ISSN:0975-9646

Security Enhancement in HASBE for Cloud Computing Environment

B. K.Ugale[1], 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 all the users and cloud service providers are from different domains so data privacy and security the critical and important issues for data storage. A secure user imposed data access control mechanism must be provided before cloud users have the privilege to outsource important data to the cloud. In this model we have combined role based access control and attribute access control to improve the performance of the system as well it uses one time password and trust management to extend the security.**

***Keywords*—RBAC, ABAC, OTP, Trust Management.**

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.

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) [3] and BiBa[4] are two famous security models related to access control. The number of schemas has 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) was proposed which turns out to be well suited for access control due to its expressiveness in describing access control policies.

In this project, we propose a hierarchical attribute-set-based encryption (HASBE) scheme for access control in cloud computing. It extends the ciphertext-policy attribute-set-based encryption (CP-ASBE) scheme by Bobba et al. with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control.

II. LITERATURE SURVEY

The ABE was first introduced by Sahai and Waters as a new method for fuzzy id entity-based encryption. The primary drawback of the scheme in is that its threshold semantics lacks expressibility. ABE schemes are classified into key-policy at-tribute-based encryption (KP-ABE) and ciphertext-policy at-tribute-based encryption (CP-ABE), depending how attributes and policy are associated with ciphertexts and users' decryption keys. In a KP-ABE scheme, a ciphertext is associated with a set of attributes and a user's decryption key is associated with a monotonic tree access structure. Only if the attributes associated with the ciphertext satisfy the tree access structure, can the user decrypt the ciphertext. In a CP-ABE scheme, the roles of ciphertexts and decryption keys are switched; the ciphertext is encrypted with a tree access policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given ciphertext, the key can be used to de-crypt the ciphertext. Since user's decryption keys are associated with a set of attributes, CP-ABE is conceptually closer to traditional access control models such as Role-Based Access Control (RBAC).

Sr. No	Paper Title	Author	Findings
1	HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing	Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE	It gives the concept of HASBE as well as attribute based access control.(KP and CP)
2	"Achieving Secure Role Based Access control on Encrypted Data in Cloud Storage.	Lan Zhou, Vijay Varadharajan, and Michael Hitchens.	This paper introduces the concept of Role based access control
3	"Scalable and secure sharing of Personal Health records in cloud computing using Attribute based encryption	Ming Li, Shuchenge Yu,Yao Zheng	From this paper, we got the Personal Health record as a base concept for implementation.

Table 2. Literature Survey

In traditional scheme, service provider's stores outsourced data in encrypted form on server to protect user's sensitive data, while the decryption keys are disclosed to authorized users only. However, these scheme having several drawbacks about this trivial solution. First of all, this requires an efficient key management mechanism to distribute decryption keys to authorized users, which is very difficult task. Next, this approach lacks scalability and flexibility; as the number of authorized users becomes large, the solution will not be efficient any more. 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.

ABE turns out to be a good method for flexible scalable and fine-grained access control solutions. The schema proposed by Yu et al. uses KP-ABE for access control mechanism, together with a re-encryption technique for efficient user revocation. In this schema each file is encrypted by using symmetric data encryption key (DEK), which is further encrypted by a public key related to a set of attributes in KP-ABE, which is generated according to an access structure. The encrypted data file is stored with the corresponding attributes and the encrypted DEK. If the associated attributes of a file stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK, which is used in turn to decrypt the file. The Problem with Yu et al.'s scheme is that the encryptor is not able to decide who can decrypt the encrypted data except choosing descriptive attributes for the data, and has no choice but to trust the key issuer.

Hierarchical attribute-based encryption (HABE), proposed by Wang et al. combines hierarchical identity-based encryption (HIBE) and CP-ABE to achieve fine-grained access control in cloud storage services. However, HABE uses disjunctive normal form policy and assumes all attributes in one conjunctive clause are administrated by the same domain master. Thus the same attribute may be administrated by multiple domain masters according to specific policies, which is difficult to implement in practice. Furthermore, compared with ASBE, this scheme cannot support compound attributes efficiently and does not support multiple value assignments.

III. SYSTEM ARCHITECTURE

A. Problem Statement:

Combining Attribute based access control and Role based access control to take advantage of both and extending security of the system with the help of One time password and Trust worthiness.

B. Motivation

In today's emerging Cloud computing era resources of the computing infrastructure can be provided as service by means of the Internet. As gifted as it is, this model also brings many new challenges for data security and access control. Users outsource sensitive data on the third party cloud servers. These cloud servers does not provide access control of both role based and attribute based. So there is a need of the system which can combine both attribute and role based access control to take the advantage of both. At the same time, System must be secure. So, to extend the security system uses OTP and Trust worthiness.

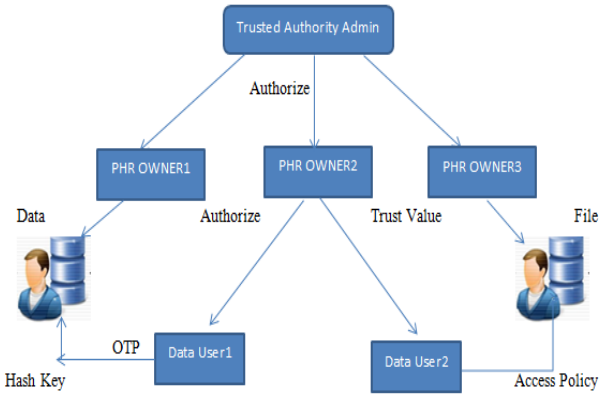


Fig. System Architecture

System Modules

- Registration and Login for user and PHR owner
- Encryption and decryption of data
- Access Policy Generation
- Hash Key Generation
- Assigning new attributes to the user
- Assigning new File to the user
- One time password generation
- Trust Management

IV. DESIGN AND IMPLEMENTATION

A. Data Flow Diagram

A DFD shows what kinds of information will be input to and output from the system, where the data will come from and go to, and where the data will be stored. It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel.

DFD Level 1:

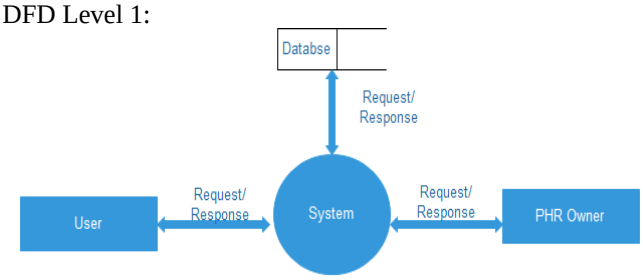


Fig: Data Flow Diagram Level 1

The Level 1 DFD shows more concise structure of the project. The level 1 DFD shows User and PHR owner interact with the system with the help of Database. When user submits query, system interacts with PHR owner or Database and generate response. Fig 5.2 shows the DFD Level

DFD Level 2:

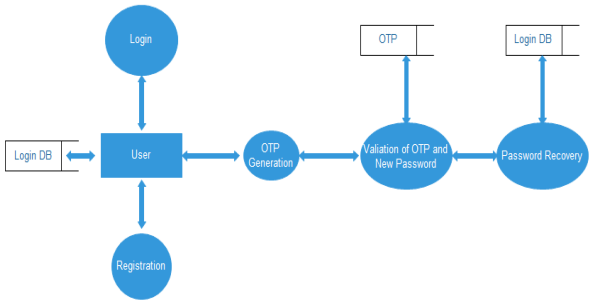


Fig: Data Flow Diagram Level 2

DFD Level 3:

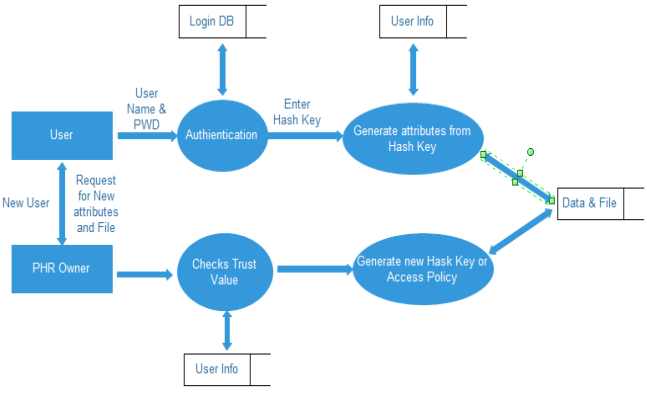


Fig: Data Flow Diagram Level 3

B. Mathematical Model and Algorithms

The presented Encryption algorithm applied on the data and file which gives the encrypted data and file which is get stored in to database and decryption algorithm is applied when user request for data or file and if user satisfy the access policy.

Algorithms for DATA Access

Setup

- It outputs Encryption key and Decryption key.

- Encryption(M,EK)
  - It take as input the Encryption key EK and data M. It outputs a cipher text.
- Hash Key Generation (U,AL)
  - The identity of user U , and attribute list. It out-puts a Hash key for user U.
- Decryption(CT,HK,DK)
  - Take cipher text as input and Hash Key HK for user U and decryption key DK. It outputs a message m. If the Hash Key matches with Attributes assigned to the user U.

Algorithms for File Access

- Setup
  - It outputs Encryption key and Decryption key.
- Encryption(F,PK)
  - It take as input the Encryption key EK ,a File F. It outputs a cipher text.
- Access Policy(F, Roles and Parameters)
  - The File, select Roles and parameters. It out-puts a Access policy AP for File F .
- Decryption(CT,AP)
  - Take cipher text and Access Policy AP as input for File F and decryption key DK. It decrypts a file F If the Access Policy AP matches with the user Parameters.

Algorithms for Hash Key Generation

Set of Role R= {r1, r2, r3….}
Set of Attribute List(Extra attributes)= {li1, li2, li3….}
Set of User U= {u1, u2, u3….}
1. List = List of Attribute assign to the user (U).
2. Foreach (string Role in R or string Attribute in List)
{
Foreach (char ch in Role or Attribute)
{
AK =AK + ch;
}
A set of Hask key AK= {hk1, hk2, hk3….}
}
3. In the Value we get ASCII value of that character.
4. ASCII values save into the database.

Algorithms for Access Policy Generation

Set of Role R= {r1, r2, r3….}
Set of Attributes A= {a1, a2, a3….}
Set of Files F= {f1, f2, f3….}
string access_policy=null;
1. List = List of Roles Selected by owner for specific file(F).

2. Attr= List of Attributes Selected by owner for specific file (F).
3. Foreach (element in List or Attr)
{
access_policy= access_policy+ element Converted in to Appropriate string.
}

Example:

1. Role and parameter selected by data owner:

Input: "(Role=Patient|Organization=Apple Hospital)"

Output: (Person.Role[0].equals(Person.Role1) OR Person.organization[0].equals
(Person.organization1))

Algorithms for OTP Generation:

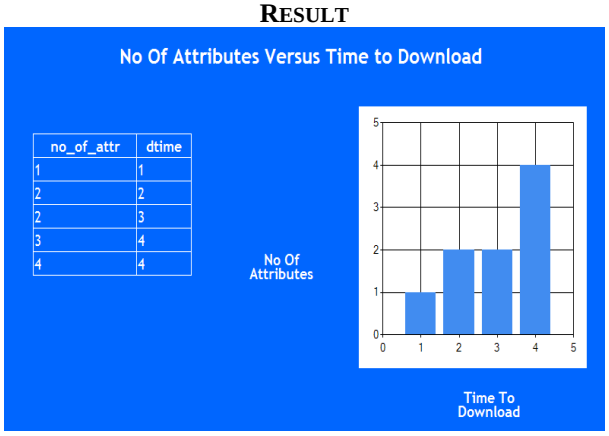
1. string password="";
2. int len=6;
3. List={list of allowed characters}
4. for(;password length<=len;)
5. {
c=select random character List;
password=password+c;
}
6. Send OTP to user through mail and message.
7. Store OTP into database for user authentication.

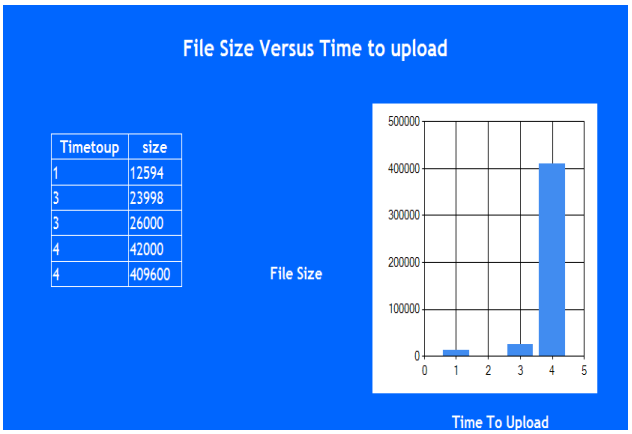
Algorithms for Trust Value generation:

Select User U={u1,u2,u3…}
Owner selects users for vote V={v1,v2,v3…}
for each voter in V
{
vote=rating given by Voter;(between 0 to 10)
Trust=(Trust + Vote)/2;
}

1. Store Trust value in to Database
2. If (Trust value>5)
User id Trustable
else
User is not trustable;

RESULT





CONCLUSIONS

This project implements the HASBE with extending security with the help of One Time Password and Trust worthiness. Trust worthiness allows to take advantage of extra attributes only if the user is trustable. Also it improves the performance of the system by combining the attribute and roll based access control. It improves the security of the system using the concept of one time password. Cloud is still a promising technology and desires various perfections 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.