Encryption Schemes for Data Storage in Cloud: A Survey

Sneha Raghavan T
Department of ISE
JSSATE
Bangalore , India
snehatraghavan@gmail.com

Apoorva G
Department of ISE
JSSATE
Bangalore , India
apoorvag30@gmail.com

Kusuma A
Department of ISE
JSSATE
Bangalore , India
kusumaananth@gmail.com

Rekha P M
Assistant Professor, Department of ISE
JSSATE
Bangalore , India
rekha_math@rediff.com

***Abstract*— Cloud computing is one of the emerging technologies, in which hardware resources and software resources of computing infrastructure are provided as service to user over internet. This technology requires users to entrust their data to cloud service providers for the data to be outsourced. The top concern is security and privacy of the outsourced data. Since the data is shared over network proper access control should be maintained. There are many encrypting schemes that provide security in clouds .This paper presents a survey on various attribute based encryption schemes in cloud that provide security and flexibility in dealing with fine grained access control for outsourced data.**

Keywords – Security; Access Control; Encryption schemes.

I. INTRODUCTION

Cloud computing is an emerging technology that uses internet to provide efficient storage and computing services to customers. In recent years cloud computing has attracted widespread attention from IT industries. Different service oriented cloud computing models have been proposed, which includes Infrastructure as a service (Iaas), Platform as a service (Paas), Software as a service (Saas). Benefits of cloud computing are reduced costs, reliability, scalability, flexibility. The business people and entrepreneurs no longer need to invest in hardware or software systems to maintain IT systems. All virtual resources, weather application, hardware, software or data are provided by service providers and users are required to pay only for the services they require.

Security problems in cloud computing become serious obstacles in spite of enormous potential of cloud computing. Due to internet based data storage and management, data security and privacy in cloud are major security concerns. In cloud computing data must be given by user to cloud service provider for storage and business operations.

Cloud service providers are usually enterprises which cannot be usually trusted. Hence cloud users must make sure that their data is kept confidential to outsiders including cloud service providers.

Data confidentiality is not the only security requirement, flexibility and fine grained access controls[8] are also equally important in cloud computing model. This paper focuses on the survey of different attribute based [7] encryption schemes which provide flexible access control and security. Section-II represents the literature survey of various encryption schemes. In section-III we compare various attribute encryption schemes, design issues of access control and security. Section IV concludes with discussions.

Sneha Raghavan.T, Apoorva G and Kusuma A are pursuing 8th semester Bachelor of Engineering, in the Information Science and Engineering (ISE) department at JSS Academy of Technical Education, Bangalore.

Rekha P. M is a faculty, Department of Information Science and Engineering, JSS Academy of Technical Education Bangalore.

II. RELATED WORK

There are different existing schemes that provide security, data confidentiality and access control in cloud computing.

A. Attribute based encryption

Attribute based encryption scheme (ABE) [1,6] was introduced by sahai and waters in 2005. The main goal is access control and security [8] ,in ABE scheme, cipher text are not encrypted to one particular user as in public key cryptography. Rather, both cipher text and user decryption keys are associated with a set of attributes or a policy over attributes. A user is able to decrypt a cipher text only if there is a match between the decryption key and the cipher text.

A crucial security feature of Attribute based encryption is collusion resistance. This scheme lacks threshold semantics expressibility. It does not satisfy the fine grained access control, scalability and user revocation. ABE schemes are classified into two types depending on how attributes and policy are associated with cipher texts and users' decryption keys. They are Key-policy attribute- based encryption (KP-ABE) [1] and Cipher text-policy attribute- based encryption (CP-ABE) [2].

B. *Key policy Attribute based encryption*

In 2006, Goyal proposed a key-policy attribute-based [1] (KP-ABE) scheme as shown in figure 1. Users are assigned with an access tree structure over the data attributes. AND and OR gates are used as interior nodes of the access tree. The Leaf nodes are associated with data attributes. Data is associated with attributes for each of which public key is defined. The secret key of the user is defined to reflect the access structure. A user's decryption key is associated with a monotonic tree access structure. User is able to decrypt a cipher text if the data attributes associated with cipher text satisfy the key's access structure. The use of this encryption scheme KPABE provides fine grained access control.

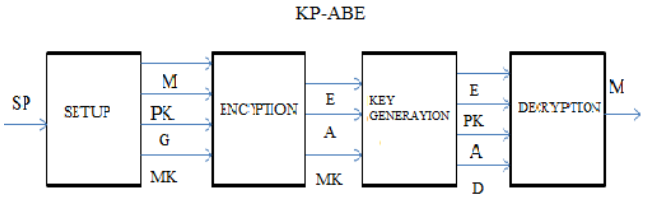

Figure 1: KP-ABE structure

KP-ABE consists of four algorithms.

Setup: This algorithm takes security parameters as input. It outputs PK public parameter and MK master key.

Encryption: This algorithm takes as input a message M, a set of attributes γ, and public parameter PK. Output is cipher text E.

Key Generation: This algorithm takes as input an access structure A, master key MK, public key PK, output is decryption key D.

Decryption: This algorithm takes as input cipher text E, decryption key D, access control structure A, public key PK. It outputs message M if attributes belong to access tree structure.

The drawbacks of KP-ABE is that the access policy is built into an users private key, so data owner cannot choose who can decrypt the data except choosing a set of attributes which can describe this data. It lacks flexibility in attribute management and scalability in dealing with the multiple levels of attribute authorities.

C. *Cipher text Attribute based Encryption*

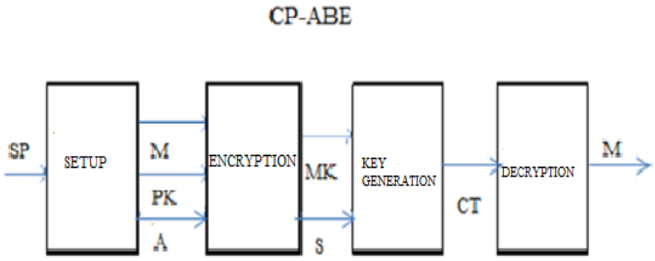

Figure 2: CP-ABE structure

CP-ABE [2] was introduced by Sahai. In CP-ABE scheme the cipher text is encrypted with the tree access policy chosen by encryptor and the corresponding decryption key is created with respect to set of attributes as shown in Figure 2. A user can decrypt cipher text if the set of attributes associated with decryption key satisfies the tree access policy. The concept of this scheme is similar to traditional access control scheme. Hence it is more natural to apply CP-ABE instead of KP-ABE. KP_ABE used attributes to describe the encrypted data and built polices into users keys but in CP-ABE attributes used to describe a users credential and an encryptor encrypting data determines a policy for who can decrypt.

CP-ABE consists of four algorithms:

Setup: This algorithm takes security parameter as input and provides public parameter PK and Master key MK as output.

Encrypt: This algorithm takes as input the public parameter PK, a message M, and an access structure A. The algorithm will encrypt a Message M and produce a cipher text CT, such that only a user that processes a set of attributes that satisfies the access structure will be able to decrypt the message.

Key Generation: This algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

Decrypt: This algorithm takes as input public parameter PK, a cipher text CT, which contains an access policy A and a private key SK. If the set S of attributes satisfies the access structure A, then the algorithm will decrypt the cipher text and return a message M.

The drawbacks of CP-ABE are that it lacks flexibility and efficiency in specifying policies and managing user attributes. In CP-ABE scheme decryption key only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies.

D. *Attribute Set based Encryption*

ASBE is also known as Cipher text Attribute Set Based Encryption [3] (CP-ASBE). To overcome the limitations of CP-ABE, CP-ASBE was introduced by Bobba. ASBE is extended from CP-ABE, which organizes user attributes into a recursive set structure and allows users to enforce dynamic constraints on combining attributes to satisfy a policy. By grouping user attributes into sets, the attributes from same set can be combined freely. CP-ASBE can support compound attributes without sacrificing the flexibility to easily specify policies involving the underlying singleton attributes. Similarly multiple assignments for a given attribute can be supported by placing each assignment in a separate set.

The challenge in constructing a CP-ASBE scheme is selectively allowing users to combine attributes from multiple sets within a given key while still preventing collusion. It also lacks the hierarchical structure.

E. *Hierarchical Identity Based Encryption*

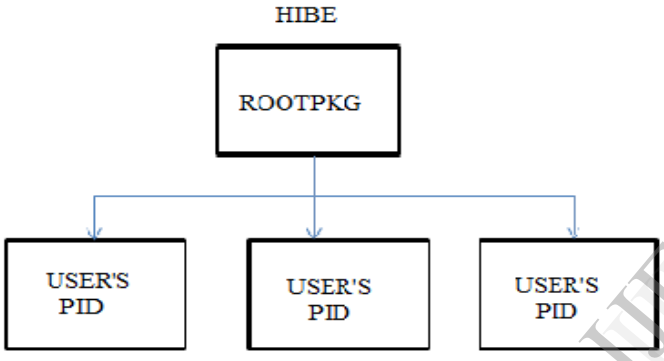

Figure 3: Hierarchical structure of HIBE

HIBE [4] is a scheme which allows hierarchy in defining security. Figure 3 shows a 2-level HIBE (2-HIBE) scheme with a root private key generation (PKG) domain PKGs and users where each one of them is associated with primitive IDs (PIDs) that are arbitrary strings. A user's public key consists of their PID and their domain's PID (in totality called an address). In 1-HIBE, there is only one PKG that distributes private keys to each user (whose public keys are their PID). Whereas in a 2-HIBE , users retrieve their private key from their domain PKG. Domain PKGs can compute the private key of any user in their domain, provided they have previously requested their domain secret key from the root PKG (who possesses a master secret).Levels of hierarchy can be extended further by adding sub-domains and so on.

HIBE includes a trusted third party (in the form of a root certificate authority) and allows a hierarchy of certificate authorities: the root certificate authority can issue certificates for other certificate authorities, who in turn can issue certificates for users in their respective domains. The original key structure which specifies the attributes associated with the users' decryption key. IBE system does not allow for such a structure. Moreover HIBE scheme greatly reduces the workload on master server(s).

F. *Hierarchical Attribute Based Encryption*

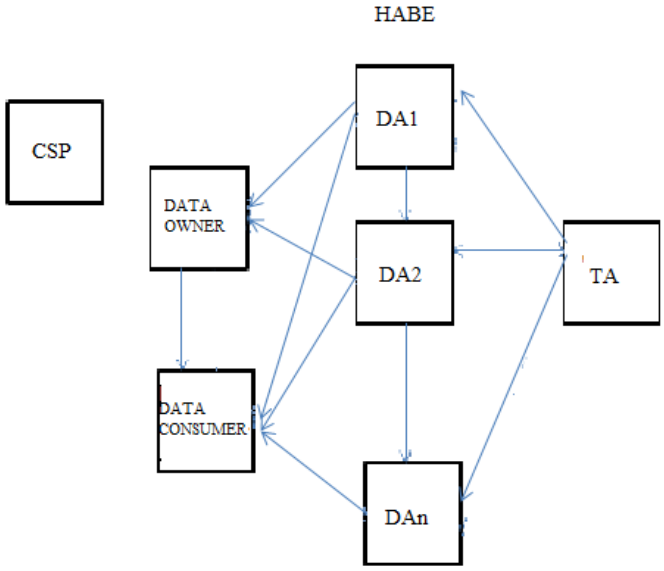

Figure 4: HABE structure.

HABE [5] is an encryption formed by combining HIBE [4] and CP-ABE [2] encryption schemes to achieve fine grained access control in cloud storage services. This uses fully delegating computation to the cloud providers. HABE assumes all the attributes in one conjunctive clause which are administrated by the same domain master. Therefore the same attribute may be administrated by multiple domain masters according to specific policies, which is difficult to implement in reality. When compared to ASBE [3] this scheme does not support compound attributes efficiently and does not support multiple value assignments.

The HABE system consists of five types of parties namely, a cloud service provider, data owners, data consumers, a number of domain authorities and a trusted authority as shown in figure 4. Cloud service provider manages a cloud to provide the data storage service. The data owners encrypt their data files and store them in the cloud for sharing with data consumers. Data consumers access the shared data files and download the encrypted data files of interest from the cloud and then decrypt them. Domain authority administers data owner or data consumer and is managed by its parent domain authority or the trusted authority. Domain authorities delegates keys to sub-domain authorities at next level or users in its domain. Trusted authority is the root authority and is responsible for managing top level domain authorities. Trusted authority is responsible for generating and distributing system parameters and root master key and authorizing the top level domain authorities. Each user in the system is assigned a

III. COMPARISON OF DIFFERENT ENCRYPTION SCHEME.

Techniques/Parameters	ABE	KP-ABE	CP-ABE	HABE	HIBE
Fine-Grained Access Control	Low	Low	Average	High	Low
Efficiency	Average	Average	Average	High	Low
Computational Overhead	High	High	Average	Low	High

Table 1: Comparison of different encryption schemes.

Table 1 summarises the fine-grained access control, efficiency and computational overhead of the various attribute encryption schemes that have been discussed in the paper.

IV. CONCLUSION AND FUTURE WORK

In this paper we discuss various encryption schemes starting from ABE, KP-ABE, CP-ABE, HIBE and HABE. Each successive encryption scheme is an improvement over its predecessor scheme of encryption. In this paper we focus on security, efficiency, scalability and fine-grained access control algorithms and their uses .

Our future work focuses on a scheme that will overcome the drawbacks of the present attribute encryption algorithm schemes in terms of flexible storage and fine grained access control.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai and B. Waters, “Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data”, ACM conference on Computer and Communications Security (ACM CCS), 2006.

[2] J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-policy attribute based encryption,” IEEE Symp. Security and Privacy, Oakland, CA, 2007.

[3] R. Bobba, H. Khurana, and M. Prabhakaran, “Attribute-sets: A practically motivated enhancement to attribute-based encryption,” in Proc.ESORICS, Saint Malo, France, 2009.

[4] Dan Boneh, Xavier Boyen, Eu-Jin Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext”, Advances in Cryptology—EUROCRYPT 2005, volume 3493.

[5] G.Wang, Q. Liu, and J.Wu, “Hierachical attibute-based encryption for fine-grained access control in cloud storage services,” ACM Conf. Computer and Communications Security (ACM CCS),Chicago,IL,2010.

[6] R. Ostrovsky and B. Waters. “Attribute based encryption with nonmonotonic access structures”.In Proceedings of the 14th ACM conference on Computer and communications security, pages 195{203. ACM New York, NY, USA,2007.

[7] M. Pirretti, P. Traynor, P. McDaniel and B. Waters, “Secure Atrribute-Based Systems”, ACM conference on Computer and Communications Security (ACM CCS), 2006.

[8] S. Yu, C.Wang, K.Ren and W. Lou. “ Achieving Secure, Scalable and Fine-grained Data Access Control in Cloud Computing “. In Proceedings Of IEEE INFOCOM 2010 , pages 534-542.

[9] Cheng-Chi Lee, Pei-shan chung,and Min-shiang Hwang, “A Survey on Attribute based Encryption scheme of access control in cloud Environment”, International journal of network security Vol-15, July 2013.

[10] A. Sahai and B.Waters.”Fuzzy Identity Based Encryption. In Advances In cryptology-Encrypt, volume 3494 of LNCS, pages 457-473. Springer 2005.

[11] C. Cocks. An identy based encryption scheme based on quadratic residues. In IMA Int. Conf..pages 360-363, 20001.

[12] D. Boneh and M.Franklin. Identity Based Encryption from the Weil Pairing. In Advances in Cryptology-CRYPTO, Volume 2139 of LNCS, Pages 213-9. Springer, 2011.

[13] C.Gentry and A. Silverberg.Heiraachical ID-Based Cryptography. In Proceedings of ASIACRYPT 2002,PAGES 548-566.

[14] T. Nishide, K. Yoneyama, and K. Ohta.” Attribute-based encryption with partially hidden encryptor-specified access structures”. In S. M. Bellovin, R. Gennaro, A. D. Keromytis, and M. Yung, editors, ACNS, volume 5037 of Lecture Notes in Computer Science, pages 111–129, 2008.

[15] M. Chase.” Multi-authority attribute based encryption”. In S. P. Vadhan, editor, TCC, volume 4392 of Lecture Notes in Computer Science, pages 515–534. Springer, 2007.

[16] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano. ”Public-Key Encryption with Keyword Search”. In Advances in Cryptology { Eurocrypt, volume 3027 of LNCS, pages 506{522. Springer, 2004.

[17] S. Muller, S. Katzenbeisser, and C. Eckert.” Distributed Attribute-Based Encryption”. In Proceedings of ICISC 2008, pages 20-36.

[18] Nuttapong Attrapadung, Benoit Libert, and Elie de Panafieu, “Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts”, 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011.

[19] C. Gentry and A. Silverberg. “Hierarchical ID-Based Cryptography”. In Proceedings of ASIACRYPT 2002, pages 548-566.