ISSN:0975-9646

A Survey on Access Control and Encryption Mechanisms for Cloud Computing

Ms. B. K.Ugale[1], Mr. R. N. Phursule[2]

[1] *Student,* [2] *Assistant Professor,, Department Of Computer Engineering,*
Imperial College Of Engg. & Research,Wagholi
Savitribai Phule University.Pune, India.

***Abstract*— Recent years cloud computing becomes an important paradigm in the IT industry. More enterprises prefers to use cloud computing techniques for their businesses, so cloud computing has become an important research area. In cloud computing cloud service providers and users are from different trust domains so data security and privacy are the important and critical issues for remote data storage. A secure user imposed data access control mechanism must be provided before cloud users have the liberty to outsource sensitive data to the cloud for storage. In this paper we have discussed different access control mechanism for cloud security.**

***Keywords*—IBE, ABE, RBE, ABAC, RBAC,HASBE.**

I. INTRODUCTION

Cloud computing is a new computing technology that is built on distributed and parallel computing, virtualization, utility computing and service oriented architecture. In last few years cloud computing has attracted extensive attention from industry and academia. Cloud computing provides lots of benefits including flexibility, scalability, reducing cost and so on.It provides different service oriented models like Infrastructure as a Service (IaaS), Platform as a Service (Paas) and Software as a Service (SaaS).Cloud computing provides great benefits for academic researchers, potential cloud users, IT industries. Security issues in cloud computing becomes a serious problem. Due to the internet based data storage and management, data security and privacy becomes one of the prominent security issues. In cloud computing users have to store their data on the cloud service providers for storage and business operations, while the cloud service providers are third parties 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. So cloud providers should ensure the data security as well as data should be kept confidential from outsiders including cloud service providers and their potential competitors.

Data confidentiality and security is the first requirement in cloud computing. The service oriented computing model strongly required flexible and fine grained access control. The personal health record system requires restricted access to the medical records .Only eligible doctors and customers may allow to access of customer information to high level executives of the company only.

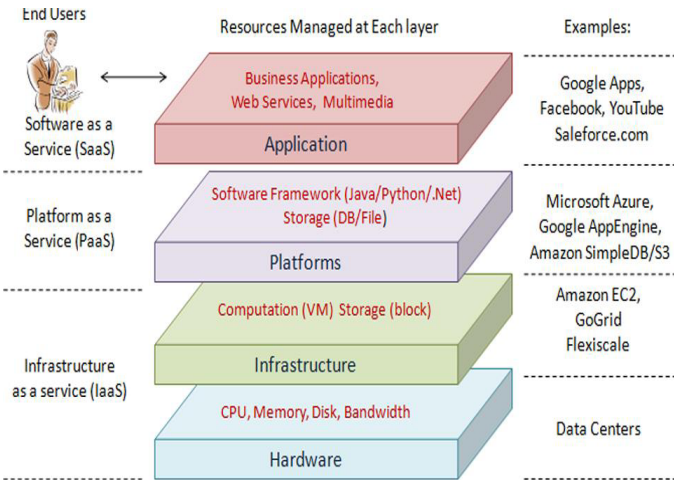

Fig1. Cloud Architecture

Access control is a classic security topic which dates back to the 1960s or early 1970s, and various access control models have been proposed since then. Bell-La Padula (BLP) and BiBa are two famous security models related to access control. The numbers of schemas have been proposed to achieve flexible and fine grained access control. Unfortunately, these schemas having some limitations because these are applicable only for the systems where data owners and the service providers are within the same trusted domain. Usually every time it is not possible that data owner and the service providers in the same domain in cloud computing. Attribute based encryption is the new access control scheme proposed by Yu et al., which adopts key-policy attribute-based encryption(KP-ABE), to enforce fine-grained access control. However, this scheme lacks in scalability and falls short of flexibility in attribute management. In contrast to KP-ABE, ciphertext-policy ABE (CP-ABE)[1] was proposed which turns out to be well suited for access control due to its expressiveness in describing access control policies.

II. LITERATURE SURVEY

The literature survey contains study of different access control mechanism for cloud computing. Mainly we have focused on Attribute based access control, role based access control, Identity based encryption, Attribute based encryption and Role based encryption. Following table gives a list of papers that we have surveyed.

Here we have listed out some characteristics of access control and encryption schema after surveying above papers.

The characteristics of an Ideal Access control and Encryption Schema:

Data confidentiality:
Data is get encrypted before uploading to the cloud, so unauthorized user of the cloud cannot know the information about data stored on cloud. Only authorized users, those who are having decryption key can access the data.

Fine-grained access control:
A different user from the same group gets the different access right. So users belongs to the same group can access the different data according to his access rights.

Scalability:
When the number of users of the system increases it may effect on the system performance. So the performance of the system is not get affected by increased numbers of authorized users.

Flexibility:
Flexibility of the cloud allows companies to adjust to any problems that may occur during day-to-day operations. It also allows using extra resources at peak times, to satisfy consumer demands.

Security:
While updating login credentials for example password or for requesting extra attributes. We must ensure that only valid user is performing those operations. As well as system must provide security from different attacks like session hijacking, session fixation etc.

A. Identity Based Encryption

Identity Based Encryption was proposed for cipher text security and it is a type of public key encryption. In this schema, user's public key is nothing but unique information about user's identity such as email id and user's private key is generated by using the known identity of the user. As a result user can encrypt message without prior distribution of keys between participants. This schema is extremely useful where pre-distribution of keys is infeasible or inconvenient due to technical restraints.

The steps involved in this Identity Based Encryption are given below:

Setup algorithm: Private Key Generator (PKG) executes this setup algorithm once to create IBE environment. This algorithm takes security parameters as a input and generates:
-A set of system parameters P
-A master key Km

Private Key Generation algorithm: When user sends request for his private key then PKG executes this private key generation algorithm. It requires system parameters P, master key Km and user ID and gives private key d for user identity ID.

Encryption algorithm: This Algorithm takes system parameters P, message m and users ID and it generates encrypted message for a particular user having identity is ID .

Decryption algorithm: This algorithm accepts private key d, system parameters p and encrypted message c and retrieves original message m.

B. Attribute Based Encryption

The main goal of attribute based encryption[2] proposed by Sahai and Waters is to provide security and access control. This schema having trusted authority, data owner and data user. Role of trusted authority is to generate keys for both data user and data owner to encrypt and decrypt the message. In Attribute Based Encryption cipher text is not only encrypted for a single user. The drawback of attribute based encryption scheme is that data owner needs to use each user's public key to encrypt data.

Sahai and Waters proposed the concept of Key policy ABE, which is enhancement of ABE and CP-ABE[2]. KP-ABE is the dual to CP-ABE in the sense that an access policy is encoded into the users secret key and a ciphertext is computed with respect to a set of attributes,In ciphertext-policy attribute-based encryption (CP-ABE) a user's private-key is related to the set of attributes and a ciphertext stipulates an access policy over a defined attributes within the system. A user will be able to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext.

C. Role Based Access Control

In RBAC access of resources is depends on the role which is assigned to the user. In this framework access is nothing but ability of an individual user to perform different operations such as create view and modify a file. Roles are depends on authority and responsibility within the organization. Various roles are created for an organization and permissions to perform specific operation are assigned to specific role.

RBAC has been widely used, but has weaknesses: it is labor-intensive and time-consuming to build a model instance, and a pure RBAC system lacks flexibility to efficiently adapt to changing users, objects, and security policies. Particularly, it is impractical to manually make (and maintain) user to role assignments and role to permission assignments in industrial context characterized by a large number of users and/or security objects.

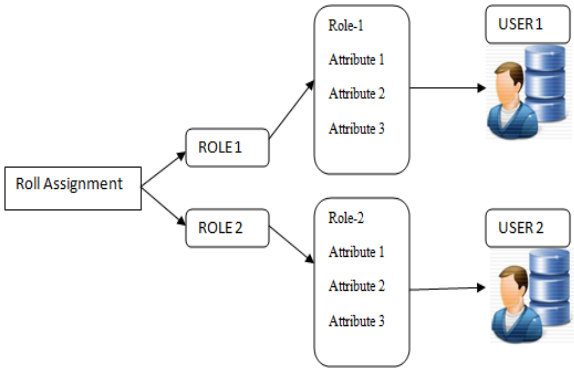

Fig.2 Role Based Access Control

D. *Attribute Based Access Control*

In attribute based access control[3] each user is associated with finite set of attributes. Data owner assigns attributes to the particular user by considering type of user. Whenever user logins and request for data, the user can access only assigned attributes .Set of attributes defines the access control.

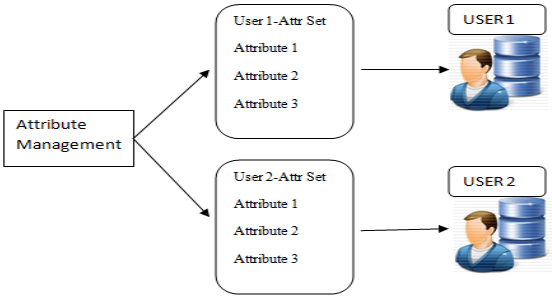

Fig.3 Attribute Based Access Control

E. *Hybrid Access Control(ABAC+RBAC)*

Combining role-based access control and attribute-based access control[3] is rising as a promising paradigm. In this schema we are combining role based access control with attribute based access control to get advantages of both. In this proposed schema we are considering three approaches to use role based access control and attribute based access control.

- Dynamic roles
- Attributed based
- Role based

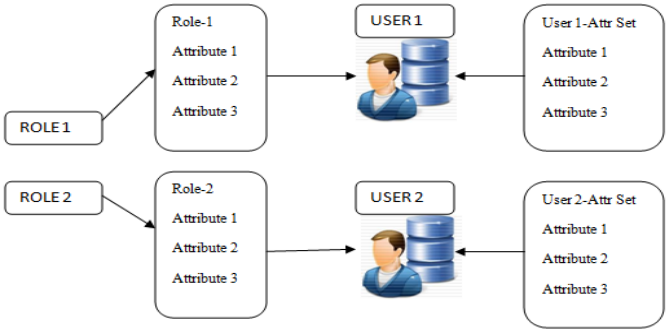

Fig.4 Hybrid access control

Dynamic roles:

In this first approach we are considering both role based access with attribute driven. As we are considering fine grained access control, using this we can assign particular role with some extra attributes to the user. And by providing decryption key user can access data which is assigned to that particular role as well as extra attributes. If any user request extra attributes than the role assigned then we will create dynamic role for that user and depending on the trust value of the user we are assigning extra attributes to that user.

Attribute Based:

Second approach is Attribute based, in this attributes are assigned to user which not from a single role. So in this case here we are using attribute based access control. So users can access different attributes related to the different roles.

Role Based:

The third option simply follows role based access control, in which roles are assigned to the users and depends on which role is assigned to that user attributes are accessible to that user.

These attribute-based policies bring to RBAC the advantages of ABAC: they are easy to construct and easy to familiarize to changes. Using this mechanism in large scale applications we can problem of permission assignment. This model is motivated by the characteristics and requirements of industrial control systems, and reflects in part certain approaches and practices common in the industry.

F. *Hierarchical Attribute and Role based access control*

In HASBE [4] schema, hierarchical user structure is used with ASBE.HASBE schema is based on attribute based access control. In our proposed schema, we are using hybrid access control to get the advantages of both attribute based access control as well as role based access control.

Figure.5 shows hierarchical structure of system users using role and trust management.

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.

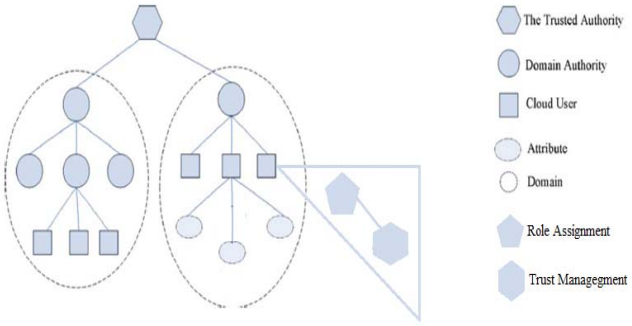

Fig.5 Hierarchical system users, Role and Trust management.

Trust Management:

Trust management is mechanism used while assigning extra attributes to the user. When user requests for extra attributes than assigned attributes in that case higher authority will check the trust value of the that user. If trust value is above threshold value then attributes are get assigned to the user otherwise attributes are not assigned to the user. Trust management helps to the data owner to assign new attributes by considering trust value.

III. CONCLUSIONS

In this paper we discussed about different access control mechanism and encryption schemas. We introduced HASBE schema with hybrid access control along with trust management and security i.e OTP. HASBE mainly focuses on scalable, flexible and fine grained data access control in cloud computing. We are providing additional security to HASBE by introducing OTP and trust management. The security can further be enhanced, Also a lot of work is been done on various other authentication and authorization techniques, integrity of data and confidentiality of data in cloud. Cloud is still a budding technology and needs various improvements and standardizations.

ACKNOWLEDGMENT

I would like to thank my Guide, Prof. R.N. Phursule for his support during the work. I would like to express my gratitude for the constant inspiration given by our head of the department and Principal I.C.O.E.R Wagholi for providing required facility and infrastructure during the work.

REFERENCES

[1] 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), Alexandria,VA, 2006.

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

[3] Keith Frikken,Mikhail Atallah, Fellowand Jiangtao "Attribute based access control" in IEEE TRANSACTIONS ON COMPUTERS, VOL. 55, NO. 10, OCTOBER 2006

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