International Conference on Advances in Materials, Computing and Communication Technologies
In Association with International Journal of Scientific Research in Science and Technology
Volume 9 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)

A Survey on Attribute Based Encryption Techniques

S. Shiny[1], Dr. J. Jasper[2], Dr. M. R. Geetha[3]
[1]Department of Computer Science, Ponjesly College of Engineering, Tamil Nadu, India
[2]Department of EEE, Ponjesly College of Engineering, Tamil Nadu, India
[3]Department of ECE, Ponjesly College of Engineering, Tamil Nadu, India

ABSTRACT

Cloud computing is a currently emerged computing paradigm . The data stored and transferred in cloud are enormous and valuable. Privacy and security becomes the significant factors in protecting the data. Fine grained ,scalable access control should be maintained in the cloud.Many schemes have been proposed and implemented for access control and security. In this paper we are going to explore various schemes for Attribute Based Encryption (ABE) and its various types.

Keywords – Access control, Attribute Based Encryption, Key policy, ciphertext policy

I. INTRODUCTION

Cloud computing is becoming undeniable part of modern information and communication system. The data stored in cloud is very sensitive so security and privacy are very important issues in cloud computing. Cloud storage requires flexible, scalable and fine grained access control. To ensure the controllable, secure sharing in the data, encryption mechanisms are used.

There have been many of the schemes proposed for encryption. In this paper we are going to discuss about Attribute Based

Encryption (ABE) schemes and its further modified types.

II. LITERATURE REVIEW

2.1. Attribute based encryption(ABE):-

Attribute based encryption (ABE) was introduced by Sahai and Waters in 2005 [1]. ABE is the generalization of Identity Based Cryptography, and is the public key cryptography technique that uses one to many encryption. Attribute Based Encryption (ABE) designed for ensuring encrypted fine grained access control for outsourced data and it uses attributes as identities for both encryption and decryption of data. ABE uses a set of four algorithms as follows:

- Setup
- Key generation
- Encryption
- Decryption

2.2. Key policy Attribute based encryption(KP-ABE):-

Goyal et al.[2] proposed key Policy Attribute based encryption(KP-ABE), the modified form of ABE. In KP-ABE attribute policies are associated with keys and the data is associated with attributes.

KP-ABE scheme is based on four algorithms:

- Setup
- Keygen
- Encrypt
- Decrypt

The attribute authority executes the setup algorithm and is also responsible for generating the secret key, and is run by the Keygen algorithm. The data owner apply the Encrypt algorithm to encrypt the data to ciphertext. Finally the user apply the Decrypt algorithm to decipher data based on secret key.

Eventhough the scheme provides fine grinded access control, it is lacking in some features. The data owner cannot decide on who can decrypt the data. Its not suitable for sophisticated broadcast encryption.

2.3. Cipher text policy ABE(CP – ABE):-

Cipher text policy attribute based encryption is another modified form of ABE and is introduced by Sahai et al.[3] and well described by Rifki et at.[4]. CP-ABE is a reverse model of KP-ABE. In CP-ABE scheme attribute policies are associated with the data and attributes are associated with keys. The keys that are associated with attributes satisfy the policy associated with data are able to decrypt the data. CP-ABE directly embedding the access policy on the cipher text. The data owner have the authority that who can access their encrypted data. The encrypted data can be kept confidential and secure against collusion attacks.

CP-ABE scheme is based on four algorithms:

- Setup
- Keygen
- Encrypt
- Decrypt

The enterprise requirements of access control is not fulfilled in CP-ABE. The user attributes logically organized as single set. So the users can use possible combination of attributes from single set.

2.4. Cipher text policy attribute - set based encryption (CP-ASBE)

CP-ASBE is introduced by Bobba et al.[5] in order to solve the limitation by CP-ABE, where user attributes logically organized as a single set. CP-ABE is an extended form of CP-ABE.

Unlike CP-ABE user attributes organized into a recursive structure in CP-ASBE. The users are allowed to combine attributes from multiple sets with in the given key. Multiple numerical value assigned to given attribute was supported in CP-ASBE.

CP-ASBE scheme is also based on four algorithms:

- Setup
- Keygen
- Encrypt
- Decrypt

The major limitation of this scheme is colluding users from combining attributes from multiple keys.

2.5. Hierarchical Identity Based Encryption(HIBE):-

HIBE is an extended form of IBE[1]. In regular IBE(1-HIBE) scheme private key is distributed by single Private Key Generator(PKG). The PKG distributes private key to all users and primitive ID (PID) as public keys[6].

On order to overcome key management overhead , 2-HIBE scheme is introduced. It consist of domain PKG, root PKG and users. All are associated with the string of PID. The PID and domains PID combined to form users public key and is known as address. A trusted third party (root certificate authority) allows hierarchy of certificates.

2.6. Hierarchical ABE(HABE):-

HABE scheme is derived by Wang et al.[6] for fine grinded access control. HABE scheme is the combination of HIBE and CP-ABE.

HABE assumes all attributes in one conjunctive clause administered by same domain master. The scheme is most complicated to implement in practice . It cannot support compound attributes. Multiple value assignment is difficult in this scheme.

2.7. Hierarchical Attribute Set Based Encryption (HASBE):-

HASBE scheme is proposed byZhiguo Wan et al. [7] , it extends cipher text attribute set based encryption (CP-ASBE or ASBE). HASBE supports compound attributes and it achieves efficient user revocation. The attributes assigned multiple values and works as recursive set based attributes.

The cloud service provider, data owner, data consumer, domain authority and trusted authority are the five types of parties in the system. The data owner and consumer is controlled by the domain authority. And the domain authority is managed by the trusted authority, and it act as the root authority. The system is organized in hierarchical order[8].

The limitation of the system is the domain hierarchy is complex and execution took long time by that the performance of the system is reduced.

2.8. Scalable Cipher text Attribute Based Encryption(SCP – ABE):-

SCP-ABE proposed by J.Wang et al.[9] to manage the communication overhead in the ABE scheme with unscalable access policy. Block linear secret sharing scheme (BLSSS) is used to provide policy managing interface. The scalability of access policy indicates the ability of dynamic updating.

Advantages:-

- Storage cost is low
- Computation and communication overhead of policy updating is less.
- Computation complexity of decryption is reduced.

III.CONCLUSION

In this paper we have analysed various attribute based encryption (ABE) schemes. ABE is used for fine grinded , flexible and scalable access control in cloud computing. Most of the schemes discussed in this paper provides fine grinded and flexible access control but scalability is less pronounced. Thus SCP-ABE provides more scalable ,flexible and fine grinded access control comparing with other schemes.

IV. REFERENCES

[1]. A.Sahai, B.Waters, Fuzzy identity- based encryption , in : Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques,EUROCRYPT'05, Springer-Verlag, Berlin, Heidelberg, 2005, pp. 457- 473.

[2]. V.Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute based encryption for fine grained access control of encrypted data, in Proc. ACM conf. Computer and communication , 2006.

[3]. J. Bethencourt, A. Sahai, and B. Waters ,Ciphertext policy attribute based encryption , in Proceedings IEEE Symposium Security and Privacy , 2007.

[4]. S. Rifki, Y. Park and S.Moon, A fully secure cipher text policy attribute based encryption with a tree based access structure , Journal of Information Science and Engineering, vol 31, pp. 247- 265, 2015.

[5]. R. Bobba, H. Khuranaand, and M.Prabhakaran, Attribute sets: A Practically motivated enhanced to attribute based encryption, in proc. Esorics, Saint Malo, France , 2009.

[6]. 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 Communication Security, 2010.

[7]. Z.Wan , J. Liu, and H. Deng, Hasbe: A Hierarchical attribute based solution for flexible and scalable access control in cloud computing , IEEE Transaction on Information Forensics and security, vol. 7, no. 2, pp. 743-754, 2012.

[8]. D. Hephzi Rachel and S. Prathiba, An enhanced Hasbe for cloud computing environment, International Journal of computer science and mobile computing, vol. 2, pp. 396-401, 2013.

[9]. Jing Wang, Chuanhe Huang, Neal N Xiong, Jinhai Wang, Blocked linear secret sharing for scalable attribute based encryption in manageable cloud storage system, Information sciences, vol. 424, pp. 1-26, 2018