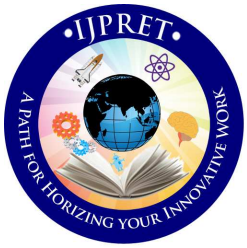
Research Article *ISSN: 2319-507X*
Anup Nimje, IJPRET, 2013; Volume 1(8): 1092-1100 *IJPRET*



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

AN INTRODUCTION TO VARIOUS ATTRIBUTE BASED ENCRYPTION SCHEMES IN CLOUD COMPUTING SECURITY FOR FLEXIBLE, SCALABLE AND FINE GRAINED ACCESS CONTROL

ANUP R. NIMJE

Student of Master of Engineering (Computer Engineering), College of Engineering and Technology, Amravati.

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Cloud Computing,
Attribute Based Encryption Technique,
Key Policy,
Cipher text Policy,
HASBE Scheme

Corresponding Author

Mr. Anup R. Nimje

Abstract

Being an emerging trend in computing technology, cloud computing is one of the most popular technology in IT industries as well as in researches. As enterprise networking technology has evolved, it has very strong requirement for computing security at enterprise level. Because, the cloud computing is the technology to use computing resources as a service with the users data, software and computation. The cloud computing is criticized by privacy advocates for greater use in which the companies hosting the cloud service control. Hence in this paper, we have discussed about the various encryption methods schemes that include the traditional security model, and further propositions made such as attribute based encryption ABE, which has been further modified to KP-ABE and CP-ABE. Among these, CP ABE is most flexible and scalable and hence we have HASBE scheme by inserting a hierarchical structure of users.

INTRODUCTION:

Cloud computing is one of the rapidly emerging trend and becoming very popular in IT industries, academicians and researchers. The cloud computing is to provide services over the network. The main theme of cloud computing is to give up data to the cloud service providers (CSP) for storage and business operations and hence the user data which is most important for his business must be secured with trust. Privacy must be preserved. Hence there are security concerns about the cloud computing.

Also fine grained access control is an important requirement and we can call it as a strong desire from the users and business requirements in that service oriented cloud computing. The sensitive data is a strong requirement in IT industries, business as well as individual cloud users.

Access control is a very popular research topic since over five decades. [1] And since then many models for security and access control were proposed. But they were not too suitable as flexibility or scalability or fine grained access point of view and these were applicable only for their trusted domains. But CSP and a cloud user not necessarily to be in their trusted domain hence there was concern about that also. So, new access control scheme was introduced by Yu et al [2] which consist of key policy attribute based encryption (KP-ABE). KP ABE provided fine grained access control. However there may be issues with flexibility and scalability while dealing with authorities at multiple levels. Whereas a ciplertext policy (CP-ABE) [3] has been proposed that was better than KP-ABE and it has well described access control policies.

In this paper we describe the propositions made after KP-ABE and CP-ABE that is a new attribute based encryption scheme called as HASBE. This is a hierarchical approach for attribute based encryption in which an advancement of CP-ABE has been made [4].

HASBE consists of structure of hierarchy of user systems that provide not only scalability but also flexibility and fine grained access control.

This paper explains the concept of HASBE that can be implemented in cloud systems.

We describe in this paper what HASBE is and how the model and algorithmic procedure and theoretical importance and future aspects of HASBE.

System model for cloud computing:

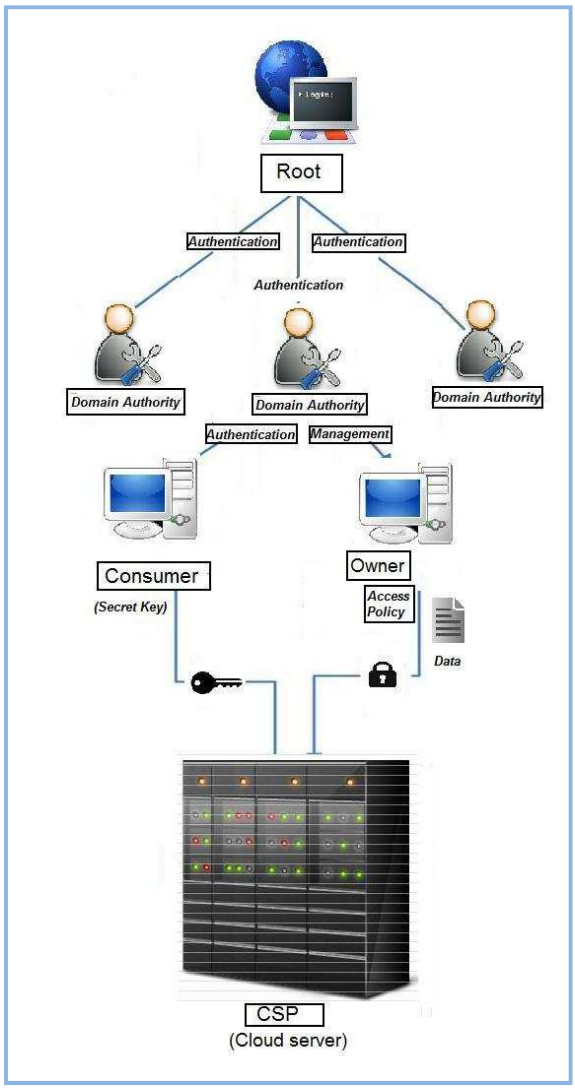


Fig.1 system model for cloud computing

As shown in Fig. 1, the cloud computing system here consists of five types of parties: a *cloud service Provider (CSP)*, *data owners, data consumers,* a number of *domain authorities, and a trusted authority*.

The *cloud service provider (CSP)* provides data storage service with clouds.

Data owners send their files by encrypting them and store or upload them in the cloud for sharing with data consumers. In order to access these shared data files on the cloud, data consumers download that encrypted data files of their interest and decrypt them. There are domain authorities that administrate the owners and customers. It means that they should belong to a same domain to avail the facility of cloud computing.

The trusted authority is the primary root authority that manages top-level domain authorities. Each top-level domain authority corresponds to a top-level organization, while each lower-level domain authority corresponds to a lower-level organization. Each domain authority regulates domain authorities at the next level or the data owners and consumers in its domain.

There are authorities that administrate the domain authority called trusted or parent domain placed in the hierarchy. We can discuss this model as a basic model and tradition cryptographic techniques used in the system. In further discussion we explain various encryption techniques with their basic information given from references.

Security Model

We consider that in security analysis purpose that the given cloud system is not necessarily to be trusted. In the given system, there is a hierarchy, each party is provided with their "keys". The *trusted authority* provides authorization at the top-level domain authorities. As shown in Fig-1 and refer fig.-2.

A domain authority is trusted by its next level domain. But there may be possibility that for unauthorized access, this means that, it may try to get the private keys of users outside its domain or scope and privileges. Hence there are security challenges for the given cloud model or domain structure.

Related ABE Schemes a brief view:

The basic cryptographic or access control method of data protection in systems was consisting of encryption outsourcing to third parties and to store decrypted data on servers and decryption keys are given to the authorized users.

However there are several drawbacks or limitations about this classic solution such as: It needs efficient key management mechanism for keys distribution to authorized users authentication which has been the most difficult problem. Secondly this approach lacks flexibility and scalability as number of authorized users become large, the solution will not be reliable. In this scheme to access it again, data to be re encrypted and new keys must be distributed to existing users again. And data owners need to be online for encrypt data and to re-distribute keys to users.

A. ABE (Attribute Based encryption):

According to *Sahai and Waters* [5] found a method for fuzzy identity based encryption. It was a better technique for getting scalable, flexible and fine grain access control mechanism. In ABE ciphertext is not encrypted to one particular user like in

traditional public key cryptography. In other hand, there is set of attributes or policy to which the user's ciphrtext and decryption keys are associated. Hence a user is able to decrypt its ciphertext its ciphertext only if decryption key and ciphertext matches. The primary drawback of the scheme was that it lacks expressibility Thus, ABE is further modified into KP-ABE and CP-ABE.

B. KP-ABE (key-policy access based encryption):

KP-ABE gives fine grained access control. Each file gets encrypted with symmetric encryption key (DEK), which is then encrypted by a public key corresponding to a set of attributes, generated by access structure. This encrypted data file is stored with attributes of file and user decrypts the file using DEK. A ciphertext is associated with a set of attributes and user's decryption key is associated with monotonic tree access structure. Here in KP-ABE, when ciphertext attributes are verified by tree access structure, the user can decrypt the ciphertext. [16]

The problem in this scheme was that encryption does not have knowledge of decryption and on whom it should trust. KP-ABE not perfectly suitable for certain applications, For example, encryption in broadcast system where users are described by various attributes and the users have to match their policies associated with the ciphertext can get decrypt the ciphertext. Hence it is better to use CP-ABE, ciphertext policy attribute based encryption.

C. CP-ABE(ciphertext-policy attribute based encryption):

In this scheme of attribute based encryption the role of ciphertext and decryption keys are changed. The ciphertext is encrypted with the tree access and decryption keys have attribute set associated. When a set of attribute associated with given decryption key can be used to decrypt the ciphertext. We can say that CP-ABE is more suitable applicable than KP-ABE for access control of encrypted data. CP-ABE [3] also has limitations to provide desired flexibility and efficiency in specifying policies and user attribute management. [4]

In CP-ABE scheme, decryption keys can only support single set of attributes. User is

allowed to use possible combination of the set only. To solve this problem, *Bobba et al* [4] introduced ciphertext policy Attribute set based encryption (CP-ASBE or shortly ASBE). It is an extended form of CP-ABE. This organizes users attribute into recursive tree structure.

ASBE can give great flexibility and access control as it enforces dynamic constraints on combining attributes to satisfy a policy.

An approach to hierarchical attribute based encryption (HASBE) to achieve fine grained access control in cloud computing:

The HASBE model [7]

HASBE was first proposed by *Wang et al [6].* It is to achieve fine grained access control. It uses *Hierarchical identity based encryption (HIBE)* and CP-ABE. It supports fine grained access control. It uses "disjunctive normal form policy" and takes all attributes in one conjunctive clause are administrated by same domain administrator.

Hence same attribute may be administrated by multiple domain admin. Comparing with ASBE, this scheme does not support compound attributes efficiency and multiple value assignments are not supported.

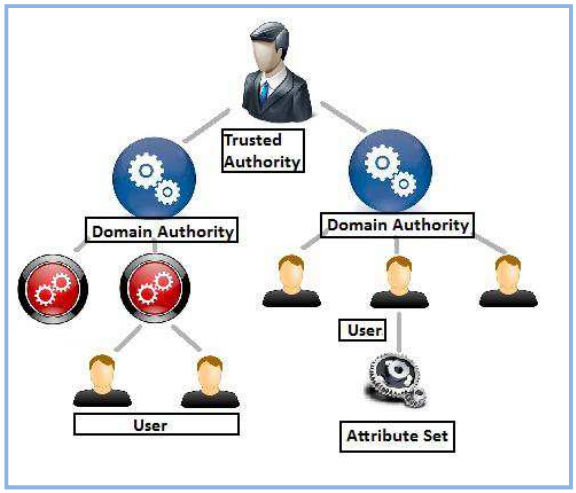


Fig-2 Hierarchical structure of system users

In relevant to the system model that has been discussed before, the HASBE model that combines the properties of both HIBE scheme as well as CP-ABE scheme, consists of a top level root domain and multiple sub-domains, where the Root Master (RM) works as the Trusted Third Party (TTP). Domain masters (DMs) corresponding to the Internal trusted parties (ITP) and users that corresponding to end users.

In a HIBE system, root master RM is followed by private key generator which is responsible for generating system keys and the domain master that combines domain PKG and attribute authority (AA) that in a

CP-ABE system, provides delegating keys to the DMs at the next level and distributing secret keys to users.

In other words that is explained by *Wang, Liu in [8]*, the HABE model, each DM and attribute is numbered with a unique identifier (ID), and each user's ID and a set of its attributes is also numbered with ID, where ID is an arbitrary string that gives unique entity.

Then it enables each entity's secret key is extracted from the DM administering itself. Public key of each entity, that denotes its position in the model, it is an ID consisting of the public key of the DM.

On comparing HASBE as given by *Wan Liu and Deng* [7] with the CP-ABE scheme, we can have some features of HASBE in flexibility, scalability and fine grained access control point of view, as given below:

1) ***Scalability of ABE***: HASBE is an extended form of CP-ABE in which it consists of hierarchical structure of users to effectively delegate the private attribute key of trusted authority generation operation to lower-level domain authorities.

By doing so, the workload of the trusted root authority gets minimized and gets shifted to lower-level domain authorities, which can provide attribute key generations for end users. Thus, this hierarchical structure achieves great scalability.

2) ***Flexibility in HASBE***: As key structure and access structure, HASBE can enforce more complex access policies than other scheme. Thus HASBE is more flexible than any other ABE scheme.

3) ***Fine-grained access control in HASBE***: The HASBE scheme can easily provide fine-grained access control. A data owner can define and enforce expressive and flexible access policy for data files.

CONCLUSION:

This paper gives a brief introduction to the security model of cloud computing and attribute base encryption schemes ABE and also by extending ABE to KP-ABE and CP-ABE, and being flexible and scalable , CP-ABE is modified to HASBE by introducing structure of hierarchy of users in CP-ABE model. Thus it gives new direction for the

attribute based encryption schemes and hence the cloud security.

ACKNOWLWDGEMENT:

Author would like to thank the professors, colleges and reviewers who helped directly or indirectly for writing this paper.

REFERENCES:

1. A. Ross, "Technical perspective: A chilly sense of security," *Commun.ACM*, vol. 52, pp. 90–90, 509.

2. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM 510*, 510, pp. 534–542.

3. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp.Security and Privacy*, Oakland, CA, 50[7].

4. R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in *Proc ESORICS*, Saint Malo, France, 509.

5. A. Sahai and B. Waters, "Fuzzy identity based encryption" in *Proc.Acvances in Cryptology—Eurocrypt*, 505, vol. 3494, LNCS, pp. 45[7]–4[7]3.

6. G.Wang, Q. Liu, and J.Wu, "Hierachical attribute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Chicago, IL, 510.

7. Cyber Guarder: A virtualization security assurance architecture for green cloud computing, by Jianxin Li, Bo Li, Tianyu Wo, Chunming Hu, Jinpeng Huai, Lu Liu, K. P. Lam, Special section: Green computing, Future Generation Computer Systems, v.28 n.2, p.368-3[7]0, February, 512, IEEE transaction.

8. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers Guojun Wang Qin Liu Jie Wu Minyi Guo computers & security30 (2011)320e331.