American-Eurasian Journal of Scientific Research 12 (4): 213-217, 2017
ISSN 1818-6785
© IDOSI Publications, 2017
DOI: 10.5829/idosi.aejsr.2017.213.217

A Survey on Attribute Based Data Sharing Scheme Using in Cloud Computing

[1]M. Karthikraj and [2]S. Arun Kumar

[1]PG Student, Department of Computer Science and Engineering,
SRM University, Ramapuram, Chennai, Tamilnadu, India
[2]Assistant Professor, Department of Computer Science and Engineering,
SRM University, Ramapuram, Chennai, Tamilnadu, India

Abstract: Cloud computing, is a booming computing paradigm, allowing users to remotely hoard their data in a server and provide services on-demand. In cloud computing cloud users and cloud service providers are nearly certain to be from dissimilar trust domains. Privacy and Data security is the critical problems for remote data storage. Encryption has become a primary security for the data which is stored in a cloud or remote servers on the internet. Attribute based encryption scheme is a visionary encryption scheme. It uses public keys which are used to encrypt and decrypt the data based on the attribute sets. ABE considers attributes as traditional public key and associates the with the secret key of the user along with the cipher text. It comes with much functionality and helps to resolve many problems in the contemporary access control schemes This paper aims to survey the Attribute Based Encryption (ABE) scheme and its two types of variants. Key- policy Attribute Based Encryption (KP-ABE) and Cipher text-policy Attribute based encryption (CP-ABE), Attribute-based Encryption Scheme with Non-Monotonic Access Structures, HABE, MA-ABE.

Key words: Attribute Encryption · Key-policy · Cipher text · Schemes

INTRODUCTION

Being in the internet era, no wonder distributed technology of computing playing a key role. Data sharing also becomes an essential role to meet the needs of distributed technology. Any small piece of data is also accessible to many users from anywhere using cloud systems. Those end server systems must have complete confidence of data it stores. The server controls the user access hierarchy and restriction to end users and peers. If the server is hacked, data integrity will be lost and security is compromised. To enhance the security, encryption techniques are embedded to the server for data confidentiality and security. Private key pairs are used by the users to encrypt the data. But typical private keys are very hard to handle for complex encryption control policies. The access policies are described as attributes (Eg. City, Position) but it is best to have as actual identities of user.

Attribute based Encryption was first introduced by Sahai and Waters. It was introduced to create encryption concepts based on expressiveness. Attribute plays a key role in ABE system. This ABE is mainly used to create policies for user access. It is aimed to fulfil one-to-many encryption with requirements specified.

ABE is a public key pair encryption. The ciphertext and the secret key that the user holds depends on the attribute value (eg: the profession he attained, place he resides). This allows the user to secure the data by encrypting it or view the secured data by decryption.

Encryption takes place using the user attributed. The decryption can be done only if the key matches the attributes of user specified. Access policy is classified into key-policy and ciphertext policy based on the user policies. The first Key-Policy Attribute Based Encryption (KP-ABE) was proposed by Goyal [2] which allows a specific access structure. The first Cipher-Policy Attribute Based Encryption was proposed by Bethencourt and many such schemes were proposed later. There are numerous schemes proposed recently using multiple authorities generating private user keys. The main security advantage of Attribute Based Encryption is collusion resistance.

Corresponding Author: M. Karthikraj, PG Student, Department of Computer Science and Engineering,
SRM University, Ramapuram, Chennai, Tamilnadu, India.

The access to data will be provided to authority only if a minimum of single key grants access. Moreover, Muller offered an distributed attribute-based encryption scheme in 2008; Yu e. proposed a finegrained data access control encryption scheme ; Tang proposed a Verifiable attribute based encryption scheme.

Enhanced ABE scheme proposed by Ostrovsky *et al*. an which supports non-monotone access structures [7]. In 2008 Muller *et al*. proposed an distributed attribute-based encryption scheme [8]. Wang *et al*. proposed a hierarchical attribute-based encryption scheme (HABE) [10] in 2010. which integrates properties in both a HIBE (hierarchal identity based encryption) model and a CP-ABE model. There after introduce MA-ABE (multi- authorities ABE) schemes that use multiple parties to distribute attributes for users. ABE schemes can be further considered as either monotonic or non-monotonic built on their type of access structure.

Literature Review: The literature survey consists of the study of Attribute Based Encryption, KP-ABE and CP-ABE.

Attribute Based Encryption (ABE): Sahai and waters first came up with the idea of Attribute Based Encryption. The main idea of attribute based encryption is public key cryptosystem in which the attributes consists of the cipher text and the secret key that is owned by the user. There are some user attributes that are connected with ciphertext, the ciphertext can be decrypted only if the attributes owned by the user key equals the cipher text attributes. Attribute Based Encryption can be classified into two groups Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE) based on the access policy enclosed into the secret key owned by the user or ciphertext.

Data Sharing Architecture: Data Owner , cloud server, key distribution centre and end user are the four major elements of Data Sharing Architecture.

Data Owner: Data owner uses cloud server to store their data, the data will always be encrypted for security reasons before storing. The data owner can work on encrypted data file and also they can set the access privilege to that.

Cloud Server: In this , a cloud is managed by a cloud service provider which is used to store data. Data files will be encrypted and stored in cloud by the data owners to share the data with data consumers. The data consumers first need to choose the data files which they need and export the encrypted data file from the cloud and then the shared data file should be decrypted. For security reasons all the end users should be authorised.

Key Distribution Centre: KDC plays many roles such as capturing the hackers, save verification parameters, offer public enquiry services for attributes such as creating secret key for a data file and share to the correct end user.

Data Consumer/End User: Each data file have different access privilege, the privileges are decided by the data owner and they also controls the data users. The end user can access the data file only if they have the access to the file and encrypted key. Normal users try to access the data files within their access privileges and hackers may try to get confidential files for which they don't have access. KDC generates and shares the secret key with the authorized users if it gets request from the user to do so.

Attacker (Unauthorized User): Cloud server is used to store the data file, in this cloud server the attacker may add the malicious data to any block , so the unauthorized users are usually considered as attackers.

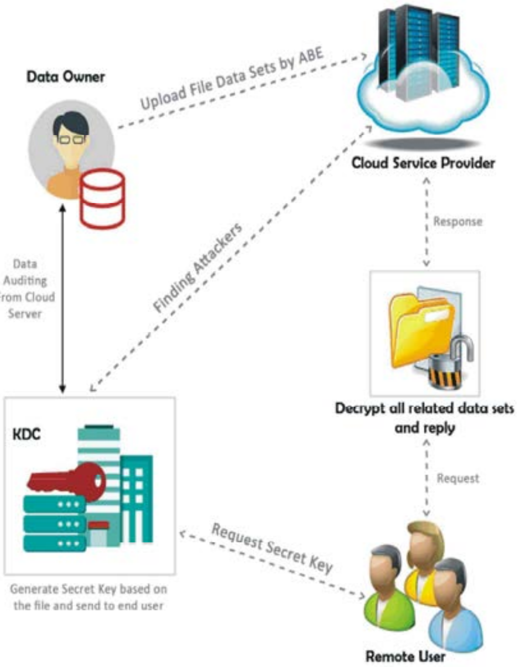
Data Owner
Upload File Data Sets by ABE
Cloud Service Provider
Response
Data Auditing From Cloud Server
Finding Attackers
Decrypt all related data sets and reply
KDC
Request
Request Secret Key
Generate Secret Key based on the file and send to end user
Remote User

Fig. 1: Architecture of Data Sharing

ABE Algorithm Model: In basic ABE, both the secret key of user and cipher text used will be labelled with attributes. A key can decrypt the cipher text to get access to the data only if it has a certain combination of attributes present on both cipher text and the secret key of user. So the decryption takes places in a KP-ABE or CP-ABE schemes only if the attribute set used in the secret key and cipher text abides the access structure.ABE basically has four algorithms. They are Setup, Encryption, Decryption and Key generation which consists of sender to send, authority to validate the data and receivers with participants.

Setup: (K, U)->(PP,MSK): This algorithm uses the parameter K as input and returns Public Key and master Secret Key as output. The senders use PP to encrypt the data. The authority alone knows the MSK which is used to create secret keys.

Key Generation: (K,PP,MSK,S)->SK: Key generation algorithm uses the inputs as public parameter PP, master secret key MSK, attribute set S and it generates a key to decrypt SK, this key helps the user to decrypt the data using an access tree structure T only if T matches.

Encryption: (K, PP, M, T)->CT : In the Encryption algorithm, the sender would encrypt a message M, using a public parameter PP, an access structure T and an attribute set S. The output of this algorithm is a ciphertext CT

Decryption: (K, PP, SK,CT)->M: In this algorithm, public parameter PP and ciphertext CT are taken as input with a secret key SK for an attribute set SK. The output of this algorithm is a message only if the associated ciphertext matches the access structure.

Key-Policy Attribute Based Encryption (KP-ABE): KP-ABE is a new refined type of ABE scheme. Goyal el al. in 2006 introduced the First key-policy scheme. Through KP-ABE encrypted data can be shared with great attention to detail and this also allows one to many relationships. In this attribute each cipher text has an attribute set and user’s secret key which is generated by authority. An access structure also policy is used to associate the secret key to decrypt the data. The access structure provides details of the list of cipher texts the user can decrypt. In other words, the decryption can be done only if the cipher text attributes matches the access structure associated with the private key. This KP-ABE scheme will be best suited for professional and structural organisations and institutions which creates rules to create access and restrictions for a particular document. This scheme prevents unauthorised user to decrypt the data even if data resides in an insecure server.

Ciphertext-Policy Attribute Based Encryption (CP-ABE): CP-ABE scheme is the other type of ABE scheme. We use remote servers to store our files for various reasons. The files may be intended to be scalable to other users using resources from elsewhere. Reliability can be achieved in case of network failures where the data can be re-created again as it is in a remote server. This scheme has its primary focus on security which has a tension with other properties. As our files get replicated there are more chances for hackers and attackers to get control of the system. This tension makes the CP- ABE scheme very useful. When there is a requirement for which user can access what files should be done securely using CP-ABE.

CP-ABE can also be categorised as an extension of identity-based-encryption. In identity based encryption, it has a master private key which used to generate many more private keys and one public key. But CP-ABE is not just an identity based encryption as it is extended with more flexibility. This allows complex rules to specify explicitly to pair a private key to a cipher text for decryption. All private keys are associated with attribute sets and the encryption has an access structure or policy which will help to decrypt the data by identifying which key will be required to decrypt.

CP-ABE has a set of attributes and a private key. The attributes are associated to users and the keys are generated based on attribute set. During encryption of a message M, an access structure is defined by an encryptor. This access structure is defined in attribute sets for Message. The rules are specified for encrypting the data, which is only those specified attributes which abides by the access structure, can be granted access to decrypt the message. Unauthorised users even if they collude they cannot decrypt the cipher text because the access policy allows the encryption to choose the key which has the associated attribute set. This concept is built upon basic access control schemes.

Attribute-Based Encryption Scheme With Non-Monotonic Access Structures: Earlier ABE schemes were restricted to expressing only monotonic access structures and there is no acceptable method to represent negative

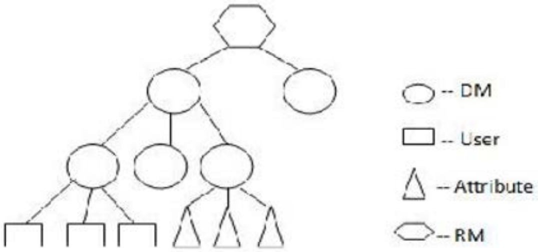

Fig. 2: HABE model

limitations in a key's access formula. Ostrovsky *et al*. proposed an ABE with non-monotonic access structure in 2007. Non- monotonic access structure can be use the adverse word to describe every attributes in the message, but the monotonic access structure cannot.

Hierarchical Attribute-based Encryption: The scheme Hierarchical attribute-based encryption (HABE) is derived over Wang *et al* The HABE model (Fig 2) holds of a root master (RM) that corresponds to the third trusted party (TTP) and many domain masters (DMs) in which the top-level DMs relate to many enterprise users and several users that correspond to totally personnel in an enterprise. The HABE scheme used the property of the hierarchical generation of keys in Hierarchical attribute-based encryption (HIBE) scheme to generate keys.

ABE Security Analysis: ABE scheme has great security features and functionalities which are specified below.

Data Confidentiality: Access to the raw data is prevented from unauthorised users. The information is encrypted from unauthorized users, as they do not have required attribute set to match the criteria of access structure policy. Hence, the unauthorised access from KGC and data-storing centers to the plain text data are prevented from the attackers.

Collusion Resistance: Collusion resistance is an important functionality in ABE scheme. If the users become dishonest and try to decrypt the data, it is not possible because the users can only have a part of attribute set and it cannot match the attribute set criteria. Even if multiple users combine their attribute set, it will not match the criteria of the access structure policy.

User/attribute Revocation: When an user leaves the system the policy revokes the access of the user to the system.

Scalability: The scheme doesn't not have adverse effects when more users enter the policy. It has the functionality to maintain the same performance throughout system for all users. Even if the users authorised are increased dynamically the system will provide good performance.

Comparitive Analysis: This comparison shows that CP-ABE scheme is much more efficient than KP-ABE scheme. This scheme is more adapted for sharing the data in a cloud on remote servers. The data owners have the complete control of the data access policy. This scheme resolves the disadvantages of using KP-ABE schemes where the encrypted data cannot decide who can decrypt the data. Access control is also supported by this scheme in real-time. It also contains the private key of user and set of attributes associated. By using this attributes only the user can be able to satisfy the access control to decrypt the data. This CP-ABE scheme also has some disadvantages. One of the drawbacks of this scheme is not completely fulfilling the requirements of access control with flexibility and efficiency. The access control has to be improved. Also only user attributes which are organised logically into a single set are supported by the decryption keys. So users cannot use attributes from different set and can only use possible combinations from a single set. Comparatively MA-ABE has a better access control and it is more scalable and has a higher collusion resistance. ABE has a good access control, however has computational overhead. In ABE, there is a low access control and it has a average efficiency and resistance towards collusion.

Technique /Parameter	ABE	KP-ABE	CP-ABE	HABE	MA-ABE
Efficiency	Average	Average, High for Broadcast type system	Average, Not efficient for modern enterprise	Flexible	Scalable
Computational Overhead	High	Most of computational overheads	Average computational overhead	Some of overhead	Average
Fine grained Access Control	Low	Low, High if there is reencryption	Average Realization of complex access control	Good Access Control	Better Access Control
Collusion resistant	Average	Good	Good	Good	High collusion resistant

Proposed System: An attribute-based data sharing scheme is being proposed for cloud computing applications, which is represented as as cipher text-policy weighted ABE scheme with removing escrow (CP-WABE-RE). It resolves two types of issues: key escrow and arbitrary- sate attribute expression.

- An improved key issuing protocol is used to resolve the key escrow problem of CP-ABE in cloud computing. The protocol can prevent KA and CSP from knowing each other's master secret key so that none of them can create the whole secret keys of users individually. Data confidentiality and privacy can be ensured.
- Weighted attribute is used to improve the expression of attribute. The weighted attribute can reduce the complexity of access policy. Thus the storage cost of cipher text and computation complexity in encryption can be reduced. It can express larger attribute space than ever under the same condition.

CONCLUSION

To conclude this paper, different attribute-based encryption schemes such as ABE and its sub categories KP-ABE and CP-ABE are analyzed and other non-monotonic schemes such as HABE and MA-ABE.The main access polices are KP-ABE and CP-ABE. Based on their type of access structure the schemes are categorized as either monotonic or non-monotonic. An attribute-based data sharing scheme is being proposed for cloud computing applications, which is represented as as cipher text-policy weighted ABE scheme with removing escrow (CP-WABE-RE). It resolves two types of issues: key escrow and arbitrary-sate attribute expression. Our scheme also enables dynamic modification of access policies of supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

REFERENCES

1. Sahai and B. Waters, 2005. Fuzzy identity-based encryption, inProc. EUROCRYPT, pp: 457473.
2. Goyal, V., O. Pandey, A. Sahai and B. Waters, 2006. Attribute based encryption for fine-grained access control of encrypted data in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), pp: 89-98, November 2006.
3. Bethencourt, A. Sahai and B. Waters, 2007. Ciphertext-policy attribute-based encryption,? in Proceedings of the IEEE Symposium on Security and Privacy (SP '07), pp: 321-334,May 2007.
4. Ostrovsky, R., A. Sahai and B. Waters, 2007. Attribute-based encryption with non-monotonic access structures, in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp: 195-203, November 2007.
5. Attrapadung, N., B. Libert and E. de Panafieu, 2011. Expressive keypolicy attribute-based encryption with constant-size ciphertexts,? in Public Key Cryptography, PKC 2011, 6571: 90- 108, Springer, 2011.
6. Goyal, V., A. Jain, O. Pandey and A. Sahai, 2008. Bounded ciphertext policy attribute based encryption, in Automata, Languages and Programming: Part II, vol. 5126 of Lecture Notes in Computer Science, pp: 579-591, Springer, Berlin, Germany, 2008.
7. Cheung and C. Newport, 2008. Provably secure ciphertext policy ABE, in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp: 456-465, November 2007. [8]. Muller, S. Katzenbeisser and C.Eckert, "Distributed attribute-based encryption," in Proceedings of ICISC, pp: 20{36, 2008}.
9. Ostrovsky, R. and B. Waters, 2007. Attribute based encryption with non- monotonic access structures. In Proceedings of the 14th ACM conference on Computer and communications security, pages 195{203. ACM New York, NY, USA, 2007.
10. Wang, Q. Liu and J. Wu, XXXX. Hierachical attribute- based encryption for fine-grained access control in cloud storage services, in Proceedings of the 17th ACM conference on Computer and communications security.