International Journal of Engineering & Technology, 7 (2.15) (2018) 64-67

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Current Issues in Ciphertext Policy-Attribute Based Scheme for Cloud Computing: A Survey

Norhidayah Muhammad[1]*, Jasni Mohamad Zain[2], Mumtazimah Mohamad[3]

[1,2] Faculty of Computer & Mathematical Sciences, Universiti Teknologi Mara, 40450, Shah Alam, Selangor, Malaysia.
[3]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Kampus Besut, 22200, Besut, Terengganu.
**Corresponding author E-mail: mrs.hidayah@yahoo.com.my*

Abstract

The use of cloud computing has increased exponentially in data resources storage over the past few years. Cloud storage reduces the overall costs of server maintenance, whereby companies only pay for the resources they actually use in the cloud storage. Despite this, security concerns in cloud computing must be a top priority. One of the common encryption methods in cloud security is Attribute Based Encryption (ABE). ABE contains two types, namely, Ciphertext Policy-Attribute Based Encryption (CP-ABE) and Key Policy- Attribute based Encryption (KP-ABE). CP-ABE is better than KP-ABE, especially in reduplication issues and fine-grained access. However, issues in CP_ABE need further improvement. Improvement for the CP-ABE scheme has been growing rapidly since 2010 to date, and five main issues need improvement. This paper reviews the proposed CP-ABE schemes during the past three years. These schemes focus on solving the five issues identified inherent in the CP-ABE scheme.

Keywords: *ABE Scheme, CP-ABE Scheme, CP-ABE Problems, Cloud Computing security.*

1. Introduction

The introduction of cloud computing is a revolutionary innovation in data resources management. Generally, cloud computing seems as if an unlimited computer's hard drive allowed a user to store and access the data over the internet. In addition, cloud data sharing is among the desired services offered by cloud service providers, which allows data owners to outsource their data to cloud data storage servers for the purpose of sharing. Users need to pay only for the storage they actually use, and this reduce the cost of server maintenance. The cloud service is very convenient to many new companies. However, it raises security concerns relating to the shared data, since the cloud storage servers and data owners are not in the same domain. Furthermore, the data owners do not fully trust the cloud storage servers. Therefore, it makes access control over the shared data a challenging issue that addresses how data owners ensure that their data stored in cloud storage servers are accessed by legitimate users[1, 2].

People put a lot of emphasis on protecting one-to-one communication such as RSA, AES, Elliptic Curve scheme. However, the security of group communication is often overlooked. One-to-one encryption cannot satisfy the demands of practical applications [3]. This is because each user should have their own private and public key for the encryption and decryption processes. Handling many keys with many users will incur bloated cloud storage, as well as redundancy and reduplication problems. For example, an institute has 1,000 staff members and the administrator wants to grant 300 of them the privilege to access an electronic document. The document must be encrypted 300 times using different public keys, and each ciphertext is deferent from others. The administrator needs to carefully send each ciphertext to the right recipient. If many documents should be distributed, handling so many ciphertexts will cause bottleneck issues [4]. In One to Many encryption, once the data owner encrypts the file, he can determine who has the right to decrypt the data by specifying the attribute user in the access policy.

The Attribute Based Encryption (ABE) scheme was proposed by Sahai and Water [5] and has obvious advantages in terms of efficiency. It is also fit for the large-scale network environments such as cloud systems. CP-ABE is a type of ABE and has become better than Key Policy-Attribute Based Encryption (KP-ABE) based on a specification of CP-ABE provide fine-grain access control. Although CP-ABE scheme was better than KP-ABE scheme, it still has issues that need to be improved. These issues are discussed in this paper, as well as the solutions proposed by previous schemes. In this paper, we address the following research questions:

a) RQ1: What are the current problems or topics that researchers focus on regarding the CP-ABE scheme?

b) RQ2: Who is involved in this current research, and what are they trying to propose and develop to solve this problem?

The remainder of the paper is structured as follows. Section 1 presents a background study of the research area, and section 2 briefly discuss related work on this topic. Section 3 discusses five problems in CP-ABE and the proposed solutions for each of the identified CP-ABE problems. Lastly, Section 4 provides a conclusion. The five issues are identified based on research schemes in the past three years from (2015-2017), and have been published in IEEE, Science Direct, ACM, and Google Scholar database.

2. Related Work

2.1. ABE Scheme

An easy way to comply The Attribute-based encryption (ABE) implements secure access control that enforces ciphertext, and can only can decrypted by the user with the correct attribute in access policies assigned by the data owner. There are two types of ABE: the first is Key Policy-Attribute-based Encryption (KP-ABE), where the attribute is assigned to ciphertext and the access policy is assigned to the ciphertext. The next is Ciphertext Policy-Attribute-based Encryption (CP-ABE), which is different from KP-ABE, where the attribute is in the private key and the access policy is in the ciphertext.

2.2. CP-ABE Scheme

Ciphertext Policy-Attribute-Based Encryption (CP-ABE) is a great achievement compared to KP-ABE, since it resolves the issue of fine-grained access control over the shared data in one-to-many communications in cloud servers. Data owners hold direct control on access policy, and the access policy is enforced cryptographically in the ciphertext. Nowadays, CP- ABE is used in a cloud computing environment because it provides protection to the cloud server and ensures the server can be fully trusted. In CP-ABE algorithm, attributes are combined with the user's secret key, where the access policy is combined with the ciphertext. If attributes in the secret key of a user satisfy the access policy in the ciphertext, then the ciphertext can be decrypted. The CP-ABE has four phases, namely, setup, key generation, encryption, and decryption.

- (PublicKey, MasterKey)
- (PublicKey, SecretKey, Attributes): Setup PrivateKey.
- Encryption(PublicKey, PlainText, AccessPolicy):Generate Ciphertext.
- Decryption(PublicKey, Ciphertext, PrivateKey): Decrypt Ciphertext.

3. Classification Of CP-ABE Scheme Issues

According to previous researchers, there are several issues in CP-ABE that were discussed and improved. Based on previous research schemes from 2015-2017, a total of 20 publications concerning CP-ABE development issues have been identified. We focus on five issues, namely, attribute revocation, constant ciphertext, fine-grained access control, hidden access policy, and multi-authority. Improvements made to the CP-ABE algorithm by previous researchers according to these problems, which are compared in Table 1.

3.1. Attribute Revocation

Attribute revocation is an important process in the CP-ABE algorithm. In this algorithm, the attributes of an entity often change with time, e.g., job position, salary, and so on. Once a user's attribute changes, the user will obtain a new secret key with a new attribute. Otherwise, the old secret key still matches with an access policy, and decryption process is carried out. One of the major hurdles for the practical application of CP-ABE is how to invalidate the secret key which belongs to a user who no longer has access privileges in the system. User revocation is followed by two security properties: forward secrecy and collusion-resistance. The forward secrecy security property guarantees that any revoked user who no longer has access privilege in the system should be prevented from decrypting any ciphertext. Re-encrypting the data is very impractical and unusable because if in a large company, there are a lot of data to be re-encrypted and it becomes more complicated if the encryptors are unavailable during the attribute and access policy update. That is the reason attribute revocation has become an interesting topic to be discussed and improved upon. Many researchers attempt to cater this problem. Jiang[6] has presented the Ciphertext-policy Attribute Based Encryption has supporting Access Policy Update (CP-ABE-APU) to support the revocation and any updating of access policies. Otherwise, Vaanchig[7] uses a dynamic binary tree instead of a static binary tree for the purpose of improving the scalability of the system. Yuan[8] has proposed PU-CP-ABE function that uses the dynamic policy update scheme, with a combination of the new matrix update algorithm and the CP-ABE schemeSdsdsds

3.2. Constant Ciphertext

In the fundamental of CP-ABE, each entity can have attributes, and each attribute is a descriptive string. Many entities may share similar attributes, which allows encryptors to specify a secure data access policy over the shared attributes to reach a group of receivers. For example, in a group of computer science, there is more than one entity that has an attribute of computer science. Ciphertext policy- Attribute based encryption schemes face the bulky ciphertext problem. In most of the existing CP-ABE schemes, the size of the ciphertext increases linearly with an increase in a number of attributes in access policy. This is because the access policy ciphertext is associated in CP-ABE, which is a boolean access policy, and the size of ciphertext is larger. Very large ciphertext size leads to computational overheads and security infringements[9]. Previous privacy-preserving algorithms protect the access policies, but require large linearly and increasing ciphertext size. It is hard to find work that can achieve privacy-preservation and constant ciphertext size at the same time [10].

The most common technique so far is to construct the access control that offers a constant size of ciphertext based on LSSS matrix (linear secret sharing scheme). However, the problem with LSSS is that the size of the access Boolean is larger than the number of clauses. Zhou[10] has proposed an algorithm named Privacy Preserving Constant-size Ciphertext Policy Attribute Based Encryption (PP-CP-ABE), which enforces access policies with wildcards and incurs constant-size of cipertext, regardless of the number of attributes. Li [11] presented a new CP-ABE that can produce constant size of ciphertex and also a constant size private key. This scheme is based on the orderedbinary decision diagram (OBDD). Malluhi [12] has proposed a CP-ABE scheme supporting fine-grained access control, and also a small ciphertext size. The ciphertext size is linear in either the size of the access boolean formula or the number of clauses, depending on which is smaller between them. Tamizharasi [13] has proposed a constant size of ciphertext and a secure CP-ABE scheme with any number of user attributes, because the size of ciphertext does not depend on the number of attributes. This scheme eliminates redundant attributes by constructing a dispensability matrix.

3.3. Fine-Grained Access Control

One of the advantages of CP-ABE is that it provides a fine-grained access control to protect data from an unauthorized party. However, in CP-ABE, data owners have the right to justify users that are qualified to decrypt the data to make sure of fine-grained access. Data owners can encrypt the data and state the attribute of the user in access policy without knowing the right person who will decrypt the data. Data owners only know the group which is allowed to decrypt the data, and state the user attribute in the access policy. Because of this, it may reduce the level of fine-grained access control of the system if user attributes or private key is leaked towards anonymous users. Several schemes have improved fine-grained CP-ABE. Xu[14] has modified the CP-ABE scheme by implementing verifiable delegation and presenting a concrete construction to ensure fine-grained access control, and at the same time, the correctness of the delegated computing results are well guaranteed.

This scheme realizes circuit's ciphertext-policy based hybrid encryption with verifiable delegation (VD- CPABE). Li[15] has proposed a new CP-ABE scheme for practical use, because existing CP-ABE is analyzed thoroughly to identify its performance bottlenecks. This CP-ABE scheme implements multithreading techniques to parallelize the key generation, encryption, and decryption processes. It also switches modes of encryption from Cipher Block Chaining (CBC) mode to Counter (CTR). Tamizharasi[16] has proposed a new CP-ABE scheme to improve the level of fine-grained access control properties. This scheme implements attribute access concepts and also user access concepts to solve the problem of fine-grained access control. Shoukun[17] constructed a new CP-ABE scheme extending the CP-ABE algorithm with a flexible mechanism of delegate; this scheme achieves both forward security and backward security.

3.4. Hidden Access Policy

In CP-ABE scheme, ciphertext is combined with access policy. The access policy contains the boolean and access formulas of the user. An access tree is implemented in the access policy and is generated by the set of Boolean formulas representing an attribute. Boolean formulas have a set of AND, and OR gates. There are several types of the Access trees such as AND Gate and threshold gate. For threshold gate, each non-leaf nodes of access tree is defined by the threshold values. The owner transmits the access policy along with the ciphertext, and everyone can have a lesson in the access policy. Sometimes hackers attempt to break the ciphertext by learning the access formula in the access policy. After they learn about the access formula and attribute in the access policy, it is easier to create a fake key and obtain access to data. Therefore it is crucial to conceal the access formula in the access policy, especially in a cloud server. Previous CP-ABE schemes only associate access policy with ciphertext, without hiding the access policy. Then hackers can get the access, and can also directly learn some sensitive information of access policy and make the data unsecure. Existing schemes based on the AND-gate with wildcard access structure cannot hide the access policy[18]. Many researchers have come up with new schemes to overcome the limitations of the previous schemes in hiding access policies. Vaduganathan [19] has proposed ABE algorithm that features conceal attributes and access policies. Attributes and Access policies are hidden by the hash function and polynomial functions.

Yadav[20] has proposed one scheme in which users do not keep the access policies with encrypted information (ciphertext). They apply composite order bilinear on that scheme. Phuong[18] has proposed a new scheme focused on hidden access policy by expanding the technique based on AND-gate with wildcards. Yadav[21] has proposed a secure CP-ABE scheme using composite-order bilinear groups which hides access policy. Jin[22] has presented an efficient CP-ABE development with hidden policy and is fully secure under static assumptions applying the dual system encryption methodology. This scheme allows AND gate with both positive, negative and wildcard access policy, with a short size of ciphertext. Li[23] has presented a searchable CP-ABE with attribute revocation, where access policy is not totally hidden so that receivers cannot extract sensitive information from the ciphertext. The safety of this scheme can be decreased to the decisional bilinear Diffie–Hellman (DBDH) assumption and decisional linear (DL) assumption.

3.5. Multi-Authority

Key authority in CP- ABE has two categories: single-authority and multi-authority. In the cloud system, multi-authority is very recommendable because it is more practicable and does not depend on a single authority. However, there are two issues in multi-authority and cannot directly be implemented. First, in system organization, system users would dynamically join or leave throughout the year. This requires that these users' authorization should also be changed correspondingly. Second, in practical applications, adding and revoking attributes is usually changed. In multi-authority, the public parameter of these schemes relies on the attribute universe, which indicates that when the system finishes initialization. The attribute universe is totally fixed. The multi-authority concept in CP-ABE is to make this scheme increase efficiency and practicality. In the single CP-ABE algorithm, there is only one authority. Thus, there might be a risk of failure. The concept of multi-authority was first introduced by Chase in 2007. Chase allows any number of authorities to monitor the attributes of the users and distribute secret keys. It can also tolerate an arbitrary number of corrupt authorities. When a number of users increases, the efficiency of decrypting the ciphertext decreases.

To overcome this problem, several schemes were developed. Huang[24] has proposed threshold-based key generation approach (TKGA) which can improve security by impeding collusion attacks. In contrast, Rouselakis[25] allows multiple authorities to control the key issuing for an exponential number of attributes, and these attributes do not need to be specified during setup. They use prime order bilinear groups. Rouselakis[26] is targeted to achieve multi authorities attributes based encryption with fast decryption by using the concept of fast decryption. Multiplicity is also achieved which solves the problem. They use AND, OR and Threshold policies. Wei[27] has constructed a multi-authority CP-ABE scheme that not only depends on one fully trusted authority, but all attribute owners have authorities to issue the private key for the user. Therefore, multi-authority helps authorities remove any user from the system. Users cannot decrypt the ciphertext after being revoked by the authority’s central, because the cloud server can update the ciphertext from the current time period to the next one. Rahman[28] has proposed a Decentralized multi-authority Ciphertext-Policy Attribute-Based Encryption (DCP-ABE) scheme, where any party can become an authority by creating a public key and generating private keys for the users by utilizing their attributes.

4. Conclusion

This work discussed the recent issues in CP-ABE during the past three years. As discussed in Section 3, this work answered two research questions (as mentioned in Section 1). We classified the recent issues in CP-ABE into five main categories. Table 1 shows the analysis of the previous scheme that was proposed by the researcher to improve CP-ABE scheme to be more efficient and practical for cloud storage. Current and future research works in CP-ABE were also discussed in this paper.

Acknowledgement

This work supported by Fundamental Research Grant Scheme (FRGS/1/2015/ICT02/UNISZA/02/1) by Malaysia Ministry of Higher Education (and the Center of Research and Innovation Management of Universiti Sultan Zainal Abidin, Terengganu, Malaysia.

Table 1: Proposed scheme for each problem in CP-ABE algorithm

		Recent Issues/Problems				
Author	Proposed Scheme	Attribute Revocation	Constant Ciphertext	Fine Grain Access Control	Hidden Access Policy	Multi-Authority
[8]	PU-CP-ABE	/				
[7]	Update CP-ABE	/		/		
[29]	CP-ABE-APU	/	/			
[23]	Update CP-ABE	/			/	
[10]	PP-CP-ABE		/		/	
[11]	Update CP-ABE		/			
[12]	Update CP-ABE		/	/		
[14]	VD- CPABE			/		
[15]	P-CP-ABE			/		
[13]	Update CP-ABE			/		
[17]	Update CP-ABE			/		
[19]	Update CP-ABE				/	
[20]	Update CP-ABE				/	
[22]	Update CP-ABE		/		/	
[24]	TKGA					/
[25]	Update CP-ABE					/
[26]	Update CP-ABE					/
[27]	Update CP-ABE	/		/		/
[30]	DCP-ABE					/

References

[1] Liew, S.-C., S.-W. Liew, and J.M. Zain, Tamper localization and lossless recovery watermarking scheme with ROI segmentation and multilevel authentication. *Journal of digital imaging*, (2013). **26**(2): p. 316-325.

[2] Zain, J.M., Strict authentication watermarking with JPEG compression (SAW-JPEG) for medical images. *arXiv preprint arXiv:1101.5188*, (2011.

[3] Chen, N. and M. Gerla. Dynamic attributes design in attribute based encryption. in *Annual Conference of ITA (ACITA)*. University of Maryland:(2009).

[4] Doshi, N. and D. Jinwala, Updating attribute in CP-ABE: A New Approach. *IACR Cryptology ePrint Archive*, (2012: p. 496.

[5] Sahai, A. and B. Waters. Fuzzy identity-based encryption. in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*.(2005) Springer.

[6] Jiang, Y., et al. Ciphertext-policy attribute based encryption supporting access policy update. in *International Conference on Provable Security*.(2016) Springer.

[7] Vaanchig, N., W. Chen, and Z. Qin. Ciphertext-Policy Attribute-Based Access Control with Effective User Revocation for Cloud Data Sharing System. in *International Conference on Advanced Cloud and Big Data (CBD)*.(2016) IEEE.

[8] Yuan, W., Dynamic Policy Update for Ciphertext-Policy Attribute-Based Encryption. *IACR Cryptology ePrint Archive*, (2016: p. 457.

[9] Odelu, V., et al., Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. *Computer Standards & Interfaces*, (2016.

[10] Zhou, Z., D. Huang, and Z. Wang, Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption. *IEEE Transactions on Computers*, (2015). **64**(1): p. 126-138.

[11] Li, L., et al., A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram. *IEEE Access*, (2017). **5**: p. 1137-1145.

[12] Malluhi, Q.M., A. Shikfa, and V.C. Trinh. A Ciphertext-Policy Attribute-based Encryption Scheme With Optimized Ciphertext Size And Fast Decryption. in *Asia Conference on Computer and Communications Security*.(2017) ACM.

[13] Tamizharasi, G., B. Balamurugan, and R. Manjula. Attribute Based Encryption with Fine-grained Access Provision in Cloud Computing. in *Proceedings of the International Conference on Informatics and Analytics*.(2016) ACM.

[14] Xu, J., et al., Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, (2016). **27**(1): p. 119-129.

[15] Li, L., et al. P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for clouds. in *17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*.(2016) IEEE.

[16] Tamizharasi, G., B. Balamurugan, and H.A. Gaffar. Privacy preserving ciphertext policy attribute based encryption scheme with efficient and constant ciphertextsize. in *International Conference on Inventive Computation Technologies (ICICT)*.(2016) IEEE.

[17] Shoukun, W., W. Kaigui, and W. Changze. Attribute-based solution with time restriction delegate for flexible and scalable access control in cloud storage. in *Proceedings of the 9th International Conference on Utility and Cloud Computing*.(2016) ACM.

[18] Phuong, T.V.X., G. Yang, and W. Susilo, Hidden ciphertext policy attribute-based encryption under standard assumptions. *IEEE Transactions on Information Forensics and Security*, (2016). **11**(1): p. 35-45.

[19] Vaduganathan, D. and S. Ramasami, Attribute Based Encryption with Attribute Hiding in Cloud Storage. *International Journal for Trends In Engineering & Technology*, (2015). **3**(3).

[20] Yadav, U.C. Ciphertext-policy attribute-based encryption with hiding access structure. in *IEEE International on Advance Computing Conference (IACC)*.(2015) IEEE.

[21] Yadav, U.C. and S.T. Ali. Ciphertext policy-hiding attribute-based encryption. in *International Conference on Advances in Computing, Communications and Informatics (ICACCI)*.(2015) IEEE.

[22] Jin, C., X. Feng, and Q. Shen. Fully Secure Hidden Ciphertext Policy Attribute-Based Encryption with Short Ciphertext Size. in *Proceedings of the 6th International Conference on Communication and Network Security*.(2016) ACM.

[23] Li, J., Y. Shi, and Y. Zhang, Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage. *International Journal of Communication Systems*, (2015.

[24] Huang, W.-B., W.-T. Su, and C.-S. Liang. A threshold-based key generation approach for ciphertext-policy attribute-based encryption. in *Seventh International Conference on Ubiquitous and Future Networks (ICUFN)*.(2015) IEEE.

[25] Rouselakis, Y. and B. Waters. Efficient statically-secure large-universe multi-authority attribute-based encryption. in *International Conference on Financial Cryptography and Data Security*.(2015) Springer.

[26] Gorasia, N., et al., Improving Security in Multi Authority Attribute Based Encryption with Fast Decryption. *Procedia Computer Science*, (2016). **79**: p. 632-639.

[27] Wei, J., W. Liu, and X. Hu, Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage. *IEEE Systems Journal*, (2016.

[28] Rahman, M.S., A. Basu, and S. Kiyomoto. Decentralized Ciphertext-Policy Attribute-Based Encryption from Learning with Errors over Rings. in *Trustcom/BigDataSE/I SPA*.(2016) IEEE.

[29] Jiang, Y., et al., Ciphertext-policy attribute-based encryption against key-delegation abuse in fog computing. *Future Generation Computer Systems*, (2017.

[30] Rahman, M.S., A. Basu, and S. Kiyomoto. Decentralized Ciphertext-Policy Attribute-Based Encryption from Learning with Errors over Rings. in *Trustcom/BigDataSE/I SPA, 2016 IEEE*.(2016) IEEE.