



An Efficient Presentation of Attribute Based Encryption Design in Cloud Data

Dr. Ananthi Sheshasaayee

Associate Professor & HOD,
PG & Research Dept of C.S & Application,
Quaid-E-Millath College (Govt.),
University of Madras
Chennai, Tamil Nadu, India

K. Geetha

Research Scholar (Part-Time)
Department of C.S & Application,
Quaid-E-Millath College (Govt.),
University of Madras
Chennai, Tamil Nadu, India

Abstract- *in this modern computer world, receptive data is stored and shared on the internet. Cloud computing is one of the up-coming technologies used for handling voluminous data and its storage. Working in this modern world, efficient techniques are needed to store the trusted cloud data in which Attribute based Encryption scheme play. Attribute is a way of public key encryption in which the secret key of the user and the cipher text are dependent. The decryption of a cipher text is only the set of attributes of the user key matching the attributes of the cipher text. There are so many encryption schemes that provide security and access control in cloud security. Attribute based encryption schemes have many advantages. This paper presents a survey based on attribute based encryption schemes that provide security and efficiency performance of the cloud data.*

Keywords – Access control, Security, Cloud computing, attribute-based encryption.

I. INTRODUCTION

Organizations need to store enormous amount of data. Network storage providers are giving the resources for organizations on demand. The Cloud computing has emerged to provide many application services to fulfill the user's demand [1]. The user also be aware about hacking and leakage of information in the cloud. In the cloud data storage application, the cloud can store the user's data and share the data's because the cloud can provide the "pay as you go" environment [4]. The data owner needs to make a flexible and scalable access control policy to command users' access right, so that only the authorized users can access the cloud data [5, 6]. One of the most important security concerns in clouds is the data security and privacy, always the first requirement of every cloud user is to provide security along with data confidentiality and flexible access control.

The decryption keys are disclosed only to the authorized users. This method has some drawbacks. Efficient key method to issue the decryption keys is desired for this established method. This method does not support scalability and flexibility, because when the number of authorized users increase it is not efficient. So, to overcome these issues many schemes are introduced. For improving the disadvantages, Sahai and Waters proposed an attribute-based encryption (ABE) scheme [7] in 2005. In 2006, Goyal proposed an key-policy attribute based encryption (KP-ABE) scheme [8] and 2007, R. Ostrovsky, A.Sahai, B.Waters proposed a non-monotonic access structure [9].

This paper focuses on the survey of different type of attribute based encryption techniques given in the following sections. Section II presents the literature survey of different type of encryption and a comparison table and section III concludes with discussions.

II. LITERATURE SURVEY

In cloud computing, the data owner wants to share the data from the cloud in the sense owner encrypt the data then uploaded into the cloud storage. All the sensitive cloud data's are encrypted to avoid the unauthorized user access of the cloud data. The different schemes exist that provide security, data confidentiality and access control. The encryption scheme provides security to the cloud data, and one of the schemes is attribute based encryption scheme. One of the encryption schemes is Attribute-Based Encryption (ABE) which is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Cipher text-Policy ABE (CP-ABE) scheme. In KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. Only the keys associated with the policy that is satisfied by the attributes associating the data can decrypt the data. In CP-ABE schemes, 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.

A. Attribute-based Encryption Scheme

Sahai and Waters proposed an attribute based encryption scheme in 2005. Attribute-based encryption (ABE) is a vision of public key encryption that allows users to Encrypt and decrypt messages based on user attributes. Standard

encryption is inefficient when selectively sharing data with many people, since the data needs to be encrypted using every User's public key. There are authority, sender and receiver in the ABE scheme, and authority's role is to generate keys for data sender and users to encrypt or decrypt data. In this scheme, the authority generates keys according to attributes; and these attributes of public key and master key, which are generated by the authority.

All the attributes used in the potential and any data user who wants to add to this system, and owns to attributes don't include pre- defined attributes. The authorities will re-define attributes and generate a public key and master key again. Data sender's to encrypt data with a public key and a set of descriptive attributes. A data receiver to decrypt encrypted data with private key sent from the authority.

Example: NASA wants to encrypt data.

Attributes : { Administrator, Manager, Engineer, Astronaut, Apollo, Space Shuttle, ISS, and Mars Rovers }

B. Key Policy Attribute Based Encryption

Key Policy Attribute Based Encryption scheme is a public key cryptography primitive that is for one-to-many communications. In this, data are associated with attributes for each of which a public key is defined. The one who encrypts the data, i.e., the encrypt associates the set of attributes to the data or message by encrypting it with a public key. Users are assigned with an access structure which is defined as an access tree over the data attributes. The nodes that are interior of the access tree [8].

Key-policy attribute-based encryption (KP-ABE) is an important class of ABE, where cipher texts 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. KP-ABE has important applications in data sharing on un trusted cloud storage. However, the cipher text size grows linearly with the number of attributes embedded in cipher text in most existing KP-ABE schemes [24].

In cloud computing, an access control mechanism based on KP-ABE together with a re-encryption technique is used for efficient user revocation. This scheme enables a data owner to reduce most of the computational overhead to cloud servers. The use of this encryption scheme KP-ABE provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access structure.

The first problem with this scheme is that the encrypted is not able to decide who can decrypt the encrypted data except choosing descriptive attributes for the data, and has no choice but to trust the key issuer. Furthermore, KP-ABE is not naturally suitable to certain applications.

C. Expressive Key Policy Attribute Based Encryption

This expressive key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic access structures (i.e., that may contain negated attributes) and with constant cipher-text size. Towards achieving this goal, show that a certain class of identity-based broadcast encryption schemes generically yields monotonic KP-ABE systems in the selective set model. A new efficient identity-based revocation mechanism, when combined with a particular instantiation of our general monotonic construction, gives rise to the first truly expressive KP-ABE realization with constant-size cipher texts. The downside of these new constructions is that private keys have quadratic size in the number of attributes. On the other hand, they reduce the number of pairing evaluations to a constant, which appears to be a unique feature among expressive KP-ABE schemes.

Among the encryption methods in clouds Attribute-based encryption (ABE), allows fine-grained access control on encrypted data. In the key-policy Attribute based encryption, the primitive enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure that specifies which all the ciphertexts the key holder is allowed to decrypt. In most ABE systems, the ciphertext size grows linearly with the

The key-policy attribute-based encryption schemes allowing for non-monotonic access structures and with constant ciphertext size. A new efficient identity-based revocation mechanism that, combined with a particular instantiation of general monotonic construction, gives rise to the first truly expressive KP-ABE with constant size cipher texts.[25]

D. Cipher Text Policy Attribute Based Encryption

Cipher text-policy attribute-based encryption can be viewed as a generalization of identity-based encryption. So as in identity-based encryption, there is a single public key, and there is a master private key that can be used to make more limited private keys. However, 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. In particular, 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[10,11].

In cipher text-policy attribute-based encryption (CP-ABE), depends how attributes and policy are associated with cipher texts and users' decryption keys. In a CP-ABE scheme, a cipher text is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes. In this scheme, the roles of cipher texts and decryption keys are switched as that in KP-ABE) the cipher text is encrypted with a tree access policy chosen by an encryptor, while the decryption key is created with respect to a set of attribute.

A highlight from this scheme is security to proven, including collusion resistance and generic group model. Implementation and performance made by Benchmarked on 64-bit AMD 3.7 GHZ workstation. Essentially on overhead beyond group operations in PBC library.

Table1

Operation	Approximate Time
Private key gen.	35 ms per attribute
Encryption	27 ms per leaf node
Decryption	0.5–0.8 ms per leaf node

However, basic CP-ABE schemes are far from enough to support access control in modern enterprise environments, which require considerable flexibility and efficiency in specifying policies and managing user attributes.

E. Cipher Text Policy Attribute Set Based Encryption

Cipher text Policy Attribute Set Based Encryption (CP-ASBE)- a new form of CP-ABE - which, unlike existing CP-ABE schemes that represent user attributes as a monolithic set in keys, organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy.

Specifically CP-ASBE allows, 1) user attributes to be organized into a recursive family of sets and 2) policies that can selectively restrict decrypting users to use attributes from within a single set or allow them to combine attributes from multiple sets. CP-ASBE can support compound attributes without sacrificing the flexibility to easily specify policies involving the underlying singleton attributes and multiple numerical assignments for a given attribute can be supported by placing each assignment in a separate set.

Table 2 Comparisons of different encryption schemes

Techniques/ Parameters	KP-ABE	EKP-ABE	CP-ABE
Access Control	Low	Better than	Average
	High if associated with re-encryption technique	KP-ABE	Realization of complex Access Control
Efficiency	Average	Higher than	Average
	High for broadcast type encryption	KP-ABE Only allows constant cipher text	Not efficient for modern enterprise environments

III. METHODOLOGY

From the above table2 comparing different encryption schemes analyzing with the different techniques and parameters. KP-ABE techniques encryption low and high associated with encryption with the access control parameters. Efficiency technique average and high for broadcast type encryption. EKP-ABE technique is better than KP-ABE in the access control, but higher than that only allows constant cipher text in the efficiency level. This paper applied the above algorithms at one level should be greater than the previous level, for this the studies the performance of different algorithms dependency on the performance of algorithm used at one level is used to decide the next level. In this way the algorithm applied at various level of hierarchical is changed to the maximum level of performance.

IV. CONCLUSION

In this paper, survey different attribute-based encryption schemes used in clouds. Many encryption schemes like KP-ABE, EKP-ABE, CP-ABE, ABE, ABE with NMAS, are discussed in which all the schemes are strong in efficient access control. Based on the discussion above, these schemes have properties: data's are encrypted with its attributes and need to care about number of users. Each attribute has public key, secret key and random polynomial. Authorized attribute can access to decrypt the cloud data. These papers conclude a survey based on attribute based encryption schemes that provide security and performance changed at the maximum level.

REFERENCES

- [1] M. Armbrust, A. Fox, R. Grith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica,

- and M. Zaharia, "A view of cloud computing," *Communications of the ACM*, vol. 53, pp. 50-58, 2010.
- [2] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *proceedings of the 14th ACM conference on computer and communications security*, pp.195-203, 2007.
- [3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.
- [4] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and Athena Vakali, "Cloud computing: Distributed internet computing for it and scientific research," *IEEE Internet Computing*, vol. 13, pp. 10-13, 2009.
- [5] C. C. Chang, I. C. Lin, and C. T. Liao, "An access control system with time-constraint using support vector machines," *International Journal of Network Security*, vol. 2, no. 2, pp. 150-159, 2006.
- [6] S.F.Tzeng, C.C.Lee, and T.C.Lin, "A novel key management scheme for dynamic access control in a hierarchy," *international journal of Network security*. Vol.12, no.3 pp.178-18-, 2011.
- [7] A.Sahai and B.Waters, "Fuzzy identity based encryption," *Advances in cryptology V EUROCRYPT*, vol.3494 of LNCS, pp.457-473, 2005.
- [8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89-98, 2006.
- [9] R.Ostrovsky, A.Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in *proceeding of the 14th ACM Conference on computer and communications security*, pp.195-203, 2007.
- [10] B.Waters, "Ciphertext-Policy attribute-based encryption" An expressive, efficient, and provably secure realization," *public key cryptography V PKC*, vol 6571 of LNCS, pp.53-70, 2011.
- [11] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute based encryption," *IEEE Symp. Security and Privacy*, Oakland, CA, 2007.
- [12] M. Pirretti, P. Traynor, P. McDaniel and B. Waters, "Secure Attribute-Based Systems", *ACM conference on Computer and Communications Security (ACM CCS)*, 2006.
- [13] A. Kapadia, P. Tsang and S. Smith, "Attribute-based publishing with hidden credentials and hidden policies", *NDSS*, 2007.
- [14] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009
- [15] Nuttapon 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, Marc
- [16] M.S.Hwang and L.C.Lin, "Introduction to Information and Network security (4ed, in Chinese), " in *Mc Graw Hill*, in Taiwan, 2011.
- [17] L.Ibraimi, M.Petkovic, S.Nikova, P.Hartel, and W.Jonker, "Mediated ciphertext-policy attribute based encryption and its application," *Information security Application*, vol.5932 of LNCS, pp.309-323, 2009.
- [18] S.Kamara and K.Lauter, "Cryptographic cloud storage," in *proceedings of the 14th international conference of Financial cryptograpy and data security*, pp.136-149,2010.
- [19] Ramasamy S, Vahidhunnisha :." Survey on Multi Authority Attribute Based Encryption for Personal Health Record in Cloud Computing, ISSN: 2278-621X, November 2013.
- [20] Q.Li, H.Xiong, F.Zhang and S.Zeng, "An expressive decentralizing KP-ABE scheme with content size cipher text," *International journal of Network security*, vol.15, no.3, pp.161-170, 2013.
- [21] A. Sahai and B. Waters, "Fuzzy identity based encryption," *Advances in Cryptology V EUROCRYPT*, vol. 3494 of LNCS, pp. 457-473, 2005.
- [22] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Proceedings of the Applied Cryptography and Network Security*, pp. 111-129, 2008.
- [23] Jin Sun, Yupu Hu, Leyou Zhang, "A Key-policy Attribute-Based Broadcast Encryption," *The International Arab Journal of Information Technology*, vol.10, No.5, September 2013.
- [24] Chang-Ji Wang, Sun Yat-sen, Jian-Fa Luo, "A Key-policy Attribute-based Encryption Scheme with Constant Size Ciphertext", **IEEE Computational Intelligence and Security**, pp 447-451, 2012.
- [25] Nuttapon Attrapadung, Benoit Libert, Elie de Panafieu, "Expressive Key-Policy Attribute-Based Encryption with constant-Size ciphertexts", *International Association for cryptologic Research*, pp.90-108, 2011.