HABE (Hierarchical Attribute Based Encryption) Model for Supporting Dynamic structure of organization.

Mr. Shashikant Govind Vaidya

Prof. Mr. Shailesh Kisan Hule

Mr. Gaurav Balvant Dagade

Mr. Sharad Arjun Jadhav

Computer Engineering,
Pimpri Chinchwad College of Engineering,
Pune, Maharashtra, INDIA.

***Abstract*—Due to rapid development in cloud computing and integration of new tools that enhances the development in cloud computing application, but cloud computing is in child state so that cloud security is often required. Many organizations want to store their confidential sensitive data in cloud in order to reduce capital expanses. Traditional way is to store data in encrypted format against the untrusted cloud service provider (CSP). The key problem is to maintain different organization structure and establishing unaccess control policy (UCP) for those confidential encrypted data, when users are no longer employee of organization. This paper aims to solve problem for supporting different organization structure and maintain their hierarchy of various users in the organizations, maintain record of employees .Our system is having integrating key feature of Hierarchical attribute based encryption (HABE) and cipher text policy attribute based encryption (CP-ABE) system, so as not only achieved high performance and fine grained access, user revocation scheme when user are not longer employee of organization.**

Keywords— Cloud computing, Hierarchical attribute-based encryption, Encrypted Data in Cloud server, Fine-grained access control, high Performance, User revocation.

I. INTRODUCTION

Cloud computing is a computational environment where we can use resources and pay only for that resources in which we are interested, so that user can enjoy service on demand. This emerging computer paradigm enable user to store their sensitive data in cloud whenever user wants that data he can download it in easy way. Cloud computing provide simplicity and efficient services to the user in order to save capital cost on hardware's infrastructure Especially for small and medium-sized enterprises with limited budgets, they can achieve cost savings and the flexibility to scale (or shrink) investments on-demand, by using cloud-based services to manage projects, enterprise-wide contacts and schedules, and the like[1].CSP can be operated for making profit to take care about sensitive confidential data, arises security and private issue. CSP can be selling out the confidential data to closest competitor company for making profit.

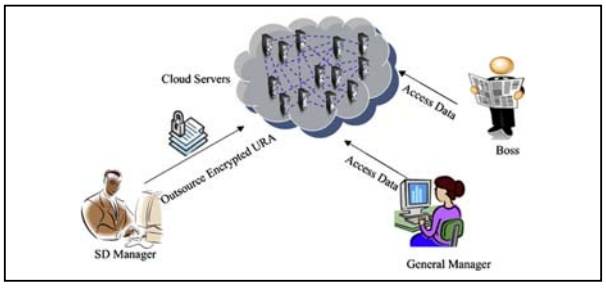

Fig 1. Application Scenario

We consider the following application scenario (see Fig. 1): Company A pays a CSP for sharing corporate data in cloud servers. Suppose the sales department (SD), the research and development department (RDD), and the finance department (FD) are collaborating in Project X [1]. The SD manager wants to store an encrypted user requirement analysis (URA) in the cloud, so that only the personnel that have certain certificates can access the document. For instance, the SD manager may specify an access control policy for this URA, as shown in Fig. 2[1]. In Fig. 2, the access control policy can be expressed as a Boolean formula over attributes. Each attribute consists of a web site specifying which party administers the attribute and an identifier describing the attribute itself, both of which can be represented as strings and concatenated with a single colon character as a separator [1]. The slash "/" in each web site denotes a concatenation between the superior and the subordinate.

The intuition behind this access control policy is that this URA should only be accessed by the boss and the general

Proc. of the Second International Conference on Advances in Computing, Control and Communication (CCN)
Editor In Chief Dr. R. K. Singh.

ISBN: 978-981-07-2579-2

manager of the enterprise, the members of Project X, and all the department managers who are involved in Project X[1]. Furthermore, the party that administers attributes "isBoss", "isGeneralManager", and "inProjectX" is superior to the party that administers attributes "isDepartmentManager", "inSD", "inRDD", and "inFD"[1]. In the above application scenario, the encrypter does not know the exact identities of the intended recipients, but rather he only has a way to describe them using certain descriptive attributes [1]. Therefore, the adopted encryption system should support an attribute-based access structure. Flexible encryption schemes such as cipher text-policy attribute-based encryption (CP-ABE), can be adopted to provide a fine grain access control for the encrypted data.

CP-ABE allows encrypting data specifying an access control policy over attributes, so that only users with a set of attributes satisfying this policy can decrypt the corresponding data [1]. For example, the data encrypted using the access structure "a1^a2" means that only the user with attributes a1 and a2, can decrypt the data [1]. In order to provide security CPABE scheme provide following properties.

- High Performance. In the cloud-computing environment, users may access data anytime and anywhere using any device [1]. When a user wants to access data using a thin client with limited bandwidth, CPU, and memory capabilities, the CP-ABE scheme should be of high performance [1]. That is, the communication costs and computation costs introduced by the CP-ABE scheme should be low enough, so that the user can successfully retrieve data from the cloud, and then decrypt it using the thin client [1].

- Full Delegation. In a large-scale enterprise with many employees, each employee needs to request secret keys from the attribute authority (AA), when he joins the enterprise [1]. If all these employees require their secret keys from one Attribute Authority (AA), there will be a performance bottleneck on the AA [1].

To reduce the workload on the AA, some CP-ABE schemes provide key delegation between users, which enables

- A user to generate attributes secret keys containing a subset of his own attribute secret keys for other users [1]. Full delegation means key delegation between AAs, where each AA independently makes decisions on the structure and semantics of its attributes [1].

- Scalable Revocation**.** In order to maintain hierarchy of organization we should know about how much employee in organization and those who are no longer employee revoke their access control policy. A user whose permission is revoked will still retain the keys issued earlier, and thus can still decrypt data in the cloud [1]. The traditional revocation scheme usually requires the AAs to periodically re-encrypt data, and re-generate new secret keys to remaining authorized users [1]. This approach will cause heavy workload on the AAs. A more scalable approach is to take advantage of the abundant resources in a cloud by allowing the AAs to delegate the CSP to re-encrypt data and re-generate keys to users, under the environment that the CSP knows nothing about the data and keys Based on the above-mentioned analysis, it is needed to propose a secure data-sharing scheme, which simultaneously achieves high performance, full delegation and scalable revocation [1].

```
http://www.companyA.com:  isBoss                                    OR
http://www.companyA.com:  isGeneralManager                          OR
http://www.companyA.com:  inProjectX                                OR
  (http://www.companyA.com/Department: isDepartmentManager  AND
     ( http://www.companyA.com/Department: inSD     OR
       http://www.companyA.com/Department: inRDD    OR
       http://www.companyA.com/Department: inFD     ) )
```

Fig 2. Sample Access Control Policy of URA

- Our contributions are as follows: supporting dynamic hierarchy of system and the system model propose a Hierarchical Attribute-Based Encryption (HABE) model, by combining the hierarchical identity based encryption (HIBE) system and the CP-ABE system [1]. The HABE model, which incorporates the property of hierarchical generation of keys in the HIBE system, and the property of flexible access control in the CP-ABE system, is more applicable to the environment of enterprises sharing data in the cloud [1]. System model propose a HABE scheme based on the proposed model, which requires only a constant number of bilinear map operations during decryption, to provide high performance. System provides a scalable revocation scheme, which allows delegating most of computation intensive tasks in revocation to the CSPs without disclosing data contents, by applying proxy re-encryption (PRE) and lazy re-encryption (LRE) to the HABE scheme [1]. Based on about above analysis. System is achieved following key feature.

II. RELATED WORK

A. Hierarchical identity-based encryption

In an identity-based encryption (IBE) system (Boneh and Franklin, 2001), there is only one private key generator (PKG) to distribute private keys to each user, which is undesirable for a large network because PKG has a burdensome job[1]. Gentry and Silverberg (2002), who have been dedicated to reducing the workload on the root PKG, introduced a HIBE scheme [1]. Their scheme with total collusion resistance at an arbitrary number of levels has chosen Cipher text security under the random oracle model and the Bilinear DiffieeHellman (BDH) assumption. A subsequent construction by Boneh and Boyen (2004) proposed a HIBE system with selective-ID security under the BDH assumption without random oracles [1]. In both constructions, the length of Cipher text and private keys, as well as the time during encryption and decryption, grows linearly with the depth of a recipient in

the hierarchy [1]. For better performance, Boneh et al. (2005) proposed an efficient HIBE system which requires only a constant length of Cipher text and a constant number of bilinear map operations during decryption [1]. In recent work, Gentry and Halevi (2009) proposed a fully secure HIBE scheme by using identity-based broadcast encryption with key randomization, and Waters (2009) achieved full security in systems under a simple assumption by using a dual system encryption [1].

B. Attribute-based encryption

Sahai and Waters (2005) introduced the notion of attribute based encryption (ABE). Based on their work, Goyal et al. (2006) proposed a fine-grained access control ABE scheme, which supports any monotonic access formula[1].Their scheme is characterized as key-policy ABE (KP-ABE) since the access structure is specified in the private key, while the attributes are used to describe the Cipher text[1]. A subsequent construction by Ostrovsky et al. (2007) allows for non-monotonic access structures [1]. Bethencourt et al. (2007) introduced a Ciphertext-policy ABE (CP-ABE) scheme, in which the roles of the Ciphertext and keys are reversed in contrast with the KP-ABE scheme [1]. Muller et al. (2008) constructed an efficient distributed

Attribute-based encryption (DABE) scheme that requires a constant number of bilinear map operations during decryption, using disjunctive normal form (DNF) policy [1]. Both of the above mentioned CP-ABE schemes provide a proof of selective security under the generic bilinear group model and the random oracle model [1]. In our previous work, a conjunctive fuzzy and precise identity-based encryption (FPIBE) (Wang et al.) scheme is proposed for secure data sharing in cloud servers [1]. The FPIBE scheme is able to efficiently achieve a flexible access control by separating the access control policy into two parts: a recipient identity (ID) set and an attribute-based access control policy [1]. Using the FPIBE scheme, a user can encrypt data by specifying a recipient ID set, or an access control policy over attributes, so that only the user whose ID belonging to the ID set or attributes satisfying the access control policy can decrypt the corresponding data[1]. However, it does not address the scalability issue. In recent work, to achieve a scalable revocation mechanism in cloud computing, Yu et al. (2010b) combined KP-ABE, proxy re-encryption (PRE) (Blaze et al., 1998), and lazy re encryption (LRE) (Kallahalla et al., 2003). However, the technique in Yu et al (Boneh et al., 2005) cannot be applied directly to combine PRE and CP-ABE. Since in contrast to KP-ABE, the access structure is associated with data other than the user attribute key [1]. The first combination of CP-ABE and PRE technique was first introduced by our previous work (Wang et al., 2010) and Yu et al. (2010a). The insufficiencies in the two schemes are as follows: The former lacks security proof for the encrypted scheme and systematical descriptions for the revocation scheme, and the latter constructs a CP-ABE supporting only "AND" semantic in the access control and does not support key delegation [1]. The characteristics of a HIBE system and a CP-ABE system are supporting "full delegation" and "fine-grained access control over attributes", respectively. Therefore, a natural way is to combine these encryption models [1]. This is a non-trivial task, since the former is designed for encrypting to an exact recipient; however, the latter is designed for encrypting to a set of attributes [1]. Furthermore, we found that the HIBE scheme in Gentry and Silverberg (2002) supports "one-to many" encryption: An encrypted file can be decrypted by a recipient and all his ancestors, using their own secret keys, respectively, which can be regarded as a meeting point with a CP-ABE system [1]. Therefore, we construct public/secret keys as Gentry and Silverberg (2002), which are the intuitions of the "one-to-many" property [1]. Then, inspired by Muller et al. (2008), we found that an encryption scheme achieves not only better performance, but also the combination of a HIBE system and a CP-ABE system, using the DNF access control policy [1]. Finally, inspired by Yu et al. (2010b), we also apply PRE and LRE in our scheme to achieve a scalable revocation mechanism [1].

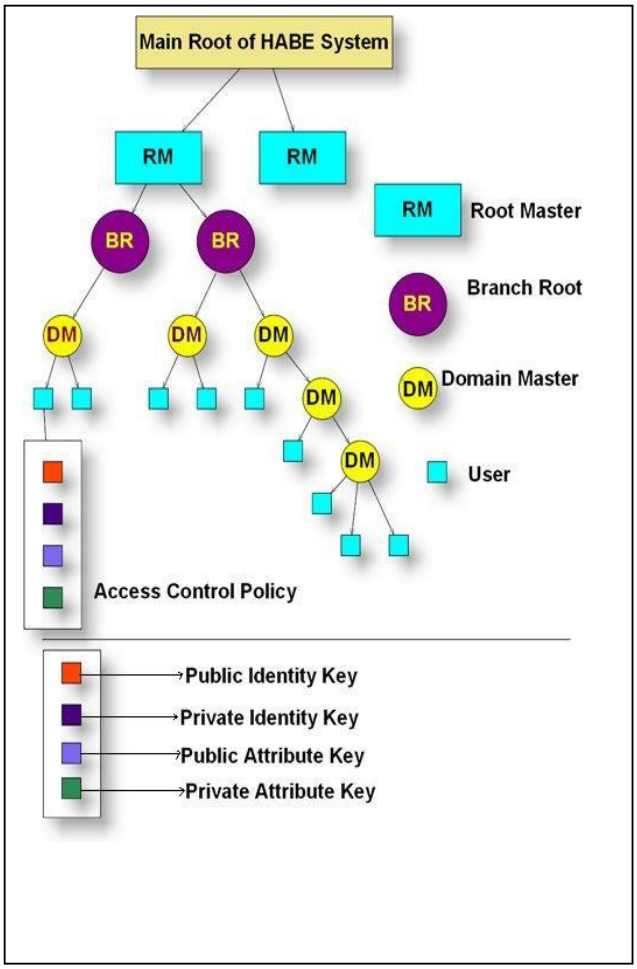

Fig 3. HABE Model.

III.OVERVIEW OF HABE MODEL

Corresponding to the system model, the HABE model, which integrates properties in both a HIBE model and a CP-ABE model, consists of a root master (RM) and multiple domains, where the RM functions as the TTP, and the domains are enterprise users[1]. More precisely, a domain consists of many domain masters (DMs) corresponding to the ITPs and numerous users corresponding to end users [1]. The RM, whose role closely follows the root PKG in a HIBE system, is responsible for generation and distribution of system parameters and domain keys. The DM, whose role integrates both the properties of the domain PKG in a HIBE system and AA in a CP-ABE system, is responsible for delegating keys to the DMs at the next level and distributing secret keys to users[1]. Specially, we enable the leftmost DM at the second level to administer all the users in a domain, just as the personnel office administers all personnel in an enterprise, and not to administer any attribute [1].Notice that other DMs administer an arbitrary number of disjoint attributes, and have a full control over the structure and semantics of their attributes [1].

IV.PRELIMINARIES

A. System model

Here we are assuming that the HABE model is composed by using following entities that is Trusted third party (TTP), Internal Trusted Third Parties (ITP), User and Cloud Service Provider (CSP).CSP is operated by its own Administrative activity which is interconnection of large server for storing encrypted files of organization and stored different replica of that encrypted file over different servers.CSP provide High Quality of services and high computational power. TTP generate keys for different organization and CSP.ITP is responsible for generating key for department and user. It also responsible for maintaining dynamic hierarchical structure of organization.

B. Security Model

As described in Haclgiimfi et al. (2002), there are two main attacks under such a circumstance, i.e., external attacks initiated by unauthorized outsiders, and internal attacks initiated by an honest but curious CSP (Yu et al., 2010b), as well as malicious end user [1].but the data stored in cloud which is to be consider as secure and communication line is also secure by using existing communication protocol SSL (Secure Socket Layer). Data is always in the form of encrypted and secrete key required for decryption, which is not decrypted easily by malicious user or cloud service provider.

V. SYSTEM CONSTRUCTION

As we know HABE Model having three important part that are TTP, ITP and end user. Following diagram shows actually system construction. There are different part which is actually perform same task. TTP contain two algorithms ‘setup and ‘create_RM algorithm. ITP contains create_branch, Create_Dept, Create_User, Encryption and Decryption algorithm.

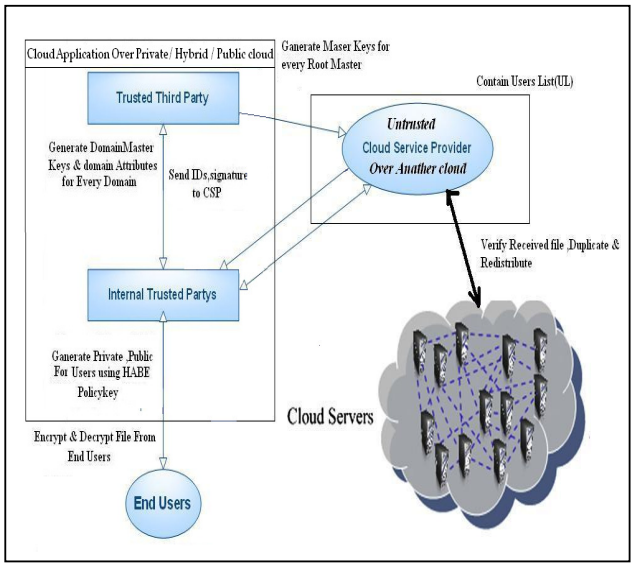

Fig 4. Construction of HABE Model

For construction of System we need to know algorithm which is follows.

A. Setup Algorithm

Setup algorithm takes a same parameter and generate master key for each organization and CSP.

```
Setup (parameter)
{
        //generate master key for Each Root master
          Generate (Mki);
}
```

B. Create Branch Algorithm

This algorithm takes a master key of each organization and parameter generates the branch id for each branch of organization.

```
create_branch(Mki,parameter)
{
            Generate (Bki);
            //Bki is for each branch of organization
}
```

C. Create Dept Algorithm

This algorithm takes a Mki,Bki,Ref_id and parameter to generate department wise key i.e. Dki.

```
Create_dept (Mki,Bki,Ref_id,parameter)
{
        //Dki is department wise key
        // Ref_id is id of parent node
        Generate (Dki);
}
```

D. *Create User Algorithm*

This algorithm takes a Mki,Bki,Dki and parameter o generate User id Uid.

```
Create_User(MK,Bid,Dki,parameter)
{
        If (true) Generate (uid);
        Else error;
}
```

E. Encryption Algorithm

This algorithm takes a plane text file F and valid user access policy on that file and generate cipher text file and it will be stored on cloud service provider. A is disjoined normal form (DNF) policy.

```
Encryption (F,PkalaεA)
{
    If(Pk is true)
    {
        Generate (cipher text file)
    }
    Else
    {
        Error;
    }
}
```

F. Decryption Algorithm

This algorithm takes cipher text (CT), Secrete key (SK) ε Conjunctive clause and generates plaintext.

```
Decryption (CT,SkilaεCCi)
{
    If (Ski is true)
    {
        Generate (plaintext file F);
    }

    Else
    {
        Error;
    }

}
```

ACKNOWLEDGEMENT

We thank all the staff members of Department of Computer Engineering; Pimpri Chinchwad College of Engineering, Pune, India who extended their unending support right from the idea was conceived.

We express our sincere and profound thanks to our Project Coordinator and Project Guide Prof. Sonal Gore, Head of the Computer Department Prof. Mr. S.S. Sambare and our beloved Principal Dr.A.M. Fulambarkar. Last but not least, we thank Prof. Mrs. Rajeswari and Prof. Mr. Sudharshan Deshmukh for their tremendous help in our work, all web communities and paper publications which helped & guided this work.

REFERENCES

[1] Guojun Wanga,*, Qin Liu a,b, Jie Wub, Minyi Guo-Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. In Proceeding of CCS 3 0 (2 0 1 1) 3 2 0 e3 3 1.

[2] Wang G, Liu Q, Wu J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In: Proceedings of CCS-2010 (Poster), pp. 735e737.

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attributebased encryption. In: Proceedings of ISSP; 2007. p. 321e34.

[4] aws.amazon.com/documentation/ec2

[5] s3.amazonaws.com/awsdocs/EC2/2008-12.../ec2-dg-2008-12-01.pdf

[6] www.ingrammicro.com/visitor/.../cloudcomputingfordummies.pdf.