owner Login
Menu

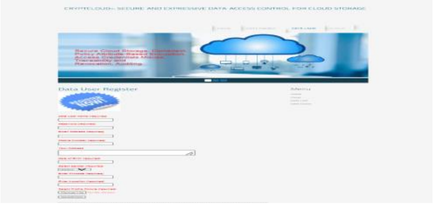
### Data User Login:


CRYPTCLOUD+: SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE
DATA USER
Secure Cloud Storage, Ciphertext-Policy Attribute-Based Encryption, Access Credentials Misuse, Traceability and Revocation, Auditing
Data User Login
Menu

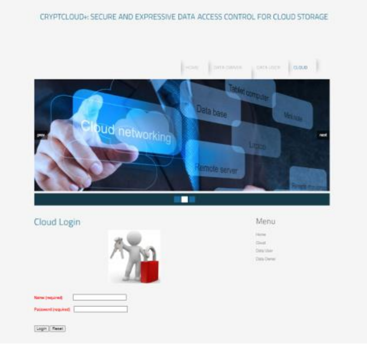
### Data Owner Registration:


CRYPTCLOUD+: SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE
DATA OWNER
Secure Cloud Storage, Ciphertext-Policy Attribute-Based Encryption, Access Credentials Misuse, Traceability and Revocation, Auditing
Data Owner Register
Menu

### Data User Registration:


CRYPTCLOUD+: SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE
DATA USER
Secure Cloud Storage, Ciphertext-Policy Attribute-Based Encryption, Access Credentials Misuse, Traceability and Revocation, Auditing
Data User Register
Menu

### Cloud Login:



CRYPTCLOUD+: SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE

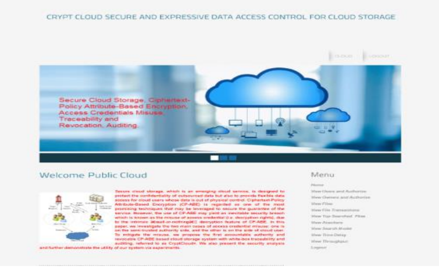
Cloud Login

Name (required)

Password (required)

Login Reset

## Dashboard:Cloud

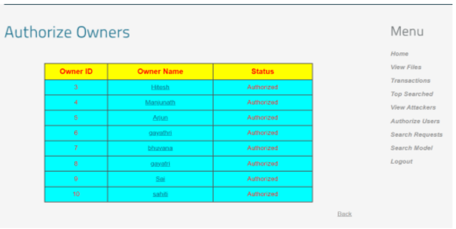


CRYPT CLOUD SECURE AND EXPRESSIVE DATA ACCESS CONTROL FOR CLOUD STORAGE

Welcome Public Cloud

Secure cloud storage, which is an emerging cloud service, is designed to protect the confidentiality of outsourced data but also to provide flexible data access for cloud users whose data is out of physical control. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques that may be leveraged to secure the guarantee of the service. However, the use of CP-ABE may yield an inevitable security breach which is known as the misuse of access credential (i.e. decryption rights), due to the intrinsic âœall-or-nothingâ€ decryption feature of CP-ABE. In this paper, we investigate the two main cases of access credential misuse: one is on the semi-trusted authority side, and the other is on the side of cloud user. To mitigate the misuse, we propose the first accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing, referred to as CryptCloud+. We also present the security analysis and further demonstrate the utility of our system via experiments.

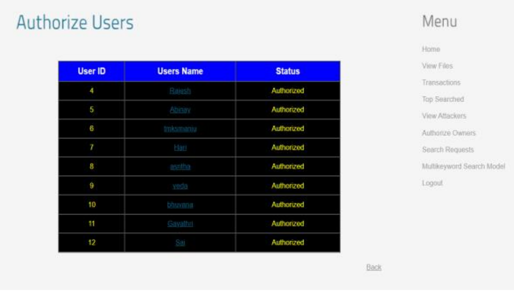
## Authorize Owners:



Authorize Owners

| Owner ID | Owner Name | Status |
|---|---|---|
| 3 | Hitesh | Authorized |
| 4 | Manjunath | Authorized |
| 5 | Arjun | Authorized |
| 6 | gayathri | Authorized |
| 7 | bhuvana | Authorized |
| 8 | gayatri | Authorized |
| 9 | Sai | Authorized |
| 10 | sahiti | Authorized |

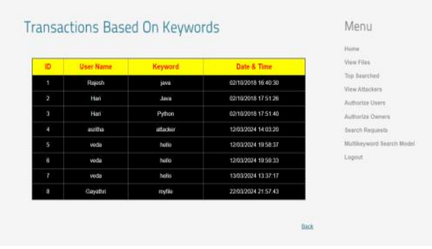
## Authorize Users:



Authorize Users

| User ID | Users Name | Status |
|---|---|---|
| 4 | Rajesh | Authorized |
| 5 | Abinay | Authorized |
| 6 | lmksmanju | Authorized |
| 7 | Hari | Authorized |
| 8 | asritha | Authorized |
| 9 | veda | Authorized |
| 10 | bhuvana | Authorized |
| 11 | Gayathri | Authorized |
| 12 | Sai | Authorized |

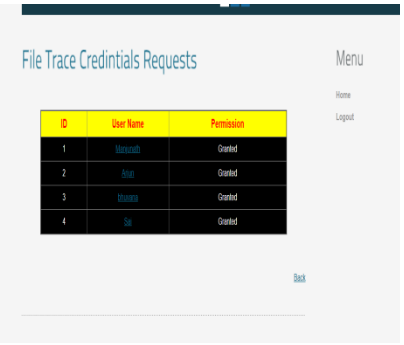
## Transactions:



Transactions Based On Keywords

| ID | User Name | Keyword | Date & Time |
|---|---|---|---|
| 1 | Rajesh | java | 02/10/2018 16:40:30 |
| 2 | Hari | Java | 02/10/2018 17:51:26 |
| 3 | Hari | Python | 02/10/2018 17:51:40 |
| 4 | asritha | attacker | 12/03/2024 14:03:20 |
| 5 | veda | hello | 12/03/2024 19:58:37 |
| 6 | veda | hello | 12/03/2024 19:59:33 |
| 7 | veda | hello | 13/03/2024 13:37:17 |
| 8 | Gayathri | myfile | 22/03/2024 21:57:43 |

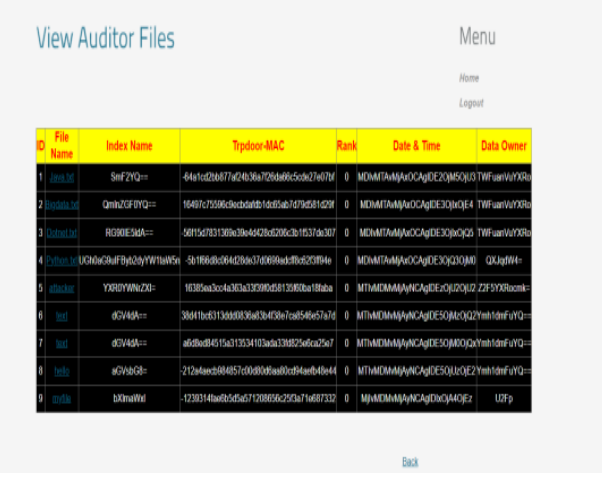
## File Trace Requests:



File Trace Credintials Requests

| ID | User Name | Permission |
|---|---|---|
| 1 | Manjunath | Granted |
| 2 | Arjun | Granted |
| 3 | bhuvana | Granted |
| 4 | Sai | Granted |

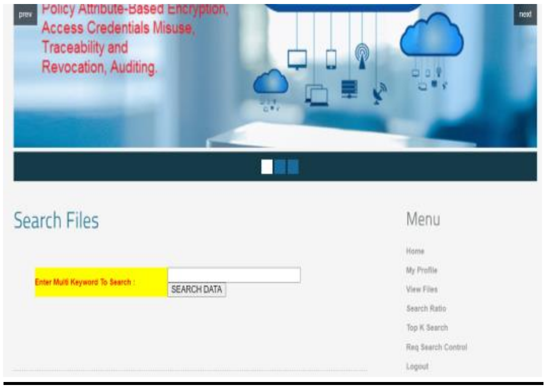
## Auditor View Files:



View Auditor Files

| ID | File Name | Index Name | Trpdoor-MAC | Rank | Date & Time | Data Owner |
|---|---|---|---|---|---|---|
| 1 | Java.txt | SmF2YQ== | -64a1cd2bb877af24b36a7f26da66c5cde27e07bf | 0 | MDIvMTAvMjAxOCAgIDE2OjM5OjU3 | TWFuanVuYXRo |
| 2 | Bigdata.txt | QmlnZGF0YQ== | 16497c75596c9ecbdafdb1dc65ab7d79d581d29f | 0 | MDIvMTAvMjAxOCAgIDE3OjIxOjE4 | TWFuanVuYXRo |
| 3 | Dotnet.txt | RG90IE5ldA== | -56f15d7831369e39e4d428c6206c3b1f537de307 | 0 | MDIvMTAvMjAxOCAgIDE3OjIxOjQ5 | TWFuanVuYXRo |
| 4 | Python.txt | UGl0aG9uIFByb2dyYW1taW5n | -5b1f66d8c064d28de37d0699adcff8c62f3ff94e | 0 | MDIvMTAvMjAxOCAgIDE3OjQ3OjM0 | QXJqdW4= |
| 5 | attacker | YXR0YWNrZXI= | 16385ea3cc4a363a33f39f0d58135f60ba18faba | 0 | MTIvMDMvMjAyNCAgIDEzOjU2OjU2 | Z2F5YXRocmk= |
| 6 | text | dGV4dA== | 38d41bc6313ddd0836a83b4f38e7ca8546e57a7d | 0 | MTIvMDMvMjAyNCAgIDE5OjMzOjQ2 | Ymh1dmFuYQ== |
| 7 | text | dGV4dA== | a6d8ed84515a313534103ada33fd825e6ca25e7 | 0 | MTIvMDMvMjAyNCAgIDE5OjM0OjQx | Ymh1dmFuYQ== |
| 8 | hello | aGVsbG8= | -212a4aecb884857c00d80d6aa80cd94aefb48e44 | 0 | MTIvMDMvMjAyNCAgIDE5OjUzOjE2 | Ymh1dmFuYQ== |
| 9 | myfile | bXlmaWxl | -1239314fae6b5d5a571208656c25f3a71e687332 | 0 | MjIvMDMvMjAyNCAgIDIxOjA4OjEz | U2Fp |

## Search Files:

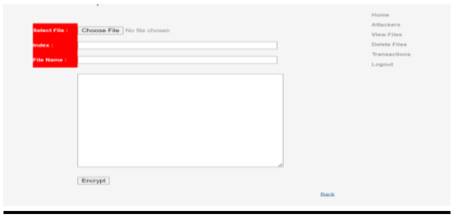


Search Files

Enter Multi Keyword To Search :

SEARCH DATA

### Upload a File:



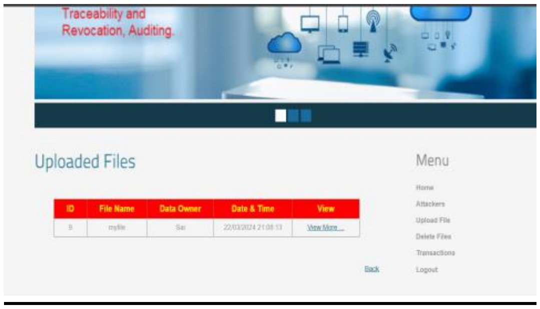
Select File : Choose File No file chosen

Index :

File Name :

Encrypt

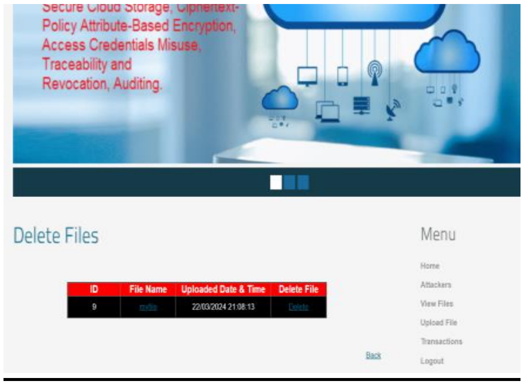
### View Uploaded Files:



Uploaded Files

| ID | File Name | Data Owner | Date & Time | View |
|---|---|---|---|---|
| 9 | myfile | Sai | 22/03/2024 21:08:13 | View More... |

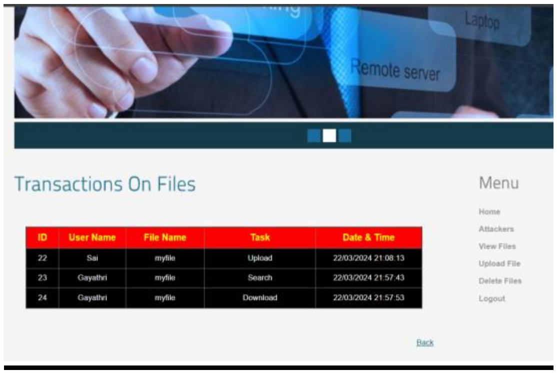
### Delete Files:



Delete Files

| ID | File Name | Uploaded Date & Time | Delete File |
|---|---|---|---|
| 9 | myfile | 22/03/2024 21:08:13 | Delete |

### View Transactions on Files:



Transactions On Files

| ID | User Name | File Name | Task | Date & Time |
|---|---|---|---|---|
| 22 | Sai | myfile | Upload | 22/03/2024 21:08:13 |
| 23 | Gayathri | myfile | Search | 22/03/2024 21:57:43 |
| 24 | Gayathri | myfile | Download | 22/03/2024 21:57:53 |

## 5. CONCLUSION

CryptCloud+ is a system designed to enhance the security of cloud storage systems utilizing CP-ABE encryption. CP-ABE encrypts data with policies based on attributes like user roles or data sensitivity, but it can be vulnerable to credential leakage. CryptCloud+ tackles this by offering white-box traceability, allowing the system to trace and revoke access from malicious users who leak credentials. This ensures that even if a user's credentials are redistributed by a semi-trusted authority, their access can still be revoked. CryptCloud+ also introduces the concept of an accountable authority, holding access authorities responsible and preventing unauthorized access. Additionally, it includes auditing capabilities to monitor access authority activities and enable effective revocation of access rights if misuse is detected. These features collectively provide a robust solution for secure data access control in cloud storage systems.

## 6. REFERENCE

- Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.

- Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.

- Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.

- Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

- Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In Advances in Cryptology-CRYPTO’92, pages 390–420. Springer, 1993.

- Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.