Enhancing Data Access Security in Cloud Computing using Hierarchical Identity Based Encryption (HIBE)

Sai Krishna Parsha, Mohd.Khaja Pasha

Abstract--Cloud computing is the latest advancements in the areas of computing technologies. The concept of offering services over the network has resulted in the development of this striking technology. It is highly promising in solving the problems related to high computing with respect to hardware availability, software availability, resource availability and many. Users can access to their data stored at the cloud on the go; they just need a thin client connected to the network. Virtualization, also being a part of this technology, solves the user's needs in much more efficient way. Like any other technology, Cloud computing also need to look into the data security issues. User's data needs to be secured from unauthorized access.

In this paper we would like to propose the implementation of data access security in cloud using the Hierarchical Identity Based Encryption (HIBE). Restricting the data access among the untrusted users can be achieved by implanting the users and its subordinates in hierarchical fashion and achieving the data access security by revealing the data only to the trusted users.

Index Terms--Cloud Computing, Data security, Hierarchical Identity Based Encryption (HIBE).

1 INTRODUCTION

Cloud computing is the technology which is the combination of many other technologies such as the utility computing, autonomic computing virtualization, service oriented architecture and many. It has got features from all these varied technologies. The goal is to provide scalable, shared resources- software and hardware- and thereby providing services over the network. The terminology 'as a service' is coupled to it and referred as providing something as a service over the network. It can be Software as a Service (SaaS), Platform as a Service (Paas), Infrastructure as a Service (IaaS) and many.

All the services provided are just based on on-demand fashion. So that users can pay only to their requirement usage. Many providers such as Google's App Engine, Amazon's EC2 and S3, Microsoft's Windows Azure made the concept of Cloud computing a reality and providing the users the taste of this technology. Users who cannot afford to build their own huge infrastructure can have their work done by the help of cloud providers at less cost.

Based on the hosting of environment and the type of users the architecture can be of four types: 1.Public Cloud, 2.Private Cloud, 3.Hybrid Cloud, 4.Community Cloud. In a public cloud, Cloud services are hosted for public usage and anyone can have their data stored and services get done using this kind of cloud. Data security plays a major role here. A private cloud is the one where the data access and service usage restricted to single authority. A hybrid cloud is shared by a limited set of organizations and has the features of both private and public cloud. Community cloud is much like the private cloud but the data is shared among the same entities of the single organization.

As in every technology the security provided to the data, the access restriction of the data by the unauthorized users makes it more reliable and makes the users use the technology without any worries. As in cloud computing[7] the users share their sensitive data for computation and it needs to be secured from malicious users. This prevention from unauthorized users can be done by encrypting the

- *Sai Krishna Parsha is currently pursuing bachelors degree program in Information Technology in Chaitanya Bharathi Institute of Technology, India. E-mail: saikrishnaparsha@gmail.com*
- *Mohd.khaja Pasha is currently pursuing bachelors degree program in Information Technology in Chaitanya Bharathi Institute of Technology, India. E-mail: mohdkhajapasha88@gmail.com*

sensitive data before uploading them to the cloud servers. Even when we encrypt the data, there are different issues to be dealt with. The data provider provides the data and intended users can use the same. But not all the users have the same privileges. The access privileges to different users are at different levels. Thus the data provider needs to list all the access levels and issue the authorization privileges accordingly. In Hierarchical Identity Based Encryption[6] scheme the users of the data can be made in the form of a hierarchy. The node at each level of the hierarchy can give the access right to its subordinates. Based on the level of the user node the access rights to the users are issued and there by securing the data from unauthorized users.

Using HIBE[2] we can restrict the access of unauthorized or partially authorized users but sometimes users may share their keys illegally. This may lead to unauthorized usage of the data.

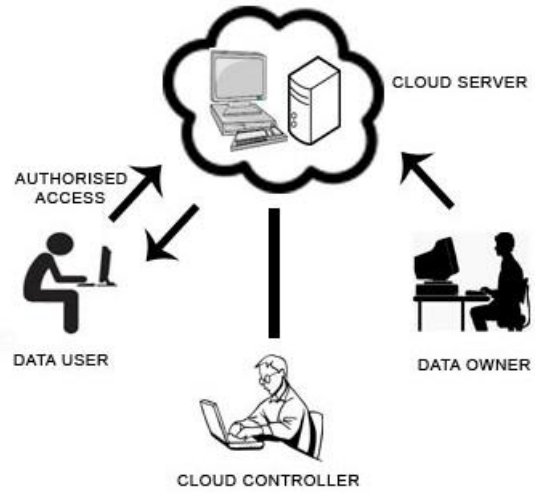


Figure 1: Cloud System

Users may give their private key to other users who do not have the access privilege or have limited access privilege. We need to have a solution for this user accountability.

2 BASIC SYSTEM

A cloud environment as shown in figure 1, basically has a cloud server where the data of the data owner is stored. The data owner is the one who uploads the data on to the server and gives various access right levels to the uploaded data usage. Data users are the ones who try to access the data stored by the data owners. These users should access to the data based on the rights they have. A Cloud Controller who manages the entire scenario. It also audits the file access transactions.

3 SECURITY TECHNIQUES

In the Hierarchical Identity Based Encryption[1] System the user identities are well organized in the hierarchy basis and at each level in the hierarchy the node can assign various access rights to its subordinates. New users can enter the system and acquire the access policies without any changes to the already existing system.

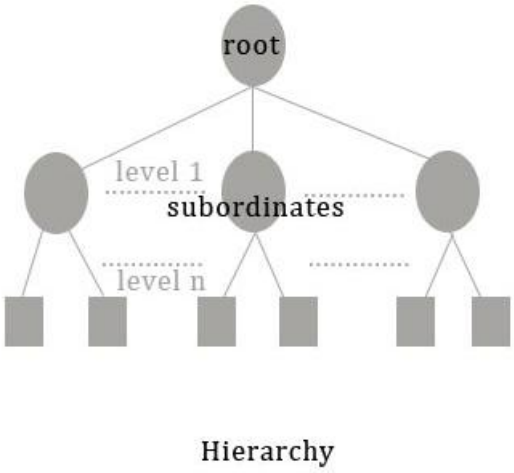


Figure 2: Information and Access hierarchy

Thus by modeling the cloud system using the HIBE model can enhance the data security of the cloud. We can assume the hierarchy as shown in the figure 2. The root has the subordinates and they further have their subordinates and the access rights are issued to them by its higher level nodes.

4 HIBE - BASED DATA SECURITY

Identity based encryption was first developed by Shamir later on constructed by Boneh, Franklin[3] and Cocks. Using dual system encryption Waters[5] provided another efficient IBE system with less public parameters. Hierarchical Identity based Encryption was first proposed by Horwitz and Lynn and constructed by Gentry and Silverberg.

4.1 HIBE-STEPS

The encryption scheme has basically five steps: Setup, Encrypt, KeyGen, Decrypt, and Delegate.

Setup (X) ⟶ ***PP, MSK***

The setup algorithm takes the security parameter X as input and outputs the public parameters PP and the master secret key MSK.

Encrypt (M, w, PP) ⟶***CT***

The encryption algorithm takes a message M, an identity vector w, and the public parameters PP as input and outputs the ciphertext CT.

KeyGen (MSK, w, PP) ⟶ SK_w

The key generation algorithm takes the master secret key MSK, an identity vector w, and the public parameters as input and outputs a secret key SK_w for that identity vector.

Decrypt(CT, PP, SK_w***)*** ⟶ ***M***

The decryption algorithm takes a ciphertext CT, the public parameters PP, and a secret key SK_w as input. If the identity vector of the secret key, w, is a prefix of the identity vector used to encrypt the ciphertext, the decryption algorithm outputs the message M

Delegate(SK_w***, w', PP)*** ⟶ $SK_{w:w'}$

The delegation algorithm takes a secret key SK_w for identity vector w, an identity w', and the public parameters PP as input. It outputs a secret key $SK_{w:w'}$ for the identity vector w:w', which denotes the concatenation of w and w'.

The data owner first runs the setup functionality and acquires a set of public parameters and the Master secret key. He also defines the hierarchy through which the access rights have to be issued. In this hierarchy the rights issued to a node can be allowed to the child and subordinate nodes thereafter. This hierarchy can also be developed in the form of a information hierarchy and also the constraint hierarchy. To allow the data user to issue personalized secrets to the intended users, the information hierarchy is useful by adding the identity of the intended user to its root node. The data owner provides the personalized private key to the intended data user corresponding to the access rights acquired by the user.

After developing the information and access hierarchies, the identity vector is developed. The encryption algorithm considers this identity vector as the parameter to encrypt the data. The result of this function is the ciphertext. The intended users are only given the secret key which is framed using the key generation algorithm.

4.2 SYSTEM DESCRIPTION

When a new file is added by the data owner on to the cloud servers, a wide set of information hierarchy and the access hierarchy is made as shown in the figure 2. Using these hierarchies a set of identity vector is developed. The data to be upload is first encrypted using the master secret key and the public parameters by taking into consideration the identity vector. During these various levels of hierarchies are encrypted by their required access levels.

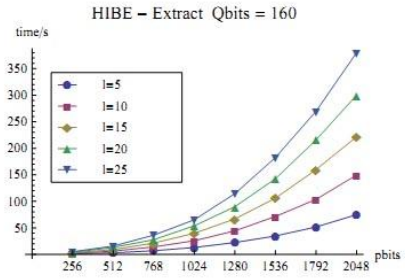
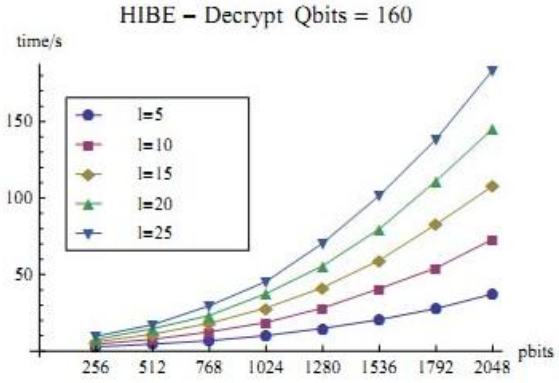


Figure 3: Extract



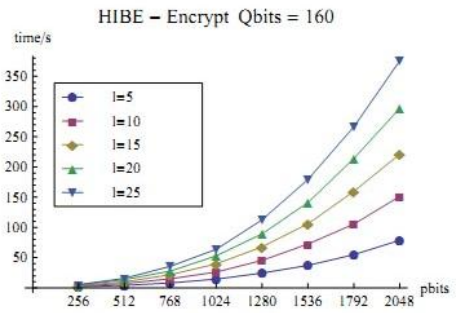
This generates the ciphertext. The data owner also generates the secret private key using the Key generation algorithm and the authorized level users are issued these secret keys based on their access rights. Using this secret key the intended users can decrypt the data. Then

after the user can have its subordinates to have the delegation.

5 PERFORMANCE ANALYSIS

The performance of the algorithm proposed here is good to certain levels of hierarchies. It is growing linearly with respect to the number of layers. As shown in the figures 3-6, the time/space cost requirement grows linearly with the number of levels included with the hierarchy.

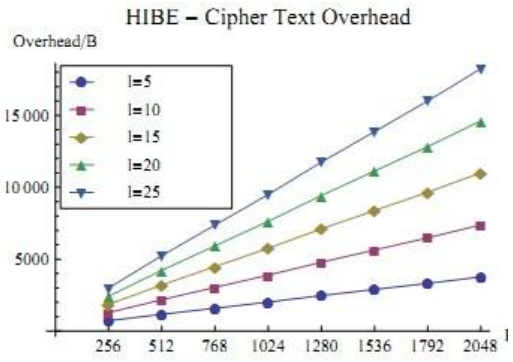
Figure 4: Encrypt



Consider pbits and qbits are the two security parameters used in the encryption technique. In figure 3, we can see that the extraction of the bits is considered by qbits keeping constant and allowing the pbits to vary. Figure 4 shows the encryption results at varied levels from 5 through 25 which shows the time cost varying linearly after certain levels. Figure 5 gives the description regarding the decryption of the same and reduced time cost. Finally figure 6 gives the ciphertext overhead per number of bytes for the same number of levels. These results show the performance of the proposal is good to certain levels of hierarchy.

Figure 5: Decrypt

Figure 6: Cipher Text Overhead



6 CONCLUSION

Cloud computing is the latest buzz word around the IT technologies over the past ten years and will be in the upcoming years for its advantages and its features. It is an amalgam of various technologies such as utility computing virtualization and many others. It is cost effective, highly reliable and scalable. Data access security is the main area to be addressed to make it more powerful. This paper proposes the data access security enhancement using the Hierarchical Identity Based Encryption. This may in practical provides the solutions for the problems such as unauthorized access to the sensitive data in the cloud.

REFERENCES

[1] Enhancing Data Security in Cloud Computing using Hierarchical Identity Based Encryption by Sai Krishna Parsha and Mohd. Khaja Pasha.

[2] Unbounded HIBE and Attribute-Based Encryption by Allison Lewko and Brent Waters.

[3] Fully Secure Anonymous Hierarchical Identity Based Encryption with constant Size Ciphertexts by Jae Hong Seo and Jung Hee Cheon.

[4] Identity Based encryption from the Weil Pairing by Dan Boneh Mathew Franklin.

[5] A survey of Identity based encryption by Joonsang Baek, Jan Newmarch, Reihaneh Safavi-Naini, and Willy Susilo.

[6] Fuzzy identity-Based Encryption by Amit Sahai and Brent Waters.

[7] Black-Box Accountable Authority Identity-Based Encryption by Vipul Goyal,Steve Lu, Amit Sahai and Brent Waters.