Attribute-based Encryption in Cloud Computing Environment

Yuping Yan
Department of Computeralgebra
Eotvos Lorand University
Budapest, Hungary
yupingyan@inf.elte.hu

Mohammed B. Alshawki
Eotvos Lorand University
Budapest, Hungary
Hochschule Furtwangen University
Furtwangen, Germany

Peter Ligeti
Department of Computeralgebra
Eotvos Lorand University
Budapest, Hungary
turul@cs.elte.hu

***Abstract*—Attribute-Based Encryption (ABE) scheme as a new cryptography primitive, shows its advantages in fine-grained access control mechanism and one-to-many flexible encryption mode. By conducting an in-depth study, we demonstrate the development trace, major work and research status of ABE. This paper mainly introduces the basic concepts of ABE, analyzes the research problems, namely key abuse, revocation, multi-authorities, and its applications on resource discovery and e-health especially in personal health record in cloud computing environment.**

***Index Terms*—attribute-based encryption, privacy preserving communication, cloud computing environment**

I. Introduction

Attribute-based encryption (ABE) is an extension of public key cryptography and identity-based encryption. In ABE scheme, both the ciphertext and the key are related to a set of attributes. According to the characteristics of information and the attributes of receivers, the encryptor can customize an encryption strategy, and the generated cipher text can be decrypted only by the users whose attribute satisfies the encryption policy.

Cloud computing environment, as a new approach to provide IT-related services, asks a higher requirements on users authentication, data management and encryption. ABE mechanism can effectively achieve non-interactive access control, greatly enriches the flexibility of encryption strategy and user authority, and expands from the previous one-to-one mode to one-to-many mode in distributed environment.

The traditional PKI encryption schemes can efficiently protect the data confidentiality, integrity and availability. However, there are four major drawbacks: 1). The users' data is completely transparent to the storage server, which leads to the leakage of users' privacy. 2). One-to-one encryption mode and the management of public keys make a high processing cost and high bandwidth consumption. 3). PKI asks for the real public key certificate of users, which has the problem of miscellaneous and multiple communications between users and servers; 4). In untrusted systems and continuously available computing environment, there are more requirements for data sharing and processing, while the resources providers also need to develop more flexible and scalable access control strategies to control the users' privileges. However, PKI encryption can not meet this requirement any more.

Fortunately, the ABE mechanism can effectively fight against these defects with its specific attributes. 1). Messages are encrypted based on the attributes of users, without paying attention to the number and identify of the members, as a result, the data encryption cost is reduced while the user privacy is protected. 2). The collusion attack is partially addressed, because the user key is related with random polynomials. Users with different identities cannot combine their keys to reach attribute requirements. 3). ABE supports the implementation of various threshold and logical operations such as 'or', 'and', 'negation' gates and Boolean expressions, which leads to a more flexible access control strategy.

Based on the characteristics of attribute-based encryption algorithm, it has a wide range of applications in the fields of distributed file management, third-party data storage, directional broadcast and so on. This paper will elaborate the basic ABE algorithms in this second chapter; in the third chapter, we will demonstrate the development trace, major work and recent research status. Furthermore, we will analyze the existing research problems in important use-cases, namely key abuse, revocation, multi-authorities. Last but not least, its applications will also be involved especially in resource discovery in IoT networks and Personal Health Record in cloud computing environment in the final two chapters.

II. Background and related work

In contrast to the traditional public key encryption algorithms, the decryptor in ABE is a subset of users, not a single one which is possible by introducing the concept of attributes. It uses the combinations of subsets' attributes as the public key to encrypt all the data, while the private key is calculated and assigned to the individual by the attribute authority based on the user attribute. Standing on the bilinear pairing techniques, the ABE builds the various access structures to achieve fine-grained access control of data. We will give the explanations

This research has been partially supported by project no. ED_18-1-2019-0030 (Application-specific highly reliable IT solutions) has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the Thematic Excellence Programme funding scheme and by the European Union, co-financed by the European Social Fund. (EFOP-3.6.2-16-2017-00013, Thematic Fundamental Research Collaborations Grounding Innovation in Informatics and Infocommunications) and by SH Programme.

978-1-7281-6330-7/20/$31.00 ©2020 IEEE.

of different mathematical definitions and the basic models of ABE, and its two main types: key policy (KP-ABE) and cipher-text policy (CP-ABE).

Definition 1. *Let $P = \{P_1, P_2, ...P_n\}$ be a set of n parties. An access structure is a collection Γ of non-empty subsets of P, i.e. $\Gamma \subseteq 2^{\{P_1, P_2, ...P_n\}}$. Any $U \in \Gamma$ is called authorized set, and any $X \notin \Gamma$ is called unauthorized set. We say Γ is monotonic access structure if for any M, N, if $M \in \Gamma$ and $M \subseteq N$, then $N \in \Gamma$.*

In ABE schemes, the access control is described by the users' attributes, while the core of the authorization set is the sets of attributes that can satisfy the access policy. Sahai and Waters [1] proposed the basic ABE, which can only support the simplest (t, n) threshold access structure, and can be described as follows: t is the value of threshold while the n represents the total number of visitors. If the access set is equal or larger than t, then we say the set is legal, that is, access possible, and vice versa. However, many practical applications need more flexible access control policies to support the "AND", "OR" and "NOT" gates, thus a variety of different types of access structures are proposed, such as AND gate access structures, LESS and tree access structures.

Definition 2 (Bilinear pairing [2])**.** *Let G and G_1, be two cyclic groups of prime order p and q respectively, and let $g \in G$ be a generator. A pairing is a map $e : G \times G \to G_1$, which satisfies the following properties:*

a. Non-degeneracy: $\exists g \in G, e(g, g) \neq 1$;

b. Bilinearity: $\forall x, y \in Z_p, \forall h, \Theta \in G$, $e(h^x, \Theta^y) = e(h, \Theta)^{xy}$;

c. Computability: $\forall h, \Theta \in G$, there exists an efficient algorithm to compute $e(h, \Theta)$.

Bilinear mapping is a function in which elements in two linear spaces can generate elements in the third linear space, and all parameters in the function are linear. Previously, it can only be used in the attack models of scheme proof. However, now it plays a more important role in encryption structures, especially in ABE and IBE. In many cases, the security of pairing-based protocols are related to the following variants of the Diffie-Hellman problems:

Definition 3 (Computational Diffie-Hellman assumption (CDH))**.** *Consider a cyclic group G of order q, a random generator g and random $a, b \in Z_q^*$, it is computationally intractable to compute the value g^{ab} from (g, G, q, g^a, b^b).*

Definition 4 (Decisional Diffie-Hellman (DDH) assumption)**.** *With the random $a, b, c \in Z_q^*$,(g^a, g^b, g^{ab}) and (g^a, g^b, g^c) cannot be clearly distinguished in polynomial time.*

Definition 5 (Bilinear Decisional Diffie-Hellman (BDDH) assumption)**.** *With the random $a, b, c \in Z_q^*$,(g^a, g^b, g^c, g^{abc}) and (g^a, g^b, g^c, g^d) cannot be clearly distinguished in polynomial time.*

It is obvious that if there is a bilinear pairing of $G \times G \to G_1$, the DDH problem can actually be solved quickly (CDH does not solve it). Therefore, cryptographic protocols based on bilinear pairings are generally based on BDDH (Bilinear Decisional Diffie-Hellman).

A. The basic ABE

The basic ABE consists of four phases: $Setup()$ to initialize, $Extract()$ to generate the keys, $Encrypt()$ to encrypt and $Decrypt()$ to decrypt. When the system is initialized, the BDH parameter generator runs to generate two cyclic groups G and G_1 of prime order p, generator g, and bilinear pairings $e : G \times G \to G_1$. d is the threshold parameter.

a. $Setup(\lambda, d) \to (PK, MSK)$: authorized institutions randomly select parameters $y, t_1, t_2, ...t_n \in Z_p$, and get the main system secret key $MSK = (y, t_1, ...t_n)$, while the public parameter $PK = (T_1 = g^{t_1}, ...T_n = g^{t_n}, Y = e(g, g)^y$.

b. $KeyGen(A_u, MSK) \to SK$:based on the threshold parameter d, the authorized institutions select a $d - 1$ degree polynomial P_x and make $P_x(0) = y$. The secret key of user is $SK = \{D_i = g^{p(i)/t_i}\}_{i \in A_u}$.

c. $Encrypt(m, A_c, PK) \to CT$: the sender inputs the attribute sets A_c and randomly select $s \in Z_p$, the cipher text $E = (A_c, M = mY^s = e(g, g)^{ys}m), \{E_i = g^{t_i S}\}_{i \in A_c}$.

d. $Decrypt(CT, SK) \to m$: if $|A_u \wedge A_c| > d$, then the receiver select any d, set as $i \in \{A_u \wedge A_c\}$, then compute $e(E_i, D_i) = e(g, g)^{p(i)s}$. According to the LaGrange polynomial, we can find $Y^s = e(g, g)^{p(0)s} = e(g, g)^{ys}$. Finally, the plaintext is calculated $m = CT/Y^s$. If $|A_u \wedge A_c| < d$, the receiver can not decrypt the message.

$KeyGen$ algorithm adopts the threshold secret sharing strategy to embed the secret y into the different components D_i in SK, meanwhile, SK relates to the random polynomial p to prevent collusion attack. Encrypt algorithm adopts bilinear pairing to encrypt the message and the users' attributes sets are embedded into the users' secret key, making the ciphertext relates to users' attributes. The random number can prevent the users from decrypting the subsequent ciphertext if the user decrypts successfully for the first time.

However, the access control strategy can not be decided by resource owners and it is limited from "AND", "OR" and "NOT" gate operations in the basic ABE. In order to solve these two disadvantages, Bethencourt et al. [5] proposed the CP-ABE mechanism, in which the ciphertext access policy is specified by the sender. Goyal et al [4] proposed a KP-ABE mechanism, which supports the "AND", "OR" and threshold operation of attributes.

B. The Key-Policy ABE

The algorithm shown below embeds tree access structure in users' secret keys. By using attribute sets to encrypt messages, it makes ciphertext associate with the encryption attribute sets.

The difference between KP-ABE and the basic ABE lies in the KeyGen and Decrypt algorithms.

b. $KeyGen(PK, MSK, A_{u-KP}) \to SK$, it still follows the secret sharing mechanism. First, we assume that d_x is the threshold value of node x, and define a $(d - 1)$

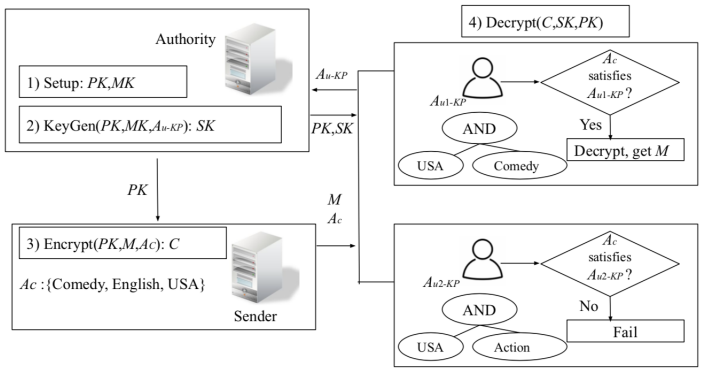

Fig. 1. KP-ABE illustration

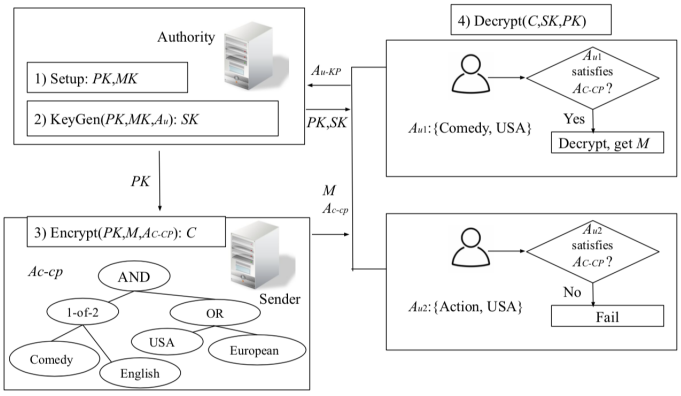

Fig. 2. CP-ABE illustration

degree polynomial P_x for each node x. By representing the root by r, we make $P_x(0) = y$. Meanwhile, the authorized institutions will randomly select d_r numbers of values which can satisfy P_r and fix the P_r. From the top to the bottom, we apply the formula $P_x(0) = P_{parents}(index(x))$ to calculate the values of $P_x(0)$ in each node. $Index(x)$ is the sequence of all children nodes in the parents node of x.

d. $Decrypt(CT, SK) \rightarrow m$: From the bottom to up, by using a recursive function, we decrypt each node to obtain the secret value to recover the plaintext.

From the algorithm and illustration, we found that KP-ABE can only afford "AND" operation. Ostrovsky et. al. [7] used the broadcast revocation mechanism to expand into "NOT" gates. However, it asks for a double size of ciphertext and secret keys.

C. The cipher-policy ABE

In CP-ABE mechanism, we embed the tree access structure into ciphertext, and combining attributes sets we generate the users secrete keys.

The CP-ABE is different from the basic ABE algorithm. The length of public keys and public parameters are independent from the number of system attributes. The uses two-level random masks to prevent user collision. The $KeyGen$ uses two-level random masks to prevent user collision. The Encrypt is similar with the $KeyGen$ algorithm of KP-ABE, and the only difference is $P_r(0) = s$. $Decrypt$ algorithm is similar with KP-ABE, but the operation number of bilinear pairing is doubled. The access tree embeds into the ciphertext, which makes data access conrtol is possible in CP-BAE, while KP-ABE has no authority check because the users' key includes access tree.

D. Comparison and analysis of different algorithms

The above three ABE algorithms have significant differences in complexity, strategy, flexibility, and the scope of applications.

Similarity: Both KP-ABE and CP-ABE can support complex access policies and afford threshold, "AND", "OR" and "NOT" gates operations.

Difference: KP-ABE fits more in the applications that users specify the requirements, such as pay television system, databases access, while CP-ABE is more suitable in situations that senders specify the strategy for accessing ciphertext, such

as social networking site access, electronic medical systems and so on.

III. Recent research problems of ABE

The core issues of algorithm security research are the correctness and security, key management and its scalability. At present, the main research work of ABE is divided into the ABE schemes, revocation schemes of ABE, accountability of ABE, and the multi-authorities of ABE. In ABE schemes, the dynamic property increases the complexity of key revocation, and the key is not relevant with users ID, which making it impossible to prevent and trace illegal users by pirating a legitimated user's private key. What is more, in most large-scaled distributed applications, multi-authentication parties are required to cooperate together to meet a higher scalability and fault tolerance. From all these aspects, we will discuss the main research challenges.

A. Keys and Attributes Revocation

Due to the key leakage and the changes of users permissions, it is inevitable to consider the revocation of keys and attributes. According to the definition of Attrapadung and Imai [6], the current approaches of keys and attributes revocation are divided into indirect revocation and direct revocation. In direct revocation mode, the sender specifies the revocation list when encrypting the messages, which achieving the revocation directly. In indirect revocation mode, the authorized institution releases the key update periodically and only the users who are not revoked can update the key.

1) Directed revocation: It was first proposed by Ostrovsky et. al. [7] in CP-ABE scheme. Combing with the "NOT" gate access control strategy, it associates the revoked user attributes with ciphertext, which revoked users can not decrypt the ciphertext but it increases the size of ciphertext and users' private keys.

2) Indirected revocation: The first solution given by Pirretti et al. [8] was to limit the use of keys by issuing an additional expiration data attribute. During update, the key artifacts corresponding to the attributes are no longer issued. However, this approach is quite inefficient and can not reach the practical application requirements. For examples, the encryption parties should negotiate with organization to set attribute validity period. During updating, the workload of key update mechanism linearly relates to the number of users in the system, and a secure channel is required between the key update mechanism and each user.

In order to reduce the stress on the key renewal agency, eliminate the coordination between encryption parties and organizations, Bethencourt et al [5] proposed a revocable ABE scheme using binary tree. Each user is set to associated with the leaf node of the binary tree, thus the number of key updates is logarithmic to the number of users. The key is divided into private keys, which relates to the access control structure and key update, which relates to the time, and is published by authorized parties to eliminate online interaction during update. Throught broadcast, the authority can update the keys without any interactions or secure channel. However, such revocation is essentially a complete revocation of the user keys. In reality, it is necessary to revoke user attributes in a fine-grained way rather than revoking all permissions.

In order to achieve immediate revocation rather than complete revocation, Ibraimi at al [9] introduced a semi trusted third party as arbiter. Basically, a trusteed third party publishes a list of revoked users, and the sender directly excludes the revoked user during encryption. However, the arbitrator holds part of the key and participates in the deception, so he must be honest and online.

B. Multi-Authority Attribute Based Encryption

In traditional ABE mode, there is only one trusted organization to manage all attributes. However, in practice, single institution can not satisfy the requirements of large-scale distributed environment, and attribute authority is vulnerable to centralized attack. In addition, the workload of distributing all users' authentication keys by a single institution is too heavy. Thus, we need a multi-authority scheme to reduce the workload, and decrease the attack risk. Multi-authority attribute based encryption (MA-ABE) is first proposed by Chase et al. [10], in which multiple organization manage different attribute sets and distribute keys within their authority. However, this schemes asks for a centralized organization which should be fully trustful, otherwise, the whole system will crash. According to apply of central authority (CA), the current research is divided into multi-authority with CA and multi-authority without CA.

The multi-authority ABE system includes data owner (DO), Data User (DU), and n attribute authority (AA). A user proves to one of the attribute authorities that his attributes and requests for the corresponding decryption keys. The combination of all attribute authorities main keys is the main key of the whole system. If you have enough different attribute users, the main key is easy to be leaked. Thus, the contradiction of correctness of decryption and the security of the system is the research difficulty of multi-authority ABE.

In order to solve the trust problem of CA, Bozovic et al. [11] proposed a semi-honest CA based on the DBDH assumption. In order to avoid the security vulnearbility bought by CA, Lin et al [12] proposed a threshold MA ABE by used key distribution (DKG) and joint zero secret sharing (JZSS) technology [13].

C. Accountability of ABE

In ABE schemes, the abuse of private key is particularly serious. The difficulty of accountability of ABE lies in the trace of pirated keys. Currently, the source of the pirated key is mainly from users and authorized agencies. The solutions for determining the responsibility of pirated keys are the following:

a). Li, Ren and Kim [15] positions responsibility to users or authorized institutions regarding the accountability in CP-ABE. This strategy effectively prevents key sharing between collusion users. The users first obtains his own certificate

public key by registering with a trusted certificate center, and then applies for an attribute private key to the authority. The user's decryption key contains private key corresponding to the certificate public key. It is assumed that the confidentiality of the key in the certificate is higher than the attribute private key issued by the authority. If users share their decryption key, the private key of the certificate will be leaked. This pirated key tracking algorithm determines whether there is the private key of the certificate that has a valid certificate public key. If it exists, it means that the users has leaked its decryption key; otherwise, it is from authorized institution.

b). Li et. al. [15] positions responsibility to users and achieve hiding policy in CP-ABE. The core of this algorithm is to embed the users' identity into attribute private key to prevent collision attacks and sharing keys. This tracking encryption algorithm focuses on the suspicious users. Only suspicious users whose attributes set meets the cipher-text policy can decrypt the message. Thus, we can determine the originator of the pirabted key.

c). Yu et al. [16] locates responsibility to the users, and the senders hide some attributes. It proposed against key abuse KP-ABE (AFKP-ABE) based on the DBDH and D-Linear assumptions. A unique identity is associated with a user and is embedded as an attribute in the user's private key. The tracking algorithm relates the relevant attributes of the suspicious identifier with the ciphertext. Thus, only the users with the suspicious identifier can decrypt the tracing ciphertext, thereby poviding the evidence of piracy.

IV. ABE in Resource Discovery

The number of connected devices in Internet of Things (IoT) is growing exponentially, and the amount of produced data by these participating devices is increasing as well. The IoT networks allow observing the physical environment (e.g. through sensors) and perform actions (e.g. through actuators). But, these devices mostly have limited computation and storage power and the generated data by these devices is transferred and stored on a more powerful node (e.g. in the cloud). Securing the transmitted data in the IoT is challenging due to huge number of devices, limited computing power of IoT devices and the connectivity feature that is provided by the IoT. These challenges vary depending on the IoT application.

In resource discovery [23], the resources are discovered in the network depending on their attributes. Without a proper authentication and confidentiality mechanisms, these resources are vulnerable to attacks such as unauthorized access or denial of service. On the other hand, the initiator of the discovery request is also vulnerable to revealing its sensitive data during an insecure discovery process. The issues in the resource discovery can be summarized in three points: access control, privacy and availability. In *access control*, the data that is provided by the resources need to be accessible by authorized entities in the network. The *privacy* of the entities in the network has to be guaranteed, i.e. the issuer of a discovery process provides some information about itself and the required resources during the discovery process. The issuer has to control on the potential entities that might access to this information which might leads to privacy issues. In the networks without any restrictions on the discovery process, the *availability* of the resources can be attacked, to prevent the authorized entities to have access to the required resources.

Adopting ABE in resource discovery makes the authentication and access control to be done without any need to a centralized trusted third party. Therefore, the communication can be secured and work in peer-to-peer mechanism. Authors in [24] utilized ABE to secure the request the issuer of the lookup process during the resource discovery. Attributed based Encryption was used to add security during the service discovery process by protecting the user's requests and restricting the access to the discovery of a service. In addition, adopting ABE in the discovery restricts the access to the resources in the system. However, their solution is still vulnerable for the denial of service attack. Wang et. al. [25] proposed a distributed ABE for discovery in mobile social networks. The proposed scheme utilize multi-authority ABE that achieves the fine grained access control and privacy without additional special signatures. The initiator encrypts the information with an access policy defined by herself.

V. ABE in E-Health

PHR (Personal Heath Record) system is a patient centered electronic medical information exchange platform. Patients can manage, maintain their medical data in this system, and share their personal information with their families and friends. Meanwhile, medical staffs can get access to a patient's complete medical records online, which helps to make more efficiently and accurately develop medical plans for patients. With the increase of all kinds of data and the continually development of cloud computing applications, to store data in cloud computing environment is becoming more and more common and popular. With its high reliability, dynamic scalability and low cost, patients tend to upload their PHR to the cloud, so that they can access the data in the cloud anytime and anywhere using intelligent terminal devices.

However, there are some privacy issues we should consider. ABE mechanism is considered as the best choice for efficient information sharing in the cloud environment, by solving the problems of access control, security and efficiency that the traditional public key cryptography system can not handle in the cloud environment. However, some sensitive information is always set as the attributes in access policy by encryptor, such as dental,Europe which is set by the patient in the personal health system. These attribute information is rather easy to disclose the privacy of the patient. Therefore, how to realize the privacy protection of sensitive information in the cloud environment data sharing has become the focus of research in this area.

Wang et al. [17] proposed hierarchical attribute-based encryption for fine-grained access control in cloud storage services. They achieved secure medical data transfer and consolidation by first combining the hierarchical identity-based encryption (HIBE) system and the ciphertext-policy

attribute-based encryption (CP-ABE) system, and then making a performance-expressivity tradeoff, finally applying proxy re-encryption and lazy re-encryption to the proposed scheme. In order to achieve fine-grained access control and extensible data control for PHR, the paper [18] uses priority level based encryption (PLBE) technology to encrypt PHR files.

Xhafa et al. [19] proposed the attribute based health record sharing system with privacy aware in cloud computing. It adopts the multi-authority cipher-policy ABE to achieve user accountability, which protects the privacy of users by hidden access policies. Han et al. [20] proposed a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme to improve the security and privacy. This is the first paper that protect the users' attributes by adopting commitment and zero knowledge proof technologies. Qian et al. [21] did their reseach on the direction of PHR with ABE attribute revocation. It supports users attribute revocation and strategy updates based on multi-authority attribute-based encryption.

Summarizing the above, most of the ongoing research use ABE as a cryptography tool to achieve fine-grained access control and privacy preserving in cloud management system. However, there is no existing efficient solution of PHR with ABE scheme solving the problems of attribute revocation and user accountability in distributed multi-authorities cloud computing environment.

VI. Conclusion and future work

This paper briefly introduces the concepts of attribute-based encryption with its research problems and applications of ABE schemes especially in resource discovery (RD) and Personal Health Record (PHR). Concluding the above, we suggest some interesting future research topics:

a. Currently, there is no method for user accountability in basic ABE;
b. The problem of the trustworthiness of authorized institution. In ABE schemes, once the authorized institution is destroyed, the attackers can obtain the key of any user and decrypt all ciphertexts. Actually, Goyal et al. [22] adopts black box mode to solve the problem of the complete trustworthiness of the authorized institution in IBE system, but in ABE mechanism, there is still no effective solution;
c. There is still no solution for the attribute revocation CP-ABE scheme with user accountability. The current research has realized the flexible and revocable CP-ABE mechanism under the standard assumption. However, it does not solve the problem of user accountability.

References

[1] A. Sahai, B. Waters, "Fuzzy identity based encryption", Advances in Cryptology EUROCRYPT 2005. Berlin, Heidelberg: Springer Verlag, 2005. pp. 457–473.

[2] D. Boneh, M. Franklin, "Identity-Based encryption from the weil pairing", SIAM Journal on Computing, vol. 32(3), 2003, pp. 213–229.

[3] Z. Yang, J. Schwenk, "Strongly authenticated key exchange protocol from bilinear groups without random oracles", International Conference on Provable Security, 2012, pp. 264–275.

[4] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-Based encryption for fine-grained access control of encrypted data", Proc. of the 13th ACM Conf. on Computer and Communications Security. New York: ACM Press, 2006, pp. 89–98.

[5] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-Policy attribute-based encryption", Proc. of the 2007 IEEE Symp. on Security and Privacy. Washington: IEEE Computer Society, 2007, pp. 321–334.

[6] N. Attrapadung, H. Imai, "Conjunctive broadcast and attribute-based encryption", Proc. of the Pairing-Based Cryptography-Pairing, 2009, pp. 248–265.

[7] R. Ostrovsky, A. Sahai, B. Waters, "Attribute-Based encryption with non-monotonic access structures", Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2007, pp. 195–203.

[8] M. Pirretti, P. Traynor, P. Mcdaniel, B. Waters, "Secure attribute-based systems", Proc. of the ACM Conf. on Computer and Communications Security. New York: ACM Press, 2006, pp. 99–112.

[9] L. Ibraimi, Q. Tang, P. Hartel, W. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes", Proc. of the Information Security Practice and Experience. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 1–12.

[10] M. Chase, "Multi-authority attribute based encryption", Proc. of Theory of Cryptography Conf. Berlin: Springer, 2007, pp. 515–534

[11] C. V. Bozovi, D. Socek, R. Steinwandt, I. Villany, "Multi-Authority attribute based encryption with honest-but-curious centralauthority", International Journal of Computer Mathematics, vol. 89(3), 2009, pp. 268–283.

[12] H. Lin, Z. Cao, X. Liang, J. Shao, "Secure threshold multi authority attribute based encryption without a central authority", Proc. of the Cryptology in India-INDOCRYPT 2008, 2008. pp. 426–436.

[13] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems", Journal of Cryptology, vol. 20(1), 2007, pp. 51–83.

[14] J. Li, K. Ren, K. Kim, "A2BE: Accountable attribute-based encryption for abuse free access control", IACR Cryptology ePrint Archive, 2009, pp. 118-134.

[15] J. Li, K. Ren, B. Zhu, Z. Wan, "Privacy-Aware attribute-based encryption with user accountability", Proc. of the Information Security Conf., 2009, pp. 347–362.

[16] S. Yu, K. Ren, W. Lou, J. Li, "Defending against key abuse attacks in KP-ABE enabled broadcast systems", Proc. of the Security and Privacy in Communication Networks, 2009, pp. 311–329.

[17] G. Wang, Q. Liu, J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services", Proc. of the 17th ACM Conference on Computer and Communications Security, 2010, pp. 735–737.

[18] D. Sangeetha, V. Vijayakumar, "Enhanced security of phr system in cloud using prioritized level based encryption", Proc. of International Conference on Security in Computer Networks and Distributed Systems, 2014, pp. 57–69.

[19] F. Xhafa, J. Feng, Y. Zhang, "Privacy-aware attribute-based PHR sharing with user accountability in cloud computing", Journal of Super computing, vol. 71(5), 2015, pp. 1607–1619.

[20] J. Han, W. Susilo, Y. Mu, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption", IEEE Trans on Information Forensics and Security, vol. 10 (3), 2015, pp. 665–678.

[21] H. Qian, J. Li, Y. Zhang, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation", International Journal of Information Security, vol. 14(6), 2015, pp. 487–497.

[22] V. Goyal, S. Lu, A. Sahai, B. Waters, "Black-Box accountable authority identity-based encryption", Proc. of the ACM Conf. on Computer and Communications Security, 2008, pp. 427–436.

[23] M. B. Alshawki, B. Crispo, P. Ligeti, "A Decentralized and Scalable Model for Resource Discovery in IoT Network", IEEE 15th Interna-tional Conference on Wireless and Mobile Computing, Networking and Communications, 2019.

[24] Y.S. Trabelsi,Y. Roudier, "Enabling Secure Service Discovery with Attribute Based Encryption", Institut Eurecom Department of Corporate Communications, 2006, pp. 1–19.

[25] W. Wang, F. Qi, X. Wu, Z. Tang, "Distributed multi-authority attribute-based encryption scheme for friend discovery in mobile social net-works", Procedia Computer Science, vol. 80, 2016, pp. 617–626.