Data Security Technique in Cloud Storage

[1]Rohini G.Khalkar, [2]Dr. S.H.Patil
[1]Bharati Vidyapeeth Deemed University College of Engineering, Pune, India
[2]Dept. of CE, Bharati Vidyapeeth Deemed University College of Engineering, Pune, India

Abstract
In recent development of cloud computing, large number of enterprises can outsource their sensitive information for sharing in a cloud. To keep the shared information confidential against untrusted Cloud Service Providers (CSPs), a natural method is to store only the encrypted data in a cloud. The key issues in this approach include establishing access control for the encrypted information, and revoking the access rights from users when they are no longer authorized to access the encrypted data. This paper solves both the problems by combining a ciphertext-policy attribute-based encryption (CP-ABE) system and hierarchical identity-based encryption (HIBE) system, to provide both fine -grained access control, full delegation and high performance. HABE scheme generate encryption key i.e Master key Msk based on the hierarchical attributes so it will provide more security for cloud storage.

Keywords
Master Key Generation, Cloud Storage, Hierarchical Attribute Based Encryption

I. Introduction

A. Hierarchical Identity-Based Encryption

Identity-Based Encryption (IBE) system (Boneh and Franklin, 2001) includes only one Private Key Generator (PKG) to distribute private keys to each and every user, which is undesirable for a large network because PKG has a burdensome job. HIBE scheme is introduced by Gentry and Silverberg (2002), who have been dedicated to reducing the workload on the root PKG [3]. Their scheme with total collusion resistance at an random number of levels, has chosen ciphertext security under the arbitrary oracle model and the Bilinear Diffiee Hellman (BDH) assumption. Boneh and Boyen (2004) proposed a HIBE system with selective-ID security under the BDH assumption without random oracles. In both constructions, the length of private and ciphertext keys, as well as the time during encryption and decryption, grows linearly with the depth of a recipient in the hierarchy. Boneh et al. (2005) proposed an efficient HIBE system which needs only a constant length of ciphertext and a constant number of bilinear map operations during decryption for better performance [1]. In recent work, Gentry and Halevi (2009) proposed a completely secure HIBE scheme by means of identity-based broadcast encryption with key randomization, and Waters (2009) achieved complete security in systems under a straightforward assumption by using a dual system encryption [2].

B. Attribute-Based Encryption

Sahai and Waters (2005) introduced the concept 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 [4]. The attributes are used to describe the ciphertext since the access structure is specified in the private key. This scheme is characterized as key-policy ABE (KP-ABE). Bethencourt et al. (2007) introduced a ciphertext-policy ABE (CP-ABE) scheme, in which the roles of the ciphertext and keys are inverted in contrast with the KP-ABE scheme. Muller et al. (2008) created 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 [5]. 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.).

II. Motivation

Our main design goal is to assist the enterprise users to efficiently and securely share confidential information on cloud servers. High performance, practicability, fine-grained access control, and scalability can be achieved using this model in cloud storage.

A. Master Key and User Key Association Model

In current systems private key generation algorithms/techniques are used. So it creates the problem of key storage and key transfer each time. It is very difficult to maintain the keys for large number of files in cloud storage. As the key is generated based on hierarchical attributes entered by user the HABE (Hierarchical Attribute Based Encryption algorithm) scheme will generate the keys on one machine which can act as server and send it for encryption/decryption. So it reduces the overhead of storing/ managing the keys in cloud storage for security purpose.
Corresponding to the hierarchical 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(Trusted third party), and the domains are enterprise users.

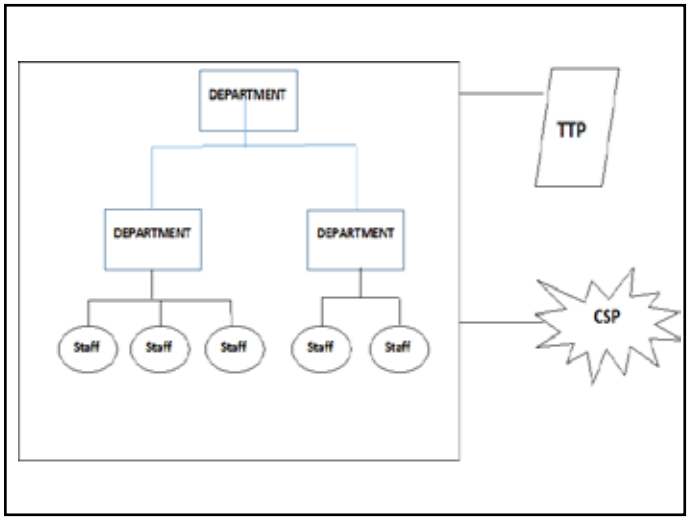

Fig. 1: Hierarchical Model

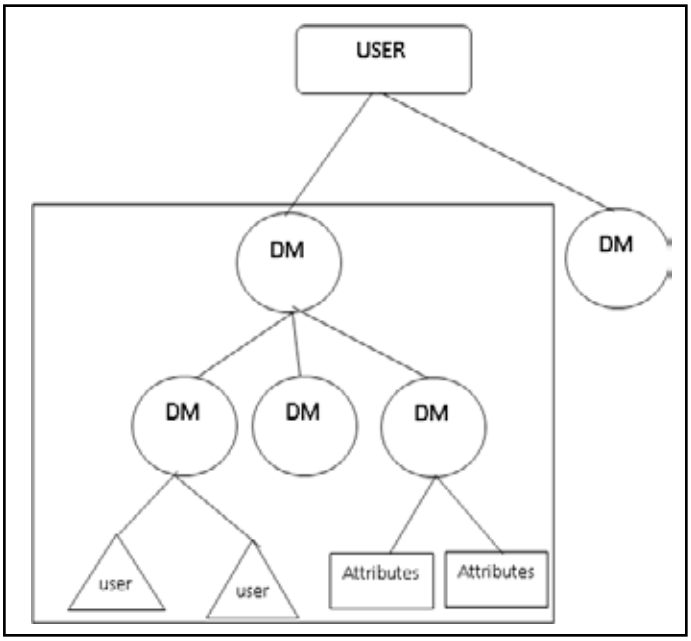

Fig. 2: HABE Model for Encryption

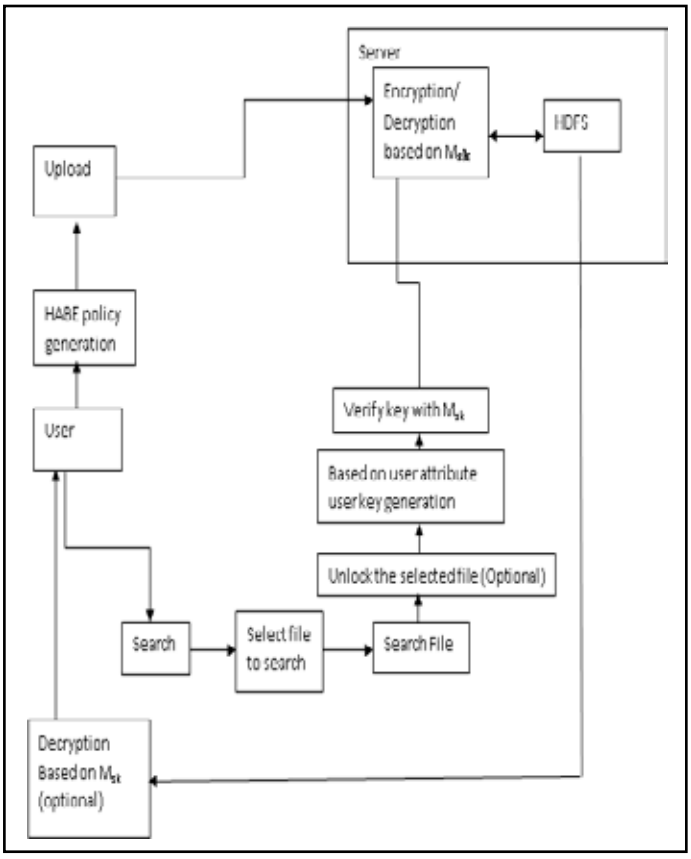

Fig. 3: System Model

IV. Working of Master Key and User Key Association Model

Whenever user wants to upload the file on cloud storage first HABE policy is generated based on user attributes. Based on hierarchical attributes master key Msk is generated. Based on master key file is encrypted and stored on HDFS on server side. If user wants to search the file for downloading the user have to login first to check the authority with user attribute key and Msk of respected file. Then authorized user can select the file for downloading. User can unlock the file if necessary. Based on user attribute user select the file for downloading. User key is verified with Msk .i.e It will find associate key if valid. If it is valid then only on Msk and user can download it from cloud. For Master key generation i.e. Msk levels are created at the time of user registration and based on levels Msk will be created.

As master key is generated based on hierarchical attributes and levels are created for generation of master key Msk for each file. So it is more secure than existing systems. At the time of decryption user key is generated based on user attributes. Msk and user key is associated and if it is valid then only file is available for decryption or downloading. Master key is generated based And,OR conditions as hierarchical attributes are used.

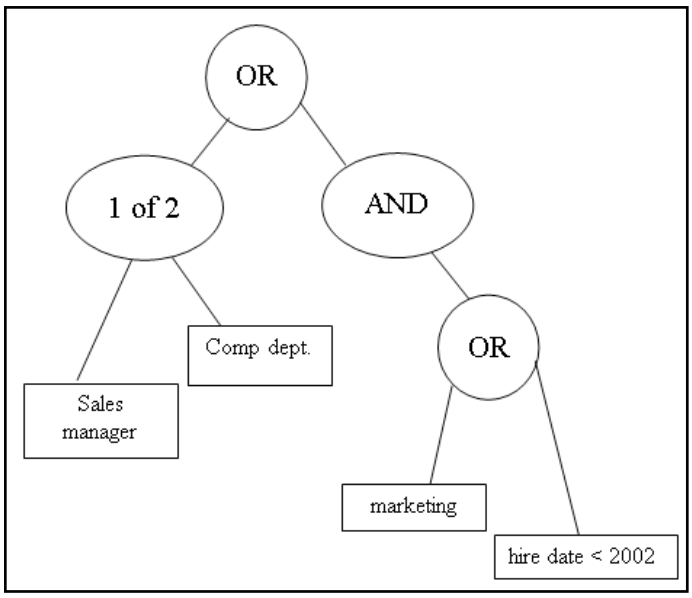

Fig. 4: Master Key Generation

V. System Level Description

The process consists of following components:

A. System Setup

Core setup contains hadoop architecture for file storage and better security. Hadoop structure can implement various features for data storage. For ex.. Facebook database storage which is used by millions user every day.

B. Key Generation Server

It is third party server which can generate Msk(Master Key) for each file based on hierarchical attributes and levels created by user.

C. User

Authorized user can use cloud storage. Msk and user key association can give better security for uploading and downloading files from cloud storage.

VI. Conclusion

Master key and User key association model can be used to maintain the security of files with individual Msk for each file. Data integrity can be achieved through association of user key and Msk of each file. Authorized user can upload or download any type of file from cloud server. Key generation time can vary based on number of attribute levels created for that file and size of the file.

References

[1] Boneh D, Boyen X, Goh E.,"Hierarchical identity based encryption with constant size ciphertext", In: Proceedings of EUROCRYPT. LNCS, Vol. 3494, 2005, pp. 440-56.

[2] Gentry C, Halevi S.,"Hierarchical identity based encryption with Polynomially many levels", In: Proceedings of TCC. LNCS, Vol. 5444, 2009, pp. 437-56.

[3] Gentry C, Silverberg A.,"Hierarchical ID-based cryptography", In: Proceedings of ASIACRYPT. LNCS, vol. 2501, 2002, pp. 548-566.

[4] Goyal V, Pandey O, Sahai A, Waters B.,"Attribute-Based encryption for fine-grained access control of encrypted data", In: Proceedings of CCS, 2006, pp. 89-98.

[5] Muller S, Katzenbeisser S, Eckert C.,"Distributed attribute-based encryption", In: Proceedings of ICISC, 2008, pp. 20-36.

[6] 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. 735-737.

[7] Waters B.,"Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions", In: Proceedings of CRYPTO. LNCS, Vol. 5677, 2009, pp. 619-36.

[8] Guojun Wang, Qin Liu, Jie Wu, Minyi Guo,"Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers in "computers & security "(Elsevier)", 30 (2011), pp. 320-331

[9] Ms.Rohini G. Khalkar, Prof. Dr. S.H.Patil,"Data Integrity Proof Techniques in cloud storage", In: International Journal of Computer Engineering and Technology (IJCET), Vol. 4, Issue 2, March-April 2013, pp. 454-458.

[10] Zhiguo wan, Jun'e Liu, Robert H. Deng,"HASBE: A Hierarchical Attribute Based Solution for flexible and scalable access control in cloud computing".

Rohini G. Khalkar has received her B.E degree in Computer from N.D.M.V.P. Samaj's College of Engineering, Nasik, India in 2008, the MBA degree in Information Technology from Bharti Vidyapeeth Deemed University, Pune, India in 2011 . She is MTech Computer Student in Bharti Vidyapeeth Deemed University College of Engineering, Pune.

Prof. Dr.S.H.Patil, has received his B.E degree in Computer from Walchand Institute Of Technology, Shivaji University ,Sangli,India in 1989, the M.E degree from government college of engineering, Pune, India in 1992, the Ph. D from Bharti Vidyapeeth Deemed University, Pune, India in 2009. He is the Body member of All India Technical Education, World Scietific Engineering and academics society, International association of computer engineering, Association of electronics and electrical engineering etc. He has joined Bharti Vidyapeeth University College Of Engineering in 1991 and working as Head Of Department ,Computer Engineering from 2000 till date.