Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage

T. Venkateswara Rao¹, V Pradeep²
¹M.Tech Student, Dept of CSE, Nova’s Institute of Technology, Eluru, West Godavari-534447, A. P., India
²Assistant Professor, Dept of CSE, Nova’s Institute of Technology, Eluru, West Godavari-534447, A. P., India

Abstract: Data access control is an efficient way to make sure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results demonstrate that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

Index Terms: Access control, multi-authority, CP-ABE, attribute revocation, cloud storage

INTRODUCTION

CLOUD storage is an vital service of cloud computing, which offers services for data owners to host their data in the cloud. This new model of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer depend on servers to do access control. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. The authority can be the registration office in a university, the human resource department in a company, etc. The data owner defines the access policies and encrypts data according to the policies. Each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies. There are two types of CP-ABE systems: single-authority CP-ABE where all attributes are managed by a single authority, and multi-authority CP-ABE where attributes are from different domains and managed by different authorities. Multi-authority CP-ABE is more appropriate for data access control of cloud storage systems, as users may hold attributes issued by multiple authorities and data owners may also share the data using access policy defined over attributes from different authorities. For example, in an E-health system, data owners may share the data using the access policy "Doctor AND Researcher", where the attribute "Doctor" is issued by a medical organization and the attribute "Researcher" is issued by the administrators of a clinical trial. However, it is difficult to directly apply these multi-authority CP-ABE schemes to multi-authority cloud storage systems because of the attribute revocation problem. In multi-authority cloud storage systems, users’ attributes can be changed dynamically. A user may be entitled some new attributes or revoked some current attributes. And his permission of data access should be changed accordingly. However, existing attribute revocation methods either rely on a trusted server or lack of efficiency, they are not suitable for trade with the attribute revocation problem in data access control in multi-authority cloud storage systems. In this paper, we first propose a revocable multi-authority CP-ABE scheme, where an efficient and secure revocation method is proposed to resolve the attribute revocation problem in the system. Our attribute revocation system is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt) and forward security (The newly joined user can also decrypt the previously published ciphertexts). Compared to the conference version of this work, we have the following improvements: 1. We modify the framework of the scheme and make it more practical to cloud storage systems, in which data owners are not involved in the key generation. Specifically, a user’s secret key is not related to the owner’s key, such that each user only needs to hold one secret key from each authority instead of multiple secret keys associated to multiple owners. 2. We greatly improve the efficiency of the attribute revocation method. Specifically, in our new attribute revocation method, only the ciphertexts that associated with the revoked attribute needs to be updated, while in, all the ciphertexts that associated...
with any attribute from the authority (corresponding to the revoked attribute) should be updated. Moreover, in our new attribute revocation method, both the key and the ciphertext can be updated by using the same update key, instead of requiring the owner to generate an update information for each ciphertext, such that owners are not required to store each random number generated during the encryption. We also highly improve the expressiveness of our access control scheme, where we remove the limitation that each attribute can only appear at most once in a ciphertext.

RELATED WORK
Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a technique that is designed for access control of encrypted data. There are two types of CP-ABE systems: single authority CP-ABE where all attributes are managed by a single authority, and multi-authority CP-ABE where attributes are from different domains and managed by different authorities. Multi-authority CP-ABE is more appropriate for the access control of cloud storage systems, as users may hold attributes issued by multiple authorities and the data owners may share the data using access policy defined over attributes from different authorities. However, due to the attribute revocation problem, these multi-authority CP-ABE schemes cannot be directly applied to data access control for such multi-authority cloud storage systems. To achieve revocation on attribute level, some re-encryption-based attribute revocation schemes are proposed by relying on a trusted server. We know that the cloud server cannot be fully trusted by data owners, thus traditional attribute revocation methods are no longer suitable for cloud storage systems. Ruj, Nayak and Ivan proposed a DACC scheme where an attribute revocation method is presented for the Lewko and Waters’ decentralized ABE scheme. Their attribute revocation method does not require a fully trusted server. But, it incurs a heavy communication cost since it requires the data owner to transmit a new ciphertext component to every non-revoked user. Key Generation, Data Encryption, Data Decryption and Attribute Revocation

SYSTEM ANALYSIS
EXISTING SYSTEM: This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution.

DISADVANTAGES OF EXISTING SYSTEM: Chase’s multi-authority CP-ABE protocol allows the central authority to decrypt all the ciphertexts, since it holds the master key of the system. Chase’s protocol does not support attribute revocation.

PROPOSED SYSTEM: In this paper, we first propose a revocable multi-authority CP-ABE scheme, where an efficient and secure revocation method is proposed to resolve the attribute revocation problem in the system. Our attribute revocation system is efficient in the sense that it incurs less communication cost and computation cost, and is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new ciphertext that requires the revoked attribute to decrypt) and forward security (The newly joined user can also decrypt the previously published ciphertexts if it has sufficient attributes). Our scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semitrusted in some scenarios, our scheme can still guarantee the backward security. Then, we apply our proposed revocable multi-authority CP-ABE scheme as the underlying techniques to build the expressive and secure data access control scheme for multi-authority cloud storage systems.

ADVANTAGES OF PROPOSED SYSTEM: We modify the framework of the scheme and make it more practical to cloud storage systems, in which data owners are not involved in the key generation. We greatly improve the efficiency of the attribute revocation method. We also highly improve the expressiveness of our access control scheme, where we remove the limitation that each attribute can only appear at most once in a ciphertext.

SYSTEM ARCHITECTURE:
DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data generated by the system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

DATA FLOW DIAGRAM:

- **Registration**
  - **Login**
    - **CA**
      - send key
    - **Admin**
      - send file
    - **File Encrypt**
    - **User**
      - receive secretkey
    - **File Upload**
      - enter filename and secretkey
    - **View files**
      - download file

However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity.

**Attribute Authorities:** Every AA is an independent attribute authority that is responsible for entitling and revoking user’s attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key for each user reflecting his/her attributes.

**Data Consumers:** Each user has a global identity in the system. A user may be entitled a set of attributes which may come from multiple attribute authorities. The user will receive a secret key associated with its attributes entitled by the corresponding attribute authorities.

**Data Owners:** Each owner first divides the data into several components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies.

**Cloud Server:** Then, the owner sends the encrypted data to the cloud server together with the ciphertexts. They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user’s attributes satisfy the access policy defined in the cipher text; the user is able to decrypt the cipher text. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data.

**INPUT DESIGN**

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy.

Input Design considered the following things:
- What data should be given as input?
- How the data should be arranged or coded?
The dialog to guide the operating personnel in providing input.
Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system. It is achieved by creating user-friendly screens for information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maze of instant. Thus the objective of input design is to create an input layout that is easy to follow.

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system’s relationship to help user decision-making.
1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.
The output form of an information system should accomplish one or more of the following objectives.
- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

CONCLUSION

In this paper, we proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access control scheme for multi-authority cloud storage systems. We also proved that our scheme was demonstrable secure in the random oracle model. The revocable multi-authority CPABE is a technique, which can be applied in any remote storage systems and online social networks etc.

REFERENCES