International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

"File Access Control Through Access Tree And Attribute Based Encryption In Cloud Computing : A Survey"

Ravi Mitra Reddy. L
M.Tech Student, VTU
Computer Networking, EWIT
Bangalore.

Harsha B. R.
Assistant Professor, VTU
Department Of ISE, EWIT
Bangalore.

Abstract

Cloud Computing has been transformed as fifth utility after the four utilities water, gas, electricity and telephone to provide services for users. Cloud Computing has become a significant technology that delivers dynamically scalable IT resources over the internet. Since data was stored in the cloud through internet, security problem is one of the most important issue in providing service to a user using cloud computing. In this paper I provide a technique called Hierarchical Attribute set based Encryption(HASBE) to give security and fine grained access control to the users of cloud computing. It was an enhancement for the technique called Attribute based Encryption(ABE) which is inflexible to handle complex control policies.

Key terms– Cloud Computing, HASBE, ABE

I. Introduction

Cloud Computing has become a significant technology that delivers dynamically scalable IT resources over the internet[1]. Cloud Computing is popular because of its infrastructure that is in the form of a cloud. Presently users are interested to access a content independently through internet rather than accessing in their own systems. Cloud Computing provides this type of independent access by storing data in a cloud. This infrastructure of a cloud consists of cloud service providers who provides cloud to store the data and consumers who upload the data and can download from anywhere and by using any supporting device. Some of the advantages of Cloud Computing are it reduces cost expenditure by providing some services and also reduces complexity and maintenance with less operational risk, scalability and flexibility.

Cloud Computing users can use variety of devices like PCs, smartphones, PDAs, laptops to access storage and application development platform over the internet. Any user can upload and download data into the cloud at any time.

Figure 1. Cloud Computing Architecture

Several service-oriented cloud computing models have been proposed.

Infrastructure-as-a-Service(IaaS)

This service gives computer infrastructure as a service along with the raw storage and networking. IaaS cloud providers provide on-demand resources for large pools of storage such as virtual-machine disk image library, virtual local area network, firewalls, ip addresses etc. The advantage of this

service is there is no need to buy any servers, data-centre space or network equipments for storage of the data. It also provides a set of APIs for management and interaction with the infrastructure by customers. Amazon EC2[2], HP cloud, Racspace cloud, Oracle Infrastructure as a Service are the examples of IaaS

Software-as-a-Service(SaaS)

It is also referred as on-demand software in which it delivers a software product and its associated data whenever a user demands. Cloud providers install and manage application software in the cloud This software is centrally hosted and each user can access by using thin client normally a web browser over internet. Google Docs, Microsoft office 365 are the examples of SaaS

Platform-as-a-Service(PaaS)

This service delivers a computing platform that includes operating system, database, webserver, programming language execution environment and a solution stack as a service. PaaS enables users to build their own platform for an application. It facilitate deployment of applications with less cost and complexity of buying and managing the software and hardware equipments. Google AppEngine[5], AWS Elastic Beanstalk[3], OrangeSpace, IBM cloud[4] are the examples of PaaS.

Three types of clouds can be defined[7]

Public Cloud:

Public clouds provides their dynamically scalable services through internet. public clouds are operated by the third party members. Users can access the services by using web servers or web applications. Users have to pay for subscribing a cloud on monthly basis. Data stored in the public clouds can be merged by the cloud servers and anyone can access at any time and from anywhere.

Private Cloud:

private clouds are owned and maintained by an organization. They purchase the cloud and enables access to their customers under that organization. private clouds uses firewall settings to provide security for the cloud. The organization which owned the private cloud pay the subscription fee on the space used by it. Private cloud provides more scalability than public cloud because it has limited number of users and can increase according to the organization requirement.

Hybrid Cloud:

A hybrid cloud environments is a combination of multiple public and private clouds. The complexity in hybrid clouds is distributing applications across public and private clouds.

Google Docs[6] is one of the cloud computing technology recently developed and used by the users. google docs allows the users to store the data by logging on to the google account in a cloud and can share with anybody. The user can access his document from any system and from anywhere in the world through internet. Google docs allows users to create new documents, spreadsheets, and presentations. Security is one of the vital issue when dealing with the clouds. Cloud service provider must provide security assurance for the customers who uses the cloud. Cloud can be protected by protecting the data stored in it by the customers, providing authentication, and reliable data access[8]. Cloud service provider should also able to provide backup data for customers if any loss of data occurs. Access Control is one of the problem that can come across while using cloud computing since data owners can allow access to some of his/her clients. Several solutions have been proposed to solve the access control problem. Bell la padula[10] and Biba[11] are two famous security models.

II.RELATED WORK

Since cloud computing became one of the influential paradigms in IT industry these days, it is important to provide security to the cloud. It is the responsible for cloud service providers to keep an incharge to maintain the data without loss. In case of private cloud it is responsible for the organization that owns the cloud to keep the data safe from any malicious software. But in the case of public clouds customer can access cloud data through internet so more possible chances to loss or theft of data. one more issue one can go through is access control. Cloud should provide fine grained access to the customers. To overcome these security issues and to achieve flexible and fine grained access so many security models have been proposed. *yu et al* proposed a model known as attribute based encryption which provides an encryption technique for uploading and downloading the data.

Attribute based encryption(ABE)[12]:

The scheme of encrypting data using its attributes was first introduced by Sahai and Waters. This scheme is based on fuzzy-identity based encryption

which inturn based on identity-based encryption.

Identity based encryption(IBE):

Shamir raised a question “What if your name could be your public key?” in 1984. Boneh and Franklin in 2001 given answer as "yes" and provided the encryption scheme based on identities. Encryption using their own name as identity is defined as Identity base encryption. First this scheme was given for simplifying the management of public keys, since each user has to develop his own public key. But later this model becomes unwieldy because if an user x wants to send a message to y. x uses his identity as his public key and transmits to y. y receives the message and will not trust the message completely so that the message has been sent by x or any other attacker on identity of x. This needs an trusted authority that tells the message was confidential.

Fuzzy-identity based encryption(FIBE):

Fuzzy identity based encryption[16] is one of the type of attribute based encryption. All Identity based encryption applications views identity as a string of constant but fuzzy identity based encryption uses biometric identities. In this scheme a user with a secret key for the identity @ is able to decrypt a ciphertext encrypted with the public key @' if and only if @ and @' are within certain defined metric distance. Fuzzy IBE gives two most important applications, firstly it uses IBE with biometric identities as attributes such as iris scan attributes. sencondly, fuzzy IBE can be used for application Attribute based encryption. The main advantage of fuzzy IBE is error-tolerant.

Hierarchical Identity based Encryption(HIBE):

As Shamir proposed the idea of identity based encyption has some disadvantages like Bob's receive his private key from an authority called Private Key Generator(PKG) that computes private key by its master key and its identity. This requires Bob to send its authentication to PKG and requires a secure channel to send these authentication messages. Another disadvantage is that PKG knows its master key and private key i.e., key escrow is inherent in identity-base encryption.

To overcome these disadvantages Horwitz and Lynn proposed hierarchical-identity based encryption[15] has been proposed. This scheme just adds hierarchical structure for IDE scheme. This structure consists of a PKG under which many PKG's are connected in next level. Thus the burden on one PKG in identity-based encryption in reduced. The top-level PKG generate and distribute private keys for next level PKG's and it proceeds to next level. PKG also require to verify the user's identity whenever request comes. This scheme is called 2-HIBE

Since data is stored in cloud, cloud service provider should provide assurance for security and confidentiality. since it is vulnerable to steal the data if it is directly stored in the cloud, a scheme called attribute based encryption was proposed that encrypts the data and stores it in the cloud. In this case if the data stored has been stealed cannot be decrypted. In attribute based encryption both users private keys and ciphertext will be associated with set of attributes or a policy over attributes. A user is able to decrypt the data only if there is a match between private key and cipher text to be decrypted. The disadvantage of this scheme is lack of expressiness and not applicable for large systems with more number of keys. ABE scheme has been classified into key-policy attribute base encryption(KP-ABE) and ciphertext-policy attribute based encryption(CP-ABE).

Key-Policy Attribute based Encryption (KP-ABE):

In this type of encryption scheme a ciphertext is associated with set of attributes and users key is associated with any monotonic tree access structure. This is a public-key cryptographic method. Data is associated with attributes for each of which a public key component is defined. The encyptor associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned a access tree structure that is, interoir nodes of the access tree are threshold gates and leaf nodes are associated with attributes. A user is able to decrypt if and only if the data attributes satisfy his access structure. Drawbacks of this scheme includes lacks flexibility in attribute management and lacks scalability in dealing multiple levels of attribute authorities.

Ciphertext-Policy attribute based encryption (CP-ABE):

In certain distributed systems a user should only be able to access the data if he/she posses a certain set of attributes. To employ this technique we need to use trusted server. The problem here is if any server compromises the confidentiality of the data stored in

it is compromised. So whenever an user needs to upload any data into a cloud it should be in a encrypted form so that if any unauthorized user tries to access he/she need to decrypt it which he cannot without the key.

In ciphertext-policy attribute based encryption a user private key will be associated with an arbitrary number of attributes. When an encryptor encrypts a message, they specify an associated access structure over attributes. A user can able to decrypt the ciphertext only if that users attributes pass through the ciphertext access structure. For example head of CBI agent can encrypt a sensitive information and provide access as follows, if(management level>5) OR (name: charles). As shown in above example the access structure for whom provided only can access the encrypted data. Whenever a user requests a particular file to access to the server, the server must check the authentication of the user whether he was allowed to access or not from the access structure.

III.PROPOSED MODEL

Hierarchical Attribute based encryption model:

Wang et al[13] proposed hierarchical attribute based encryption model to achieve fine-grained access control on the data stored in clouds

As depicted in Figure2, the cloud computing system consists of five parties. They are *cloud service provider, data owner, data consumer, a number of domain authorities, and trusted authority*

The cloud service provider provides cloud to store the data requested by a client. The provider provides certain security mechanisms to entrust the data stored in it from malicious attacks. Data owners can request a separate cloud for his/her organization this is called private cloud. whereas data owner can upload the data into the cloud by paying it some amount this is

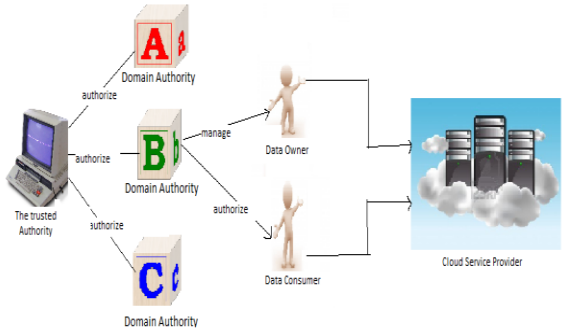

Figure 2. HASBE scheme structue

called public cloud. Data owner can store the data in an encrypted form to avoid malicious attacks from the internet and can share data to whom needed.

Data consumers who has access granted to view the data can download the data and should decrypt it to read. Each data owner and data consumer is administered by a domain authority. Each domain authority may consists of more than one owner and consumers. There may be more than one domain authority maintaining database of owners and consumers. All these domain authorities are maintained under parent domain authority or trusted authority.

Hierarchical attribute based encryption[14] is proposed by combining both hirechical identity based encyption and CP-ABE. The trusted authority is responsible for generating and distributing system parameters as well as master keys and authorizing top level domain authorities. So trusted authorities can also be referred as public key generators. Each and data owner or consumers should have their own private keys which are kept secret without revealing.

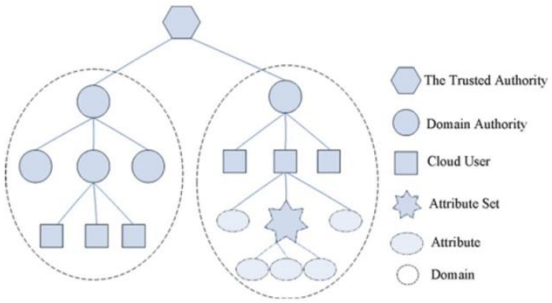

Figure 3.Hierarchical structure of system users

As shown in the above hierarchical structure under the trusted authority there are many domain authorities. Attribute set was used to represent the

attributes for decrypting the data. Since attribute sets are used the HASBE scheme allows recursive set based attributes. The depth of key is defined by the number of recursives used. The data stored may not be stored in one cloud and can be distributed through the clouds.

Data owners/consumers need not be always online at any time. while they come online only when necessary. Whereas cloud service providers, domain authorities and trusted authorities should be online always. Since many customers can uploading and downloading data at any time.

1) Scalability:
we extend ASBE with hierarchical structure by giving the private key generation operation to lower level domain authorities instead of only on top level domain authority. By doing so the workload on the trusted root authority is shifted to lower level authorities. This the hierarchical structure provides scalability over ASBE.

2) Flexibility:
Compared with yu et al scheme, HASBE organizes user attributes into a recursive set structure and allows users to impose dynamic constraints on how those attributes may combined to satisfy a policy. So HASBE can support compound attributes and multiple numerical assignments for a given attribute conveniently.

3) Fine-grained access control:
Since ciphertext is encrypted with a tree access policy chosen by an encryptor and the corresponding decryption key is associated with set of attributes. Also HASBE provides dynamic access structure for users to provide fine-grained access control.

4) Efficient user revocation:
User revocation is achieved by using expiration_time as an attribute to each user's key. So we can update users key by simply adding new expiration_time to the existing one. It is responsibility of the lower level domain authorities to keep some state information of the users key instead of generating and distributing the key every time needed. This makes HASBE more efficient.

5) Expressiveness:
In HASBE, users key is associated with set of attributes, So HASBE is conceptually closer to traditional access control methods such as Role Based Access Control(RBAC).

CONCLUSION

In this paper I introduced HASBE scheme by extending Ciphertext policy Attribute Based Encryption scheme with hierarchical structure. This scheme realizes scalable, flexible and fine grained access control in cloud computing. 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.

REFERENCES

[1]R. Buyya, C. ShinYeo, J. Broderg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility".

[2] Amazon Elastic Compute Cloud (Amazon EC2) [Online]. Available: http://aws.amazon.com/ec2/

[3] Amazon Web Services (AWS) [Online]. Available: https://s3.amazonaws.com/

[4] R. Martin, "IBM brings cloud computing to earth with massive new data centers," *InformationWeek* Aug. 2008[Online].Available:http://www.informationweek.com/news/hardware/data_centers/209901523

[5] Google App Engine [Online]. Available: http://code.google.com/appengine/

[6] "Cloud Computing: The Next Great Technological Innovation, the Death of Online Privacy, Or Both?" Derek Constantine.

[7] "Security Guidance for Critical Areas of Focus in Cloud Computing v3.0".pdf

[8 "A Hand Book of Cloud Computing" Borko Furht, Armando Escalante.

[9] A. Ross, "Technical perspective: A chilly sense of security," *Commun. ACM*, vol. 52, pp. 90-90, 2009.

[10] D. E. Bell and L. J. LaPadula, Secure Computer Systems: Unified Exposition and Multics Interpretation The MITRE Corporation, Tech. Rep., 1976.

[11] K. J. Biba, Integrity Considerations for Secure Computer Sytems TheMITRE Corporation, Tech. Rep., 1977.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attibute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Alexan- dria, VA, 2006.

[13] 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.

[14] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security and Privacy*, Oak- land, CA, 2007.

[15] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption," in *Proc. ESORICS*, Saint Malo, France, 2009.

[16] A. Sahai and B. Waters, "Fuzzy identity based encryption," in *Proc. Acvances in Cryptology—Eurocrypt*, 2005, vol. 3494, LNCS, pp. 457-473.

[17] G. Wang, Q. Liu, and J. Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Chicago, IL, 2010.