ATTRIBUTE SET BASED ENCRYPTION FOR SCALABLE AND FLEXIBLE ACCESS CONTROL IN CLOUD COMPUTING

E. Swapana¹, P. Arjun Kumar²

¹,²Joginpally B. R. Engineering College

Published online: 10 Dec 2014 © WJES – 2014

ABSTRACT:

Cloud Computing, an emerging computing paradigm, requires additional security which is provided using HASBE and this can emerge as a new security feature for various organisational platforms. We propose attribute based solution so that performance of cloud can be improved. It is implemented using cipher text policy by encrypting and decrypting the data in the cloud so that the cloud system becomes more scalable and flexible by enforcing data owners to share their data with data consumers controlled by the domain authority. Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this paper, 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 due to its hierarchical structure, but also inherits 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. We formally prove the security of HASBE based on security of the cipher text-policy attribute-based encryption (CP-ABE) scheme by Bethen court et al. and analyze its performance and computational complexity. We implement our scheme and show that it is both efficient and flexible in dealing with access control for outsourced data in cloud computing with comprehensive experiments.

Keywords: Batteries, Cloud Computing, Access Control, Data Security, Key Generation

I. Introduction

On the need of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption scheme with a fine-grained access control to encrypt outsourced data. Hierarchical Attribute Based Encryption, 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. The hierarchical Attribute Set-Based Encryption (HASBE) scheme is for accessing control in cloud computing and extended the cipher text policy attribute set based encryption. Hierarchical
Attribute Based Encryption security for data’s based on public key and master key with the help of Domain Authority Check. Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, utility computing, and service-oriented architecture. In the last several years, cloud computing has emerged as one of the most influential paradigms in the IT industry, and has attracted extensive attention from both academia and industry. Cloud computing holds the promise of providing computing electricity, and telephone). The benefits of cloud computing include reduced costs and capital expenditures, increased operational efficiencies, scalability, flexibility, immediate time to market, and so on. Different service-oriented cloud computing models have been proposed, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Numerous commercial cloud computing systems have been built at different levels, e.g., Amazon’s EC2 [2], Amazon’s S3 [3], and IBM’s Blue Cloud [4] are IaaS systems, while Google App Engine [5] and Yahoo Pig are representative PaaS systems, and Google’s Apps [6] and Salesforce’s Customer Relation Management (CRM) System [7] belong to SaaS systems. With these cloud computing systems, on one hand, enterprise users no longer need to invest in hardware/software systems or hire IT professionals to maintain these IT systems, thus they save cost on IT infrastructure and human resources; on the other hand, computing utilities provided by cloud computing are being offered at a relatively low price in a pay-as-you-use style.

Although the great benefits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security problems in cloud computing become serious obstacles which, without being appropriately addressed, will prevent cloud computing’s extensive applications and usage in the future. One of the prominent security concerns is data security and privacy in cloud computing due to its Internet-based data storage and management. In cloud computing, users have to give up their data to the cloud service provider for storage and business operations, while the cloud service provider is usually a commercial enterprise which cannot be totally trusted. Data represents an extremely important asset for any organization, and enterprise users will face serious consequences if its confidential data is disclosed to their business competitors or the public. Thus, cloud users in the first place want to make sure that their data are kept confidential to outsiders, including the cloud provider and their potential competitors. This is the first data security requirement.

Data confidentiality is not the only security requirement. Flexible and fine-grained access control is also strongly desired in the service-oriented cloud computing model. A health-care information system on a cloud is required to restrict access of protected medical records to eligible doctors and a customer relation management system running on a cloud may allow access of customer information to high-level executives of the company only. In these cases, access control of sensitive data is either required by legislation (e.g., HIPAA) or company regulations.

II. RELATED WORK

A. Cipher-Text Policy

The trusted authority calls the algorithm to create system public parameters and master key. Public parameters will be made public to other parties and Master Key will be kept secret. The attributes associated with the cipher text satisfy the tree access structure, can the user decrypt the cipher text.

B. Kp-Abe Policy:
We utilize KP-ABE to escort data encryption keys of data files. Such construction helps us to immediately enjoy fine-grandness of access control. CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies
\[
a \equiv g^k \pmod{p}; \quad \gcd(k, p-1) = 1; \text{ else } a \equiv 1?
\]
Message \( M \) (digraph, trigraph blocks)
- Public key \((g, p, y \equiv gx \pmod{p})\)
- \( M \equiv (xa + kb) \pmod{(p-1)} \)

\[\text{where } x = \text{private key } k = \text{random secret value}\]
Digital Signature \((a, b)\) sent with \( M \)
- \( yaab \equiv g^M \pmod{p} \)
The Math:
- \( g^M \equiv g(xa+kb) \pmod{p} \)
- \( (gx)^a (gk)^b \equiv yaab \pmod{p} \)
If \( M \) was modified, congruence would be violated

**III. IMPLEMENTATION**

The traditional method to protect sensitive data outsourced to third parties is to store encrypted data on servers, while the decryption keys are disclosed to authorize users only. However, there are several drawbacks about this trivial solution. First of all, such a solution requires an efficient key management mechanism to distribute decryption keys to authorized users, which has been proven to be very difficult. Next, this approach lacks scalability and flexibility; as the number of authorized users becomes large, the solution will not be efficient anymore. In case a previously legitimate user needs to be revoked, related data has to be re-encrypted and new keys must be distributed to existing legitimate users again. Last but not least, data owners need to be online all the time so as to encrypt or re-encrypt data and distribute keys to authorize users.

**IV. CLOUD ARCHITECTURE DESIGN**

**System model**

Cloud computing has computational and sociological implications. In computational terms cloud computing is described as a subset of grid computing concerned with the use of special shared computing resources. For this reason it is described as a hybrid model exploiting computer networks resources, chiefly Internet, enhancing the features of the client/server scheme. From a sociological standpoint on the other hand, by delocalizing hardware and software resources cloud computing changes the way the user works as he/she has to interact with the "clouds" on-line, instead of in the traditional stand-alone mode.
Fig 1: System model

Security Model
We assume that the cloud server provider is untrusted in the sense that it may collude with malicious users (short for data owners/data consumers) to harvest file contents stored in the cloud for its own benefit. In the hierarchical structure of the system users given in Fig. 2, each party is associated with a public key and a private key, with the latter being kept secretly by the party.

Fig 2: Example key structure.
The trusted authority acts as the root of trust and authorizes the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users that it administers, but may try to get the private keys of users outside its domain. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. In addition, we assume that communication channels between all parties are secured using standard security protocols, such as SSL.

Access structure
Fig 3: Example access structure

V CONCLUSION
The HASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes. HASBE based on the security of CP-ABE and implemented the scheme, and conducted comprehensive performance analysis and evaluation. The HASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. HASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes.

VI REFERENCES