IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014
ISSN : 2348 - 6090
www.IJCAT.org

Secure Sharing of Data over Cloud Computing using Different Encryption Schemes An Overview

[1] Raseena M , [2] Harikrishnan G R

[1] PG Scholar , [2] Asst. Professor, Computer Science And Engineering
MES College of Engineering, Kuttipuram ,Kerala, India

Abstract - Cloud computing has been envisioned as the de-facto solution to the rising storage costs of IT Enterprises. With the high costs of storage devices as well as the huge amount of data is being generated it proves costly for enterprises or individual users to frequently update their hardware. Data outsourcing to the cloud helps in reduction in storage costs and reducing the maintenance. Cloud storage stores the users data to large data centers, which are remotely located. User does not have any control on those centers .This feature of the cloud poses many security issues and need to understand and solve this problem. Data security is the most important challenges in cloud computing. To assure the clients control over access to their own data's, it is a promising method to encrypt the data's before outsourcing. So many issues are remained for achieving fine grained data access control. Such as scalability in key management, flexible access, efficient user revocation and privacy problems. So many encryption techniques are used for achieving these features. To achieve fine-grained and scalable data access control for client's data, different attribute-based encryption (ABE) techniques are used.
.

***Keywords* - Cloud computing, Data privacy, Fine grained access control, Attribute based encryption.**

1. Introduction

In cloud computing model users have to give access to their data for storing and performing the desired business operations. Hence cloud service provider must provide the trust and security, as there is valuable and sensitive data in huge amount stored on the clouds. There are concerns about flexible, scalable and fine grained access control in the cloud computing. For this purpose, there have been many of the schemes, proposed for encryption. Such as Public key encryption, Attribute-Based Encryption (ABE) schemes[1] and how it has been developed and modified further into Key Policy Attribute based encryption (KP-ABE) , Cipher-text Policy At- tribute Based Encryption (CP-ABE[2][4]) and further it has been proposed as CP-ASBE and further- more HABE,HASBE and MA ABE so on.

This is according to how flexible, scalable and fine grained access control [10] is provided by each scheme.

2. Overview

Data outsourcing to cloud storage servers is raising trend among many firms and users owing to its economic advantages. Data storage security is the major issue in the cloud storage. So securely outsourced the data to the cloud, different encryption schemes are used.

3. Different Encryption Schemes

3.1 Public Key Encryption (PKE)

In this scheme plain text is converting into cipher text using public key. Then sender gives the cipher text for you and using your private key you can decrypt it. It is simple but main disadvantage of this scheme are uses up more computer resources, if an attacker determines a person's private key, his or her entire messages can be read and the loss of a private key means that all received messages cannot be decrypted.

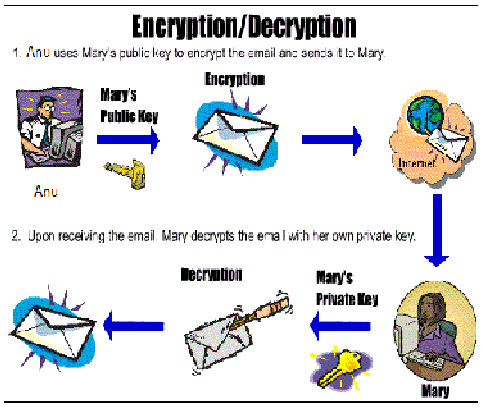

Fig 1: Public Key Encryption/Decryption

3.2 Identity Based Encryption (IBE)

IBE sender can encrypt a message using only identity without need of public key certificate. Common feature of IBE is that they view identities as a string of characters.

In IBE [7], ones publicly known identity (ex. email address) is being used as his/her public key where as corresponding private key is generated from the known identity. IBE [7] encryption scheme is a four algorithms/steps scheme where the algorithms are

a. Setup Algorithm
b. Key(private key)Generation Algorithm
c. Encryption Algorithm
d. Decryption Algorithm.

The main issues in this scheme are key management and no key revocation.

In Fuzzy identity based encryption view identities as a set of descriptive attributes. So in this scheme the error problems related to identities in IBE is solved.

Two interesting application of Fuzzy IBE are

a. Identity based encryption system that uses biometric identities.eg: iris scan.
b. It is used in Attribute based encryption.

3.3 Attribute Based Encryption (ABE)

Sahai and Waters [1] first introduced the attribute based encryption (ABE) for enforced access control[5] through public key cryptography. The main aspects are to provide flexibility, scalability and fine grained access control. In ABE scheme both the user secret key and the cipher text are associated with a set of attributes.

Suppose the Attribute sets are Computer Science, Male and age>40.Tree access structure for this is shown in Fig 2.

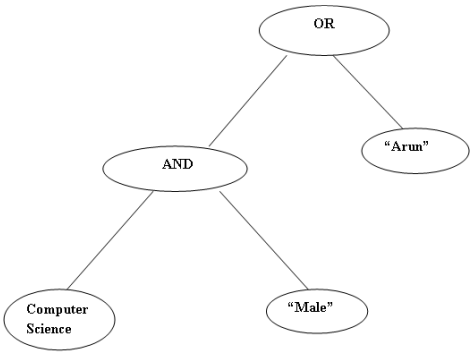

Fig 2: Access Structure for ABE

In Fig 2 interior node consists of AND and OR gates and leaves consists of different attributes. Attribute sets that satisfy the tree can reconstruct the secret message and access it.

In classical model, this can be achieved only when user and server are in a trusted domain. So different alternatives of ABE are introduced.

3.4 Key Policy Attribute Based Encryption (KP-ABE)

To enable more general access control, V. Goyal, O. Pandey, A. Sahai, and B. Waters [8] proposed a key-policy attribute-based encryption (KP-ABE) scheme. It is the modified form of classical model of ABE. In KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. In KP-ABE, a set of attributes is associated with cipher text and the user's decryption key is associated with a monotonic access tree structure [5]. When the attributes associated with the cipher text satisfy the access tree structure, then the user can decrypt the cipher text.

Limitations of KP-ABE are Encryptor cannot decide who can decrypt the encrypted data, it is not suitable for certain applications such as sophisticated broadcast encryption and it provide fine grained access but has no longer with flexibility and scalability.

3.5 Cipher text Policy Attribute Based Encryption (CP-ABE)

Sahai et al.[2] introduced the concept of another modified form of ABE called CP-ABE[2][4][1] that is Cipher- text Policy Attribute Based Encryption. In CP-ABE scheme, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. In a CP-ABE scheme, a cipher text is associated with a monotonic tree structure [4] and a user's decryption key is associated with set of attributes.

Limitations of this scheme are: it cannot fulfill the enterprise requirements of access control which require considerable flexibility and efficiency.

3.6 Hierarchical Attribute-Base Encryption (HABE)

This scheme (HABE) proposed by Wang et al [10].It is a combination of Hierarchical Identity Base Encryption(HIBE) and CP-ABE. It provides fine grained access control, full delegation and high performance.

The HABE scheme consists of many attribute authorities and many users. ABE uses disjunctive normal form policy. The same attribute may be administrated by multiple domain masters according to specific policies, which is most complicated to implement in practice.

HABE [12] model consists of a Root Master (RM) and multiple domains. One domain consists of number of domain masters and number of users related to end users. HABE model is shown in figure 3.

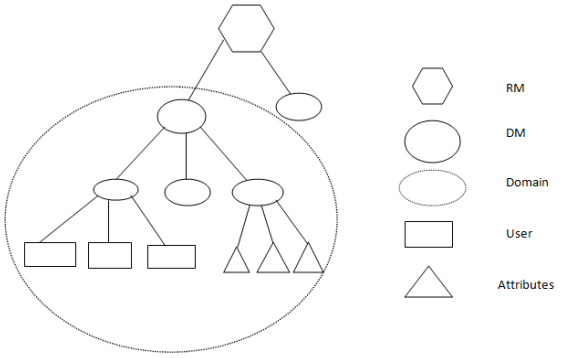

Fig 3: HABE model

It is mainly applicable to the environment of enterprises sharing data in cloud.

This scheme has issues with multiple values assignments and practical implementation is very difficult because same attribute may be administered by different domain masters.

3.7 Hierarchical Attribute Set Based Encryption(HASBE)

HASBE scheme is proposed and implemented by Zhiguo Wang et al [10].This scheme extended the ASBE scheme to handle the hierarchical structure of the system. HASBE model is shown in Fig 4.

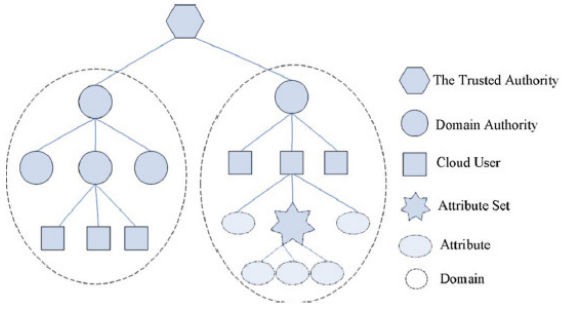

Fig 4: HASBE model

In this model trusted authority is responsible for managing top level domain authorities. Each user in this system is assigned a key structure.

This scheme provide scalable, flexible and fine grained access control in cloud computing. Efficient user revocation can be done in this scheme due to attribute assigned multiple values.

3.8 Multi-Authority Attribute Base Encryption (MA-ABE)

This scheme consists of many attribute authorities and many users. Attributes key generation algorithm will run the authority and result will send to the user. In a multi-authority ABE[3][9] scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase [11] gave a multi- authority ABE scheme which supports many different authorities operating simultaneously, each handling out secret keys for a different set of attributes.

4. Performance Analysis

Different encryption schemes are overviewed in this paper. If the data's are stored in cloud, better is attribute based encryption. Classical attribute based encryption have some problems. So different variations of ABE are analyzed. Following Table1 shows the performance of different scheme based on these criteria.

Table 1: Performance analysis of different ABE schemes

Parameters v/s ABE Technique	**Fine-grained access control**	**Efficiency**	**Computational Overhead**
KP- ABE	Low, High if there is re encryption technique	Average, high for broad cast type system	Most of computational overheads
CP- ABE	Average realization of complex	Average, not efficient for	Average computational overheads

	access control	modern enterprise environment	
HABE	Good access control	Flexible and scalable	Some of overhead
HASBE	Better access control	Most efficient and flexible	Less overhead
MA ABE	Fine grained access control	Better efficient than others	Lesser overhead than others and better revocation

Based on different criteria's such as efficiency and access control analyzed and from that MA_ABE is better than other schemes.

5. Conclusion

Data security is the major problem in cloud storage. For securing outsourced data different encryption schemes are used. If the data's are moved to the cloud advanced encryption schemes are needed. So overviewed different attributes based encryption (ABE) schemes that can be used in cloud systems for flexible, scalable and fine grained access control. In ABE scheme, there are both the secret key and cipher text are associated with a set of attributes. Different variation of the ABE is used for better access control and security. Out of these schemes, find out that the MA-ABE scheme provides more scalable, flexible and fine-grained access control than any other schemes in cloud computing.

References

[1] J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Out- sourcing Systems", IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, 2011.

[2] X. Liang, R. Lu, X. Lin, and X.S. Shen, "Cipher- text Policy Attribute Based Encryption with Ef- ficient Revocation", technical report, Univ. of Waterloo, 2010.

[3] M. Chase and S.S. Chow, " Improving Pri- vacy and Security in Multi-Authority Attribute- Based Encryption", Proc. 16th ACM Conf. Computer and Comm. Security (CCS 09), pp 121-130 ,2009.

[4] J. Bethencourt, A. Sahai, and B. Waters," Ciphertext-Policy Attribute-Based Encryption " Proc. IEEE Symp. Security and Privacy (SP), pp. 321-334 ,2007.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "At- tribute Based Data Sharing with Attribute Re- vocation", Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS 10) 2010.

[6] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute- Based Threshold Decryption with Flexible Del- egation and Revocation of User Attributes", IEEE Trans.Image process,Jun, 2009.

[7] A. Boldyreva, V. Goyal, and V. Kumar,"Identity-Based Encryption with Efficient Revo- cation", Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Wa- ters, "Attribute-Based Encryption for Fine- Grained Access Control of Encrypted Data", Proc. 13th ACM Conf. Computer and Comm. Security (CCS 06), pp. 89-98, 2006.

[9] Ming Li, Shucheng Yu,Yao Zheng, Kui Ren, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", Ieee transaction on parallel and distributed sys- tems,vol.24,no.1,january , 2013.

[10] G.Wang, Q. Liu, and J.Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services", in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL , 2010.

[11] Melissa Chase, "Multi-authority Attribute Based Encryption", In TCC, volume 4392 of LNCS, pages 515534.

[12] Guojun Wang,, Qin Liu,, Jie Wub, Minyi Guo c "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers".

Raseena M received the Bachelor's degree in Computer science and Engineering from the Mahatma Gandhi University, Kerala in 2008. Presently she is pursuing her M.Tech in the department of Computer Science and Engineering from Calicut University, Kerala. She has industry experience of three and half years. Her research interests include data security in cloud computing, cryptography and mobile cloud computing etc.

Harikrishnan G R is an Assistant Professor in Department of Computer Science and Engineering at MES College of Engineering,Kuttipuram.He received Bachelor's degree in Information Technology from Kerala University and ME in Computer Science and Engineering from Anna University, Chennai. He has a teaching experience of two and half years. His research area includes cloud computing, mobile cloud computing and cloud security.