Accountable Privacy Preserving with Attribute-Based Encryption for Cloud storage

Team Members: DUDDELA MUKESH
BOGGALA NAVEEN KUMAR REDDY
BADDULA SURESH
VOODI NARENDRA
KAMMARI LALITH KUMAR

Guide: Uma Maheshwari R

edunet foundation

OUTLINE

- Abstract
- Problem Statement
- Aims, Objective & Proposed System/Solution
- System Design/Architecture
- System Development Approach (Technology Used)
- Algorithm & Deployment
- Conclusion
- Future Scope
- References
- Images of the Project

Abstract

In the current cloud storage, Issues with access control and data security must be resolved immediately. Since it enables dynamic access control over encrypted data, multi-authority attribute-based encryption (MA-ABE) is viewed as a viable remedy for data access control security issues in the dynamic Internet of things.

But the current issue with key abuse is seriously undermining MA-ABE's security access control. Only a single authority and a small universe of attributes (users) are supported by the current accountable attribute-based encryption systems. Furthermore, they oppose revocation. Because they are built in the composite order bilinear group, some techniques are inefficient. The author of this paper suggests the first vast universe decentralized accountability system. Multi-authority attribute-based encryption scheme with outsourcing decryption based on prime order bilinear groups.

The proposed scheme allows for the dynamic capacity expansion of attributes, users, and authorities. An audit mechanism is given to judge if the suspicious key was leaked by a malicious user or by authorities and to determine the identity of the leaker.

The malicious user who divulges key can be punished by user-attribute revocation. The revocation mechanism is resistant to collusion attacks undertaken by revoked users and non-revoked users. Meanwhile, it satisfies the requirements of forward and backward security. To save resources, the outsourced decryption module is optional for users with restricted resources. According to the results of the performance analysis, it is suited for large-scale cross-domain cooperation in the dynamic cloud storage.

we extend the offer mentioned proposed system with a Ciphertext Policy Attribute Based Encryption (CP-ABE) scheme with accountability to address the security and privacy issues

Problem statement

In the real world of cloud computing, data sharing among groups demands robust security mechanisms to safeguard sensitive information. Multi Authority Attribute Based Encryption presents apromising approach for securing data in cloud environments, offering convenience and flexibility in key management and for reducing the storage cost.

edunet foundation

Aim and Objective

Aim:

The aim of the study is to enhance the security of accessing and uploading files in cloud computing environments through the implementation of Multi Authority Attribute-Based Encryption(MA-ABE) mechanisms.

Objectives:

- **Privacy Preservation**: The primary objective of AP-ABE is to preserve the privacy of sensitive data. It ensures that only authorized users with the necessary attributes can decrypt and access the encrypted data.

- **Multi-Attribute Access Control**: AP-ABE allows access control based on multiple attributes associated with users and data. This enables fine-grained access control, where access decisions can be based on various user attributes and policies.
- **Revocation and Key Management**: AP-ABE schemes often include mechanisms for user revocation and key management. This ensures that access privileges can be revoked or updated dynamically, as well as managing the distribution and update of keys.

edunet foundation

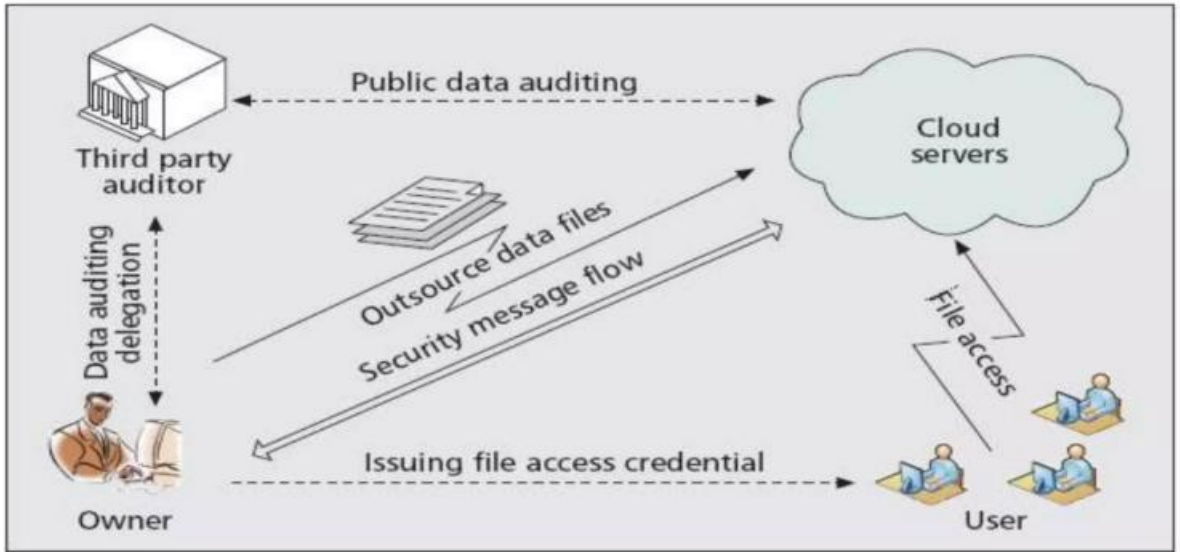
Proposed Solution

- The traceable multi-authority ABE and accountable multi-authority ABE is proposed as MA-CP-ABE scheme, which allows tracing the identity of a misbehaving user who leaked the decryption key to others.
- Proposed the first accountable authority CP-ABE with white-box traceability that provides an auditor to judge publicly whether a suspected user is guilty.
- The proposed scheme supports the dynamic capacity expansion of attributes, users, and authorities.
- It is suitable for large-scale multi-domain collaboration in the dynamic cloud.

- The proposed scheme provides an audit mechanism to judge whether a malicious user or authorities leak the suspicious key, and to determine the integrity of the content.
- The revocation mechanism is secure against the collusion attack launched by revoked users and non-revoked users. Meanwhile, it meets the requirements of forward and backward security.
- De-duplication identifies the repeated content and compress the storage system, which leads to consume less storage.
- The limited-resource user can choose to outsource decryption for saving resources. The performance analysis results indicate that the proposed scheme is more efficient and suitable for the cloud

edunet foundation

System Architecture


Public data auditing
Third party auditor
Cloud servers
Outsource data files
Security message flow
Data auditing delegation
File access
Issuing file access credential
Owner
User

edunet foundation

System Deployment Approach

Technologies are used:

- **Frontend:** HTML, CSS, JavaScript.
- **Backend:** Mysql
- **Web Server:** Tomcat Server.

edunet foundation

Algorithm & Deployment

Algorithm:

Input:

GM_{em}-> Group Member

GM_{an}-> Group Manager

CS-> Cloud Server

Output:

Result-> R

Step 1: **GM_{em}** register, login and upload files

Step 2: **GMs**view files which uploaded

Step 3: **GM_{em}**-> (req.) GMkey from **GM_{an}**

Step 4: **GM_{an}**generates key **->GM_{em}**

Step 5: **GM_{em}**<-(reci.)**GM_{an}**key **->**(req.) **CS**

Step 6: **CS** -> (send) cloud key **->GM_{em}**

Step 7: KAC encrypt all files

Step 8: **GM_{em}**access user files

Step 9: **GM_{em}**decrypt files using **KAC**

Step 10: **GM_{em}**get **R**

Deployment Steps:

1. Planning and Requirement Analysis: Define the specific requirements and objectives forgroup data sharing in the cloud using Attribute Based Encryption. Identify the target user groups, types of data to be shared, and access control policies.

2. Installation and Configuration: Install the necessary software components for implementing Identity-Based Encryption and group data sharing functionality. Configure the encryption algorithms, access control policies, and integration with cloud storage services.

3. Identity Management Configuration: Configure the identity management module tomanage user identities and attributes effectively. Set up user registration processes, authentication mechanisms, and attribute-based access control policies.

4. Key Management Setup: Establish the key management and distribution module to generate, distribute, and manage encryption keys for group data sharing. Implement mechanisms for key generation, distribution, revocation, and updates based on group membership changes.

5. Access Control Configuration: Configure the access control module to enforce fine-grainedaccess policies for shared data within the group. Define access control rules based on user

roles, attributes, and group memberships, ensuring that only authorized users can access specific data.

6. Encryption and Decryption Configuration: Configure the encryption and decryption engineto encrypt data using Multi Attribute-Based Encryption techniques. Implement encryption

edunet foundation

Conclusion

The first accountable and revocable large universe multi-authority attribute-based encryption scheme with outsourcing decryption based on prime order bilinear groups. An audit mechanism is given to judge if the suspicious key was leaked by a malicious user or by authorities and to determine the identity of the leaker. The malicious user who divulges key can be punished by user-attribute revocation. The revocation mechanism is resistant to collusion attacks undertaken by revoked users and non-revoked users. Meanwhile, it satisfies the requirements of forward and backward security. The proposed scheme is static security in the random oracle model. To save resources, the outsourced decryption module is optional for users with restricted resources. According to the results of the performance analysis, it is suited for large-scale cross-domain cooperation in the cloud.

edunet foundation

Future Scope

The system can be made more flexible and scalable using these recommendations. Please note that the system implemented here is just a prototype of idea presented via this project. The proposed scheme is static security in the random oracle model. To save resources, the outsourced decryption module is optional for users with restricted resources. According to the results of the performance analysis, it is suited for large-scale cross-domain cooperation in the dynamic cloud-aided IoT. However, the author considers improving the scheme for security without the random oracle model and more efficiency in future work.

edunet foundation

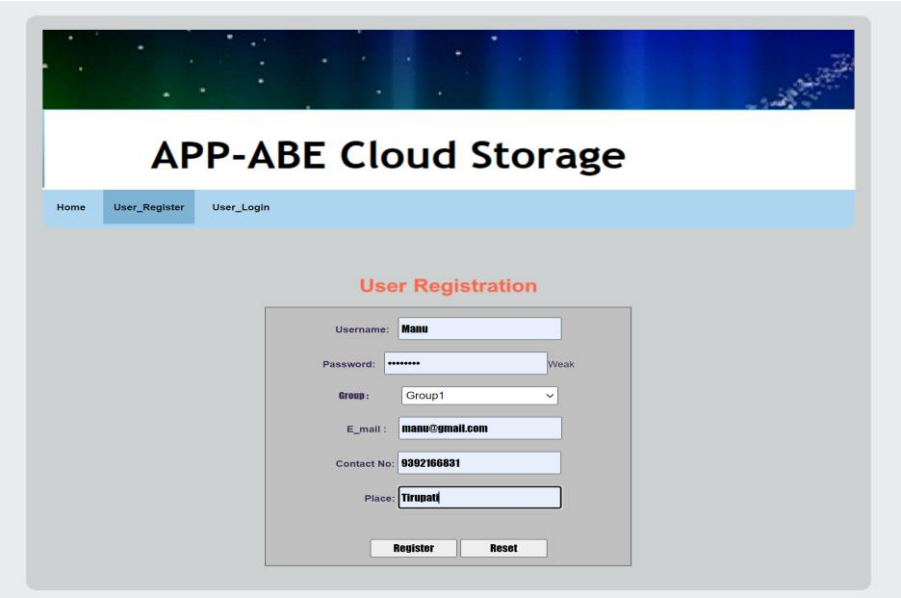
References

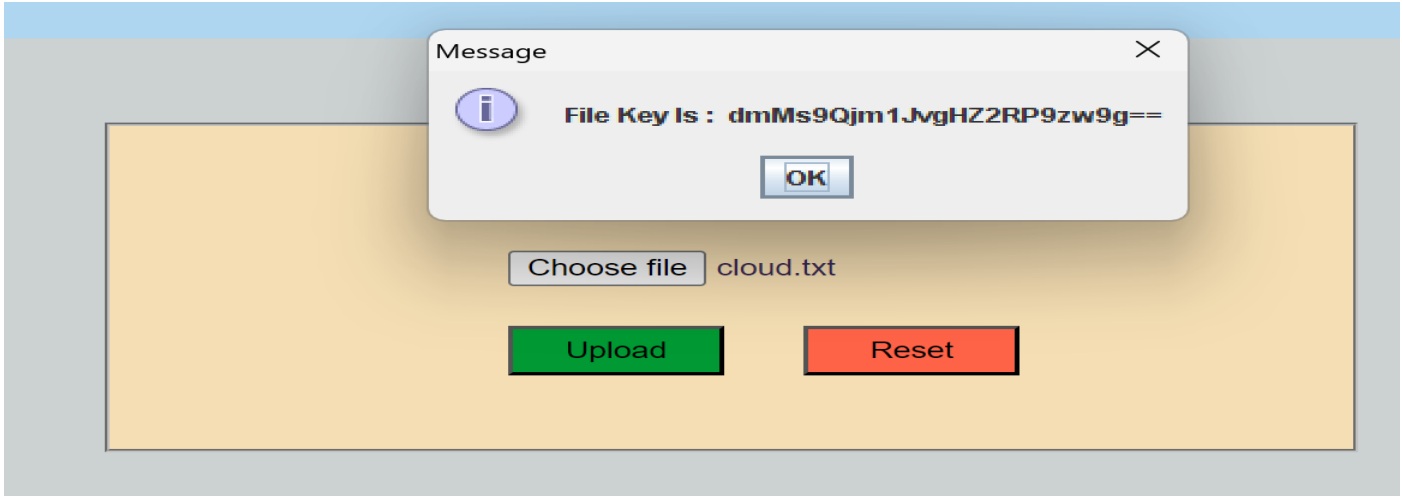
1. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh, and D. Wang, ‘‘Attribute based encryption with privacy protection and accountability for CloudIoT,’’ IEEE Trans. Cloud Comput., early access, Feb. 19, 2020, doi: 10.1109/TCC.2020.2975184.

2. J. Li, Q. Huang, X. Chen, S. S. M. Chow, D. S. Wong, and D. Xie, ‘‘Multiauthority ciphertext-policy attribute-based encryption with accountability,’’ in Proc. 6th ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS), 2011, pp. 386–390..

3. N. Chen, J. Li, Y. Zhang, and Y. Guo, ‘‘Efficient CP-ABE scheme with shared decryption in cloud storage,’’ IEEE Trans. Comput., early access, Dec. 14, 2020.

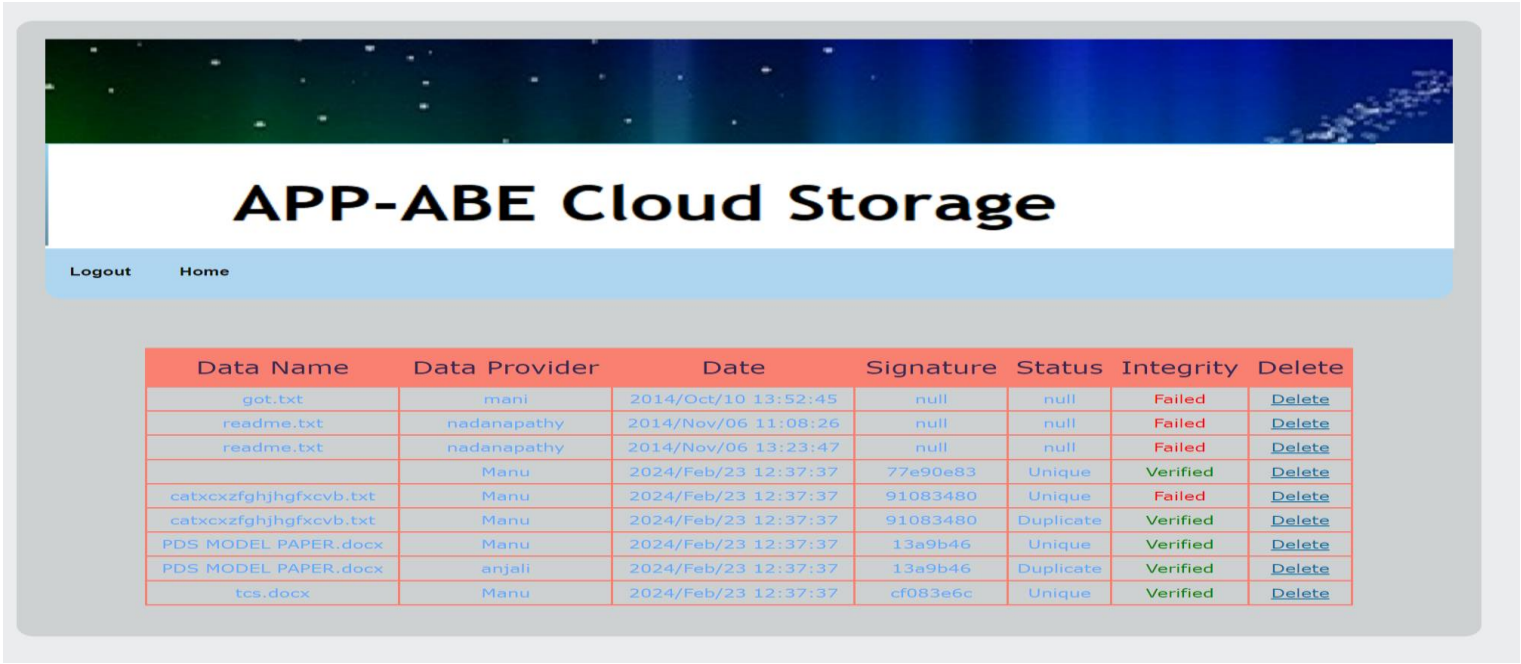
Outputs:


APP-ABE Cloud Storage
Home
User_Register
User_Login
User Registration
Username:
Manu
Password:
Weak
Group :
Group1
E_mail :
manu@gmail.com
Contact No:
9392166831
Place:
Tirupati
Register
Reset


Message
File Key Is : dmMs9Qjm1JvgHZ2RP9zw9g==
OK
Choose file
cloud.txt
Upload
Reset

edunet foundation

Data File Name	Date & Time	View
got.txt	2014/Oct/10 13:52:45	View
readme.txt	2014/Nov/06 11:08:26	View
readme.txt	2014/Nov/06 13:23:47	View
	2024/Feb/23 12:37:37	View
catxcxzfghjhgfxcvb.txt	2024/Feb/23 12:37:37	View
catxcxzfghjhgfxcvb.txt	2024/Feb/23 12:37:37	View
PDS MODEL PAPER.docx	2024/Feb/23 12:37:37	View
PDS MODEL PAPER.docx	2024/Feb/23 12:37:37	View
tcs.docx	2024/Feb/23 12:37:37	View
cloud.txt	2024/Feb/23 16:30:10	View



Data Name	Data Provider	Date	Signature	Status	Integrity	Delete
got.txt	mani	2014/Oct/10 13:52:45	null	null	Failed	Delete
readme.txt	nadanapathy	2014/Nov/06 11:08:26	null	null	Failed	Delete
readme.txt	nadanapathy	2014/Nov/06 13:23:47	null	null	Failed	Delete
	Manu	2024/Feb/23 12:37:37	77e90e83	Unique	Verified	Delete
catxcxzfghjhgfxcvb.txt	Manu	2024/Feb/23 12:37:37	91083480	Unique	Failed	Delete
catxcxzfghjhgfxcvb.txt	Manu	2024/Feb/23 12:37:37	91083480	Duplicate	Verified	Delete
PDS MODEL PAPER.docx	Manu	2024/Feb/23 12:37:37	13a9b46	Unique	Verified	Delete
PDS MODEL PAPER.docx	anjali	2024/Feb/23 12:37:37	13a9b46	Duplicate	Verified	Delete
tcs.docx	Manu	2024/Feb/23 12:37:37	cf083e6c	Unique	Verified	Delete

edunet foundation

GITHUB

https://github.com/Mukesh-developer83/Accountable-privacy-preserving-with-attribute-based-encryption

VIDEO LINK

https://drive.google.com/file/d/16KwM70GJYWa2m6ZRmscbKHpN59LJVaN2/view?usp=drive_link

Thank you!