Attribute-Based approach for Flexible Access control in Cloud Computing with Hierarchical Structure

Auhtor 1: Shaikh Sadaf Ahmed, Author 2: Prof. Dipti Patil

Department of Computer Engineering, Pillai College of Engineering New Panvel, University of Mumbai, Maharashtra, India

Abstract----Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Attribute-based encryption (ABE) has been envisioned as a promising cryptographic primitive for realizing secure and flexible access control. HASBE extends the ASBE algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control of ASBE.

Index Terms----HASBE (Hierarchical Attribute set based Encryption), CPABE (Cipher text- Policy Attribute Based Encryption), MK (Master Key), PK (Public Key), SK (Secret Key), CT (Cipher Text), CS (Cloud server), CSP (Cloud service provider).

1 INTRODUCTION

THE Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper. We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Attribute-based encryption (ABE) has been envisioned as a promising cryptographic primitive for realizing secure and flexible access control. HASBE extends the ASBE algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control of ASBE. In cloud computing, users have to be compelled to hand over their knowledge to the cloud service supplier for storage and business operations, whereas the cloud service supplier could be a business entity which cannot be totally trusted. Knowledge is a vital plus to any organization, and enterprise users can face significant issue if its confidential knowledge is disclosed to their business competitors or the general public. Thus the cloud users within the first place need to create certain that their

knowledge are unbroken confidential to the outsiders together with the cloud suppliers and their potential competitors. This is often the primary knowledge security demand. Versatile and fine grained access control is additionally powerfully desired within the service oriented cloud computing model.

1.1 EXISTING SYSTEM

ASBE (Attribute based mostly Encryption) theme. Sahai associated Waters describe a theme within which a sender will write in code a message specifying an attribute set and variety d in order that solely a recipient United Nations agency has a minimum of d of the given attributes will decode the message. There is, however, one major limitation to the SW theme. In their scheme, the user must go to a trusted party so as to obtain a secret key which will allow him to decode the messages. [6], [1]

In this case, each user must go to the trusted server, prove that he has a certain set of attributes, and then receive secret keys corresponding to each of those attributes. However, this means we must have one trusted server who monitors all attribute. In reality, we have 3 different entities responsible for maintaining this information. ABE schemes are classified into key-policy attributebased encryption (KP-ABE) and cipher text-policy attribute-based encryption (CP-ABE). In KPABE model [3], when a user requests a private key, the authority determines what combinations of attributes must be present in order for this user to decrypt and gives the user the corresponding private key.

CP-ABE is much more flexible than plain identity-based encryption, in that it allows complex rules specifying which private keys can decrypt which cipher texts. Specifically, the private keys are associated with sets of attributes or labels, and when we encrypt, we encrypt to an access policy which specifies which keys will be able to decrypt.

1.2 OBJECTIVE

The proposed system shows how HASBE extends the ASBE algorithm with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of finegrained access control of ASBE. Second, we demonstrate how to implement a full-fledged access control scheme for cloud computing based on HASBE. The scheme provides full support for hierarchical user access , file creation, file deletion, and user revocation in cloud computing. Third, we formally prove the security of the proposed scheme based on the security of the CP-ABE scheme by analyzing its performance in terms of computational overhead. Lastly, we implemented HASBE system and conducted result analysis experiments for performance evaluation, and our experiments demonstrate that HASBE gives satisfactory performance. we also measures the time complexity i.e. time required to upload and download the files on cloud.

2 REVIEW OF LITERATURE

The literature survey contains study of different schemes and research papers available on attribute based encryption scheme.

HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in cloud computing.

This paper presents the new scheme i.e. HASBE which provides the flexible and scalable access control in cloud computing. The HASBE extends the ASBE scheme with hierarchical structure and hence achieves scalability and flexibility.

A Novel Method of HASBE with Improved Efficiency and Delegation Mechanism in Cloud.

The novel method of HASBE introduces in term of delegation mechanism and improved efficiency. It provides efficiently share confidential data on cloud servers and also involves in full delegation.

The delegation defines that it involved for the transfer of authority under server permission.

A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing.

This paper proposes the observation of separating authority is often applied in business management. For example, responsibility for a company's finances is divided between the accountant and cashier. In business processes, the accountant is responsible for keeping accounts, while the cashier is in charge for making payments. By keeping these two functions divide, the company can prevent the accountant from misrepresenting accounts and embezzling corporate finances. Authorized documents frequently need to be stamped with two seals (i.e., the corporate seal and the legal representative's seal), thus avoiding a staff member from abusing his position to issue fake documents, and these seals are normally delegated to two dissimilar people. These examples of the division of authority are designed to avoid a concentration of power which could raise operational risks this paper also proposes the HASBE scheme and operations of the same.

An Enhanced HASBE for Cloud Computing Environment.

This paper proposes advantages of the HASBE scheme and enhancement of the same.

A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments.

In this paper, the survey started from basic attribute-based encryption scheme, followed by monotonic access structure which could be divided into key-policy attribute-based encryption scheme, cipher text-policy attribute-based encryption scheme. Attribute-based encryption scheme with non- monotonic structure is introduced. Thereafter, and hierarchical attribute-based encryption scheme as the end.

GASBE: A Graded Attribute-Based Solution for Access Control in Cloud Computing

This paper proposes the detailed system model of the HASBE scheme. System model consists of CSP, Data owner, Data consumer, Trusted Authority, Domain Authority.

A Survey on Attribute Based Encryption Scheme in Cloud Computing.

This paper proposes a method of encryption of a data based on the attributes of it.in this trusted authority, authorizes each user. The ABE proposes two more schemes i.e. KP-ABE and CP-ABE.

3 IMPLEMENTATION AND ALGORITHM

3.1 SYSTEM ARCHITECTURE

The system focuses on a proposed architecture Hierarchical Attribute Set Based Encryption (HASBE); which is derived from the Cipher Policy attribute-based encryption (CP-ABE) with a hierarchical data structure. This proposed approach not only achieves scalability, it achieves both flexibility and fine-grained access control of data in cloud.

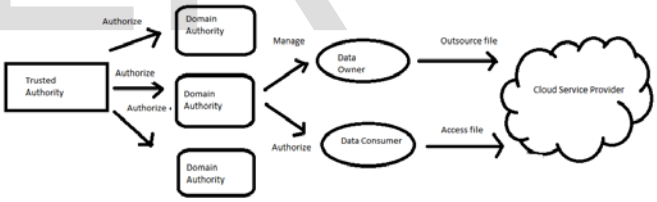

Fig 3.1 System Architecture

In Fig. 3.1, the system consists of five form of parties: a cloud service provider, data owners, data consumers, a number of domain authorities, and a trusted root authority. The cloud service provider manages a cloud to supply data storage service. Data owners encrypt or encode their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the

trusted authority are organized in a hierarchical manner. The proposed HASBE system expands the attribute based scheme to provide the hierarchical structure of system. As our system model consists of a trusted authority, multiple domain authorities, and numerous data owners and consumers. [4]

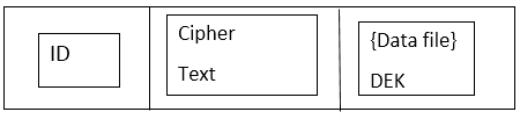

Fig 3.2 Format of data on cloud

The trusted root authority is responsible for authorizing top level domain authorities. A domain authority is responsible for authorizing the next level domains or the users in its domain. Each user in the system is allocated a key structure which specifies the attributes associated with the user's decryption key. Fig. 3.2 represents data file format of cloud.

3.2 ALGORITHMS USED

BLOWFISH ALGORITHM:

It has total 16 rounds of encryption. Each round consists of key-dependent permutation and a key and data-dependent substitution. All the operations are XORed and addition of 32 bit words. The only additional operations are four indexed array data lookup tables for each round. Initially it divides the original message into 64 bit blocks and each 64 bit blocks are processed individually.

Step1: Initially it divides the 64 bit block into two parts xL and xR of 32 bit each

Step2: At first round, xL is XORed with the subkey p1 sub key and result of XOR operation is given to Blowfish Function which again gets XORed with the xR.

Step3: xL and xR both are swapped together.

Step 4: the process continues till 16th round.

Step 5: After 16th round, xR is XORed with the p17 sub key and xL is XORed with the p18 sub key.

Step 6: Result of both XOR opration is combined together to generate 64 bit ciphertext.

Algorithm:

Divide x into two 32-bit parts: xL, xR
For i = 1 to 16
xL=XL XOR Pi
xR=F(XL) XOR xR
Swap XL and xR
Swap XL and xR(undo the last swap)
xR=xR XOR P17
xL=xL XOR P18
Recombine xL and xR

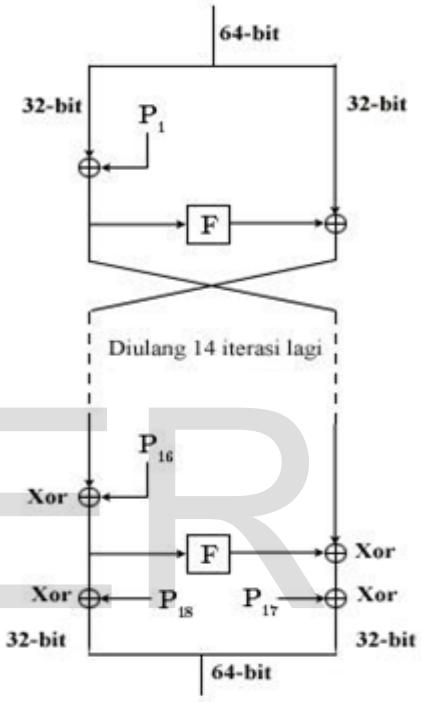

Fig 3.3 Blowfish Algorithm

MAC FOR DATA INTEGRITY:

The MAC needed two inputs a message and a secret key known only to the originator of the message. The receiver of the message verifies the integrity of the message and authenticate that the message sender has the secret key. The Hash function is used to generate the MAC. The MAC is generated by calculating the hash value of secret key and a message to be authenticated. The sender sends the message along with the calculated MAC value which will be encrypted with the secret key. At the receiver side receiver will decrypt the message with secret key and again recalculate the MAC and compares it with the MAC value send by the sender. If receiver's calculated MAC and MAC which

is send by the sender is same then the message is authenticated and the data is verified. We have used Hash MAC (SHA) algorithm for calculating the Hash function.

Definition: HMAC(M)=H[(K+opad) || H(K+ipad) || M]

4 RESULT AND PERFORMANCE ANALYSIS

4.1 PERFORMANCE ANALYSIS:

We analysed the system based on the time complexity that means the total time required to upload and download the file from the cloud. To measure the time complexity we have calculated the time required for files based on the size of the file. We have tested AES and DES Algorithms with our Blowfish algorithm, and checked the total time required to AES algorithm, DES algorithm and total time required for encryption and decryption in Blowfish algorithm for various files. Based on above comparisons we have found that the Blowfish algorithm works better instead of AES and DES algorithm

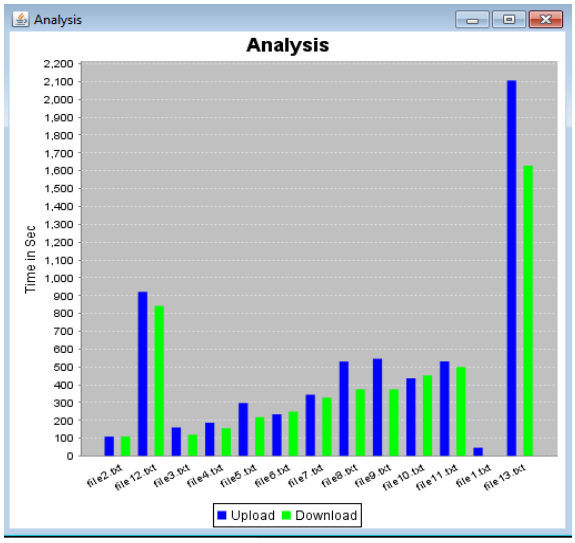

Fig 4.1 Time required for AES algorithm

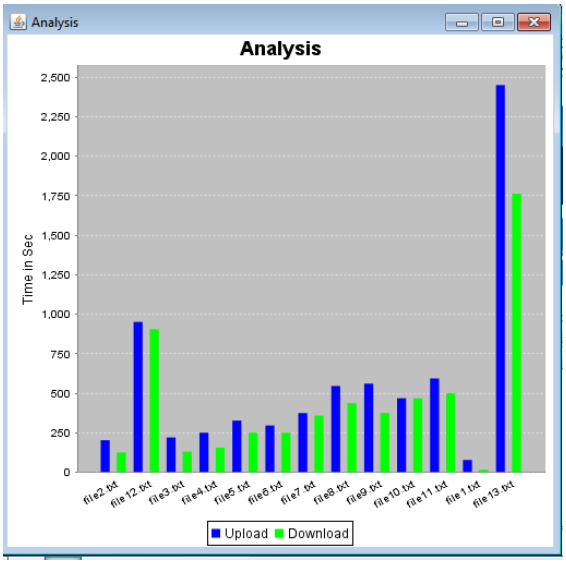

Fig 4.2 Time required for DES Algorithm

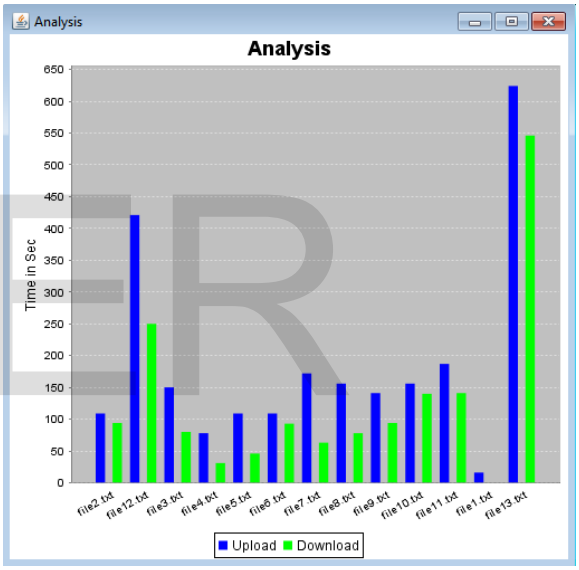

Fig 4.3 Time required for Blowfish algorithm

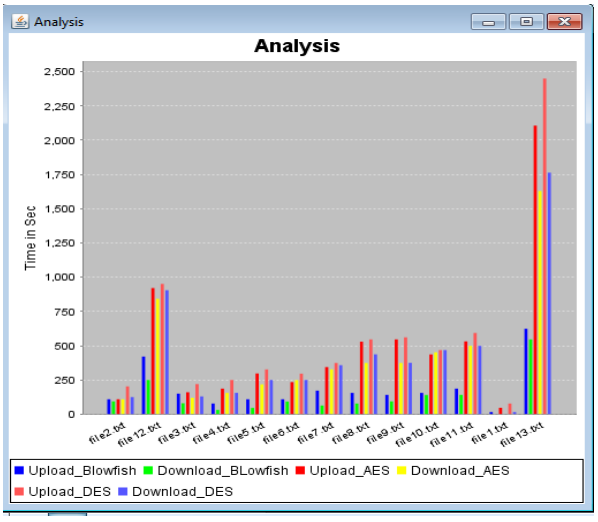

Fig 4.4 Comparative Analysis

As per the analysis we have tested we can say that the time required fir AES algorithm is more than the Blowfish algorithm. For every processed file it generates the new graph which shows the time required for both algorithm and comparison of both of them.

5 ACKNOWLEDGEMENT

It is a great pleasure and moment of immense satisfaction for me to express my profound gratitude to my dissertation Project Guide, **Prof. Dipti Patil** whose constant encouragement enabled me to work enthusiastically. My heartfelt gratitude to the H.O.D of COMPUTER ENGINEERING Department **Prof. Madumita Chatterjee** and M.E coordinator **Prof. Sharvari Govilkar** who have always been there to help and give their time and advice in spite of their busy schedule. I am also thankful to **Dr. R. I. K Moorthy**, Principal, Pillai collegeof Engineering, New Panvel, for his encouragement and for providing an outstanding academic environment, also for providing the adequate facilities. I acknowledge all the staff members of the department of Computer and Information Technology for their help and suggestions during various phases of this project work.

6 CONCLUSION

We proposed a scheme for providing scalable, efficient and flexible access control in cloud computing. The hierarchical nature of HASBE scheme provides more scalability than the previous ABE (Attribute Based Encryption) schemes. It not only supports the compound set of attributes due to flexible attribute set combinations, but also achieves efficient user revocation. We proved that the security of proposed system HASBE is better than the security of CP-ABE and KP-ABE methods.

Finally we conducted the Result analysis and evaluation, which shows its efficiency and advantages over the existing system. In the proposed system, we also checked data integrity by using HMAC algorithm, which shows data stored on cloud is safe and confidential.

7 REFERENCES

[1] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3 "A Survey on Attribute Based Encryption Scheme in Cloud Computing" international Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013

[2] D. Hephzi Rachel1, S. Prathiba2 "An Enhanced HASBE for Cloud Computing Environment" A Monthly Journal of Computer Science and Information Technology IJCSMC, Vol. 2, Issue. 4, April 2013 ,pg 396-401

[3] Chandana.V.R, Radhika Govankop,Rashmi N and R.Bharathi "GASBE: A GRADED ATTRIBUTE-BASED SOLUTION FOR ACCESS CONTROL IN CLOUD COMPUTING" International conference on Advances in Computer and Electrical Engineering (ICACEE 2012) Nov 17-18, 2012 Manila(Philippines)

[4] 1S. Gokuldev, 2S.Leelavathi 1Associate Professor, 2PG Scholar 1,2Department of Computer Science and Engineering 1,2SNS College of Engineering, Coimbatore, India "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing" International Journal of Engineering science and innovative Technology, Volume 2, Issue 3, May 2013

[5] Cheng-Chi Lee1, Pei-Shan Chung2, and Min-Shiang Hwang3 "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments" Department of Computer Science and Information Engineering, Asia Universtiy3 500 Liufeng Road, Wufeng, Taichung 402, Taiwan, R.O.C. International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013

[6] MANJEERA PATIL, 2A. SURESH BABU 1PGScholar, JNTU, Pulivendula, 2P.hd, Asso. Professor, JNTU , Pulivendula "HASBE: A HIERARCHICAL ATTRIBUTE-BASED SOLUTION FOR FLEXIBLE AND SCALABLE ACCESS CONTROL IN CLOUD COMPUTING" International journal of Electrical, Electronics and Computer system ISSN (online) 2347-2812, Volume -1, Issue -3, 2013

[7] S.Dhivya bharathi1 S. Sathyalakshmi 2 "A Novel Method of HASBE with Improved Efficiency and Delegation Mechanism in Cloud" Proc. of the Intl. Conf. on Recent Trends In Computing and Communication Engineering -- RTCCE 2013 Copyright © Institute of Research Engineers and Doctors ISBN:978-981-07-6184-4-doi:10.3850/978-981-07-6184-4_16

[8] http://www.slideshare.net/IMPULSE_TECHNOLOGY/hasbe-a-hierarchical-attribute-basedsolution

[9] http://www.youtube.com/watch?v=DnBF2rY6vX0/hasbe.html