International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Unified Scheme of Hierarchical Attribute-Based Encryption

Syeda Husna Mehanoor[1], Syeda Ayesha Thainiath[2]

Dr V.R.K College of Engineering & Technology (Affiliated to JNTUH)

Nawab Shah College of Engineering & Technology (Affiliated to JNTUH)

Abstract: ***Cloud computing, as an emerging computing paradigm, enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. Especially for small and medium-sized enterprises with limited budgets, they can achieve cost savings and productivity enhancements by using cloud-based services to manage projects, to make collaborations, and the like. However, allowing cloud service providers (CSPs), which are not in the same trusted domains as enterprise users, to take care of confidential data, may raise potential security and privacy issues. To keep the sensitive user data confidential against untrusted CSPs, a natural way is to apply cryptographic approaches, by disclosing decryption keys only to authorized users. However, when enterprise users outsource confidential data for sharing on cloud servers, the adopted encryption system should not only support fine-grained access control, but also provide high performance, full delegation, and scalability, so as to best serve the needs of accessing data anytime and anywhere, delegating within enterprises, and achieving a dynamic set of users. In this paper, we propose a scheme to help enterprises to efficiently share confidential data on cloud servers. We achieve this goal by first combining the hierarchical identity-based encryption (HIBE) system and the ciphertext-policy attribute-based encryption (CP-ABE) system, and then making a performance-expressivity trade-off, finally applying proxy re-encryption and lazy re-encryption to our scheme.***

Keywords: Cloud Service Provider (CSP), Hierarchical identity-based encryption (HIBE), Ciphertext-policy attribute- based encryption.

1. Introduction

Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, utility computing, and service-oriented architecture. We propose a hierarchical attribute-set-based encryption (HASBE) scheme for access control in cloud computing. HASBE extends the cipher text-policy attribute- set-based encryption (CP-ASBE, or ASBE for short) scheme with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control. However, most of them suffer from hardness in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing. We propose hierarchical attribute-set-based encryption (HASBE) by extending cipher-text-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability, flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. The main operations of HASBE: System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access, and File Deletion.

With the emergence of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption system with a fine-grained access control to encrypt outsourced data. Cipher text-policy attribute-based encryption (CP-ABE), as one of the most promising encryption systems in this field, allows the encryption of data by specifying an access control policy over attributes, so that only users with a set of attributes satisfying this policy can decrypt the corresponding data. However, a CP-ABE system may not work well when enterprise users outsource their data for sharing on cloud servers, due to the following reasons:

First, one of the biggest merits of cloud computing is that users can access data stored in the cloud anytime and anywhere using any device, such as thin clients with limited bandwidth, CPU, and memory capabilities. Therefore, the encryption system should provide high performance.

Second, in the case of a large-scale industry, a delegation mechanism in the generation of keys inside an enterprise is needed. Although some CP-ABE schemes support delegation between users, which enables a user to generate attribute secret keys containing a subset of his own attribute secret keys for other users, we hope to achieve a full delegation, that is, a delegation mechanism between attribute authorities (AAs), which independently make decisions on the structure and semantics of their attributes. Third, in case of a large-scale industry with a high turnover rate, a scalable revocation mechanism is a must. The existing CP-ABE schemes usually demand users to heavily depend on AAs and maintain a large amount of secret keys storage, which lacks flexibility and scalability.

2. Literature Survey

Scientific computing often requires the availability of a massive number of computers for performing large scale experiments. Traditionally, these needs have been addressed by using high-performance computing solutions and installed facilities such as clusters and super computers, which are difficult to setup, maintain, and operate.

- Cloud computing provides scientists with a completely new model of utilizing the computing infrastructure.

- Compute resources, storage resources, as well as applications, can be dynamically provisioned (and integrated within the existing infrastructure) on a pay per use basis.
- These resources can be released when they are no more needed. Such services are often offered within the context of a Service Level Agreement (SLA), which ensure the desired Quality of Service (QoS). Aneka, an enterprise Cloud computing solution, harnesses the power of compute resources by relying on private and public Clouds and delivers to users the desired QoS.
- It's flexible and service based infrastructure supports multiple programming paradigms that make Aneka address a variety of different scenarios: from finance applications to computational science.
- As examples of scientific computing in the Cloud, we present a preliminary case study on using Aneka for the classification of gene expression data and the execution of fMRI brain imaging workflow.
- Security policy is increasingly being used as a vehicle for specifying complex entity relationships. When used to define group security, policy must be extended to state the entirety of the security context.
- For this reason, the policy requirements of secure groups are more complex than found in traditional peer communication; group policies convey information about associations greater and more abstract than their pair-wise counterparts.
- This paper identifies and illustrates universal requirements of secure group policy and reasons about the adherence of the Group Security Association Key Management Protocol (GSAKMP) to these principles.

3. Problem Definition

Sender generates the public key and private key. The sender encrypts the file using public key and sends the encrypted file and private key to cloud. The receiver gets the encrypted file and private key from cloud. The sender system was some communication problem. The total process is incomplete.

4. Methodologies

Authentication

If you are the new user going to access the make request or process request then they have to register first by providing necessary details. After successful completion of sign up process, the user has to login into the application by providing username and exact password. The user has to provide exact username and password which was provided at the time of registration, if login success means it will take up to main page else it will remain in the login page itself.

Trusted Authority

Trusted Authority is Main part of this project. It creates one decryption key for the relevant encryption key. After the decryption key provided the domain authority. Domain authority, Data owner, Data consumer and Cloud service provider are controlled in Trusted Authority.

Domain Authority

Domain Authority is sub head for the trusted authority. Domain authority performs the administrator operation. Data owner will not store the data without domain authority permission and Data consumer will not get the data without Domain authority permission. So the domain authority provides the permission to the Data owner and Data consumer.

Data Owner

Data Owner store's the data in cloud service provider for secure purpose. Before Data owner get the permission from the domain authority to store the data. After getting the permission Data owner first encrypt the file or data and store the data in cloud storage or cloud service provider.

Data Consumer

First Data Consumer gets the permission from the domain authority for data. Data consumer pays some amount of money to the domain authority and gets the decryption key. Finally Data Consumer retrieves the data from cloud service provider and decrypts the data using the decryption key.

Cloud Service Provider

Cloud Service Provider is another name for cloud storage. Cloud storage is providing the security for data. Only authorized user (get permission from the domain authority) allows encrypting and storing the data. Authorized user allows retrieving the data and decrypting the data.

5. Technique Used

Hierarchical attribute-set-based encryption algorithm (HASBE):

First, we show how HASBE extends the ASBE algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control of ASBE. Second, we demonstrate how to implement a full-fledged access control scheme for cloud computing based on HASBE.

- The scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in cloud computing.
- Our system model consists of a trusted authority, multiple domain authorities, and numerous users corresponding to data owners and data consumers.
- The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities.
- We are now ready to describe the main operations of HASBE: System Setup, Top-Level Domain Authority Grant, New Domain Authority/User Grant, New File Creation, User Revocation, File Access, and File Deletion.

System Setup

The trusted authority calls the algorithm to create system public parameters PK and master key MK0.PK will be made public to other parties and MK0 will be kept secret.

Top-Level Domain Authority Grant:

The trusted authority will first verify whether it is a valid domain authority. If so, the trusted authority calls to Create DA (PK, MK0, A) generate the master key for DAi. After getting the master key, DAi can authorize the next level domain authorities or users in its domain.

New Domain Authority/User Grant:

When a new user, denoted as u , or a new subordinate domain authority, denoted as DAi+1 , wants to join the system, the administrating domain authority, denoted as DAi , will first verify whether the new entity is valid. If true, DAi assigns the new entity a key structure A corresponding to its role and a unique ID.

New File Creation:

To protect data stored on the cloud, a data owner first encrypts data files and then stores the encrypted data files on the cloud. Each file is encrypted with a symmetric data encryption key DEK, which is in turn encrypted with HASBE. Finally, the encrypted data file is stored on the cloud.

User Revocation:

Whenever there is a user to be revoked, the system must make sure the revoked user cannot access the associated data files any more. One way to solve this problem is to re-encrypt all the associated data files used to be accessed by the revoked user, but we must also ensure that the other users who still have access privileges to these data files can access them correctly.

File Access:

When a user sends request for data files stored on the cloud, the cloud sends the corresponding cipher texts to the user. The user decrypts them by first calling Decrypt (CT, SKu) to obtain DEK and then decrypt data files using DEK.

6. Conclusion and Future Work

In this paper we achieve this goal by exploiting and individually combining techniques of attribute-based Encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has most important properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed schemes is highly efficient and provably secure under existing security models.

References

[1] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,” *Future Generation Comput. Syst.*, vol. 25, pp.599–616, 2009
[2] S. Yu, C. Wang, K. Ren, and W. Lou, “Achiving secure, scalable, and fine-grained data access control in cloud computing,” in *Proc. IEEE INFOCOM 2010*, 2010, pp. 534–542.
[3] R. Bobba, H. Khurana, and M. Prabhakaran, “Attribute-sets: A practically motivated enhancement to attribute-based encryption,” in *Proc. ESORICS*, Saint Malo, France, 2009.
[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, 2007

Author Profile

Syeda Husna Mehanoor received the M. Tech degree in computer Science Engineering from DR. V.R.K College of engineering.

Syeda Ayesha Thainiath received the M. Tech degree in computer Science Engineering from Al-Habeeb College of Engineering and Technology. Working in Nawab Shah College of Engineering & Technology as an Assistant Professor in CSE dept.