A Seminar on

Revocable Multi-Authority Attribute-Based Encryption with Time Based Authority

Team Details

1. K V Sai Srujan(20EG105304)
2. J Nikhil Anand(20EG105318)
3. Mahmood Ali Khan(20EG105329)

Project Supervisor
Mrs. P. Swarajya Lakshmi
Assistant Professor

Introduction

- Cloud storage is used to store massive data, so more and more individuals and organizations shift their data from local computers to cloud. However, this new model poses a serious threat to the privacy of their owners, since the data might be accessed and analyzed by the cloud server providers for illegal or monetary purposes.

- To solve this problem, people have figured out a variety of approaches. One common way is to use the traditional public key encryption technology to encrypt data, but the data owners fail to have fine-grained access to their data flexibly.

- Then many single-authority attribute-based encryption schemes have been put forward. In these schemes, it is required that only one trusted attribute authority administers the attributes and distributes the corresponding secret keys of attributes to the data consumers.This mechanism may not meet the practical requirements in cloud storage because scaling the system might be challenging, especially if there is a need for a large number of attributes or users

1. **What it is:**

Revocable Multi-Authority Attribute-Based Encryption with Time-Based Authority (RMA-ABE-TBA) is a cryptographic scheme that combines several principles to provide advanced access control and secure data sharing.Here's a breakdown of its key components.

- Attribute-Based Encryption (ABE)
- Multi-Authority
- Time-Based Authority
- Revocability
-

2. **What is Needed:**

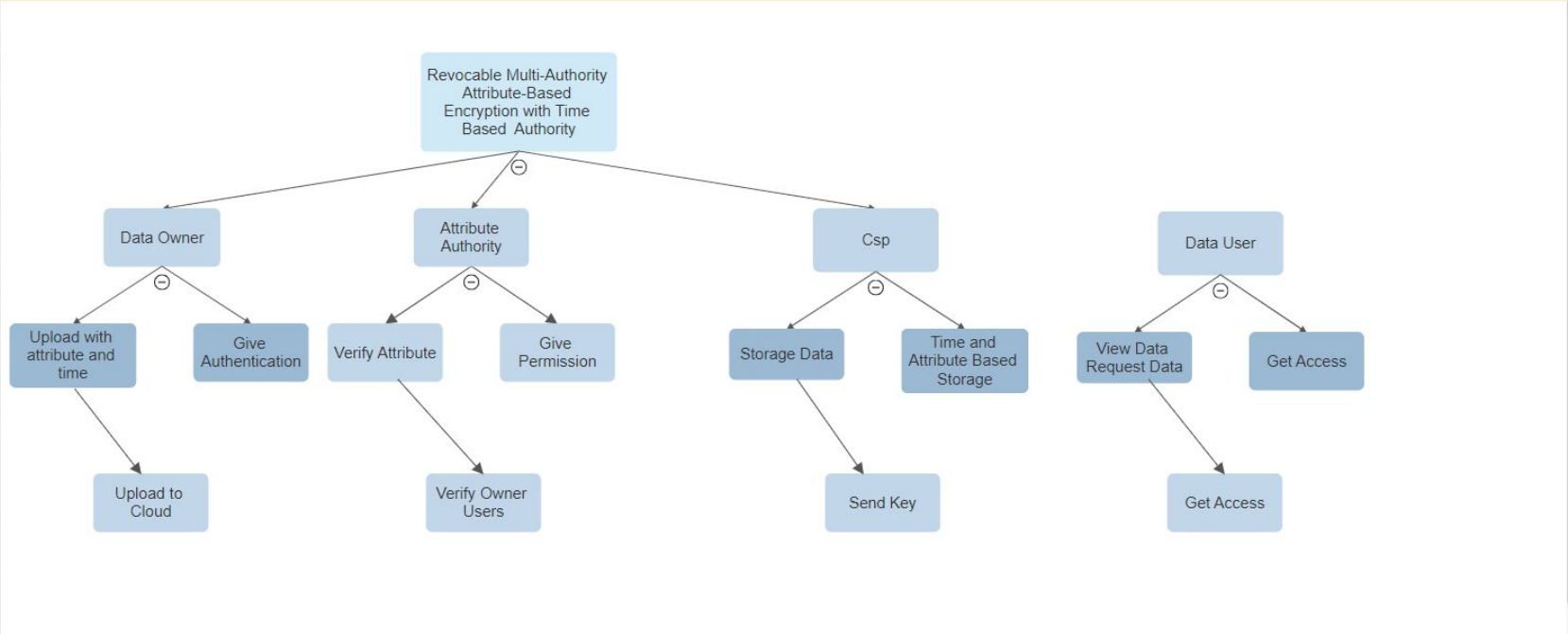
For the implementation of Revocable Multi-Authority Attribute-Based Encryption with Time-Based Authority, the following components and considerations are typically required:

- Multiple Authorities
- User Attributes
- Time Constraints
- Secure Communication Channels

3. Applications:

- Cloud Computing
- Communication Systems
- Data Sharing Platforms
- Healthcare Systems
- Financial Systems
- Government and Defense

Concept Tree



Literature

Author(s)	Strategies	Advantages	Disadvantages
Chunpeng Ge; Willy Susilo; Joonsang Baek; Zhe Liu; Jinyue Xia; Liming Fang.	Revocable ABE	Users can share data without leaving traces or revealing their identities.	Designing and implementing such a scheme can be complex, requiring expertise in cryptography, secure systems design
Vipul Goyal,Omkant Pandey,Amit Sahai ,Brent Waters	Key-Policy Attribute-Based Encryption (KP-ABE)	Users can selectively share encrypted data based on specific attributes, providing a granular control over who can access the information	As the number of users and attributes increases, managing and scaling the system becomes more challenging
K. Sethi, A.Pradhan, and P. Bera	Traceable multi-authority CP-ABE	Improve efficiency and expressiveness of our system.	This may potentially lead to exposure of decryption keys by some malicious users

Author(s)	Methods	Advantages	Disadvantages
J. Li, X. Lin, Y. Zhang, and J. Han	A secure and efficient outsourced computation on data sharing scheme for privacy computing	It introduces a keyword search function, allowing for efficient querying of encrypted data stored in the cloud without revealing the plaintext	The outsourced computation relies on the CSP, and the efficiency and security of the system are contingent on the trustworthiness and reliability of the CSP.
Q. Xu, C. Tan, W. Zhu, Y. Xiao, Z. Fan, and F. Cheng	The decentralized Attribute-Based Keyword Search (ABKS) scheme for cloud storage prioritizes security and privacy by outsourcing costly decryption operations to the cloud	The scheme is designed to handle access policies involving attributes or credentials across different trust domains and organizations	The incorporation of decentralized architecture and advanced cryptographic techniques may introduce complexity to the implementation
S. Ding, C. Li, and H. Li	A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT	The scheme is explicitly designed with the limitations and requirements of IoT devices in mind. This IoT-focused design increases the practical applicability of the scheme in real-world scenarios	The process of key generation in cryptographic schemes often involves complex operations. Depending on the specifics of the PF-CP-ABE scheme, key generation could introduce computational overhead

Problem Statement

In many contemporary data-sharing scenarios, ensuring secure and dynamic access control poses a significant challenge. Traditional access control mechanisms may fall short in providing the necessary flexibility, especially when dealing with complex and evolving user roles, attributes, and temporal constraints. Revocable Multi-Authority Attribute-Based Encryption with Time-Based Authority (RMA-ABE-TBA) is an advanced cryptographic scheme that addresses the need for secure and flexible data access control in various applications. This encryption method combines the benefits of attribute-based encryption (ABE) and revocable multi-authority to provide a robust solution for managing access to sensitive information.

Problem Illustration

To illustrate the problems addressed by our proposed Revocable Multi-Authority Attribute-Based Encryption with Time-Based Authority (RMA-ABE-TBA), let's consider a scenario in a cloud-based healthcare system. In this system, patient records are stored securely, and access is granted based on attributes such as medical specialty, role, and time sensitivity.

Scenario:

Scalability Challenge:

- Issue: The healthcare system involves numerous attributes, including medical specialty, patient status, and treatment type. As the number of attributes grows, traditional attribute-based encryption struggles to efficiently manage and scale access policies.
- Illustration: A doctor specializing in multiple areas requires access to patient records based on various attributes. The sheer number of attributes associated with different medical specialties complicates the access control system, leading to performance bottlenecks and increased computational overhead.

Revocation Inefficiency:

- Issue: In a multi-authority setting, revoking access rights in real-time can be inefficient and prone to delays. This is particularly critical in healthcare scenarios where immediate access changes are crucial for patient privacy and security.
- Illustration: When a doctor resigns or changes their medical specialty, the traditional revocation process may take time to update. During this delay, the doctor might retain access to patient records that are no longer within their professional scope, posing a potential security risk.

Integration of Time-Based Authorities:

- Issue: Integrating time-based authorities seamlessly into existing encryption schemes is often a challenge. Failure to synchronize time-based access control can lead to discrepancies, jeopardizing the security and privacy of sensitive information.
- Illustration: A healthcare system may require time-sensitive access to certain patient records based on treatment plans. Without effective integration of time-based authorities, there may be difficulties ensuring that access privileges are granted or revoked at the correct times, compromising the system's overall reliability.

Proposed Method

The proposed method, Revocable Multi-Authority Attribute-Based Encryption with Time-Based Authority, tackles challenges in secure access control for cloud storage. Using a Multi-Authority Attribute-Based Encryption framework, it introduces a novel time-based authority for dynamic access management. This approach allows authorities to adapt access policies to changing user roles. Notably, the scheme's revocable access control accommodates seamless adjustments, crucial for dynamic and collaborative environments. Positioned as a forward-looking solution, it addresses the evolving landscape of cloud computing, emphasizing dynamic access control and practical adaptability for enhanced security in cloud storage systems.

Proposed Method Illustration

The proposed method, called Revocable Multi-Authority Attribute-Based Encryption with Time-Based Authority, introduces a new way to control access securely in cloud storage systems. Imagine a system where a central cloud server manages access, and different authorities are responsible for granting access based on specific attributes.Now, the innovation here is the addition of a time-based authority, meaning that access privileges can change dynamically over time.The workflow involves setting up attributes, granting user access, managing access based on time, and efficiently revoking access when needed.

Workflow:

Attribute Setup:

- Authorities define initial attributes and associated time periods.

User Access:

- Users gain access to specific data based on their attributes and the current time period.

Time-Based Authority:

- Authorities dynamically manage access privileges over time, adapting to changing user roles.

Revocation:

- Revocation process is visually represented, showcasing the efficient removal of access privileges when needed.

Parameter

The proposed scheme Revocable Multi-Authority Attribute-Based Encryption with Time-Based Authority embraces few entities: attribute authorities (AAs), cloud service provider (CSP), data owner (DO) and data consumer (DC)

- DC Reg($info_{DC}$)→ uid. Using the DC's information $info_{DC}$(e.g., name, birthday etc.) as input, and the identity uid as output. *DC*
- AA Reg($info_{AA}$)→aid. With AA's information $info_{AA}$ as input, and identity aid as output.

- **Data encryption**: Encrypt((M, ρ),{APK_{aidk}}aidk ∈ I_A , m)→CT. The Final Output is CT
- **Data decryption**: Decrypt(CT ,{$SK_{uid,aidk}$ }$_{aidk \in IA}$)→m. The Final Output is data m
- **Time attribute access control**: A real-time attribute is an attribute whose values depend on time ti∈T. In our model, availability of a resource time (ti) environment for a subject determined based on the real-time attributes attr (x, ti),x ∈{s, o, e},with values in a linearly ordered set of availability labels
  L={`m=hi º`m−1º. . . º`1=lo}
  The availability label of attr(x, ti)is called priority when x is a subject, congestion when x is an object, and criticality when x is the environment. Availability labels are dynamically determined based on user events, the context of the requested service and system events.
- **Secret key generation**: This phase is composed of the SKeyGen algorithm.
  SKeyGen(ASK_{aid} ,$S_{uid,aid}$,{{VK_{xaid}}$_{xaid \in Suid,aid}$)→ $SK_{uid,aid.}$.Generates the secret key $SK_{uid,aid}$

Attribute revocation: This phase consists of three algorithms: UKeyGen, SKUpdate and CT Update.

- U KeyGen(ASK_{aid} ,$\bar{x}_{aid}$, $VK^{-}x_{aid}$) → $\bar{V}\bar{K}^{-}x_{aid}$, $UK^{-}x_{aid}$
- SK Update($SK_{uid,aid}$, $UK^{-}x_{aid}$) → $\bar{S}\bar{K}_{uid,aid}$
- CT Update(CT, UK)→$\bar{C}\bar{T}$.

Experiment Environment

SOFTWARE REQUIREMENTS:

- Operating system : Windows XP/7/10.
- Coding Language : Java
- Tool : Netbeans
- Database : MYSQL

HARDWARE REQUIREMENTS:

- System : i5 10 Gen
- Hard Disk : 512GB.
- Ram : 16 GB.

Project status

S.No	Functionality	Status (Completed /in-progress/Not started)
1	Literature Survey	Completed
2	Problem Definition	Completed
3	Module Design	in-progress
4	Implementation	in-progress

References

[1] Revocable Attribute-Based Encryption With Data Integrity in Clouds. Chunpeng Ge; Willy Susilo; Joonsang Baek; Zhe Liu; Jinyue Xia; Liming Fang. IEEE(2021)

[2] Vipul Goyal,Omkant Pandey, Amit Sahai, Brent Waters, “Attribute-based encryption for fine-grained access control of encrypted data”,Oct.2006.

[3] K. Sethi, A. Pradhan, and P. Bera, “Practical traceable multi-authority CP-ABE with outsourcing decryption and access policy updation,” Journal ofInformation Security and Applications, vol. 51, pp. 102435-102450, Apr.2020

[4] Q. Xu, C. Tan, W. Zhu, Y. Xiao, Z. Fan, and F. Cheng, “Decentralized Attribute-based conjunctive keyword search scheme with online/offlineencryption and outsource decryption for cloud computing,” Future Gen-eration Computer Systems, vol. 97, pp. 306-326, Mar. 2019

[5] S.Ding, C. Li, and H. Li, “A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT,” IEEE Access, vol. 6, pp. 27336- 27345, May. 2018

[6] J. Li, X. Lin, Y. Zhang, and J. Han, “KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage,” IEEET. Ser. Comput., vol. 10, no. 5, pp. 715-725, Dec. 2017

Thank you

Project seminar–I Evaluation

S.No	Rubrics	Marks
1	Concept Introduction	4
2	Literature and Parameter	5
3	Problem and Problem Illustration	8
4	Proposed Method and Illustration	8
Total		25