L-009

A Survey on Attribute-based Encryption and its Application in Cloud and Mobile Environment

安村 慶子† 石巻 優† 今林 広樹† 山名 早人†
Yoshiko Yasumura Yu Ishimaki Hiroki Imabayashi Hayato Yamana

1. Introduction

In the recent years, cloud services are utilized by many users in order to store and share data with other users so that it is easily accessible from anywhere at any time through mobile devices such as tablets and smartphones. As a result, currently, there are large amount of data on cloud servers that is managed by many users. However, if the data is stored in the server without encryption, it is possible for the cloud server itself to access and view the contents of stored data freely without any authorization. Therefore, it is not secure to store data within servers without any encryption.

While on the other hand, if we are to encrypt such sensitive data for sharing with multiple users using a traditional public encryption scheme, two problems arise. Firstly, the user will need to obtain the public key from every individual and encrypt data for each user which would be quite a handful work. Secondly, and more importantly, a user may want to share data with individuals with certain attributes, such as department or position, but may not know who has the attributes. In such case, it is not possible for the user to encrypt the data as we are not able to obtain the public key of the intended recipient. Therefore, traditional public key encryption is insufficient for sharing of data with multiple users.

Attribute-Based Encryption (ABE) is an encryption scheme first introduced by Sahai and Waters [1] that allows both data security as well as fine-grained access control of allowing different access rights to users. In this encryption scheme, attributes are associated to encrypted data and users using one of the two main ways (types), called Key-Policy ABE and Ciphertext-Policy ABE, such that only users with correct attribute keys can decrypt data. This resulted in a public encryption scheme that has one-to-many correspondence between the encryption key and decryption key instead of the traditional one-to-one correspondence. This encryption scheme has many places for application and in the recent years, with the rise of cloud, research on application of ABE for cloud and mobile has largely increased.

Although it is broadly categorized as ABE, many variants of ABE were proposed over the years for different scenarios and considerations. Some ABE schemes were proposed to achieve higher fine-grained access control, some to achieve higher efficiency such as constant-size ciphertexts, and some to satisfy other needs such as revocation to remove users or their attributes upon system update or finding malicious users, and privacy-preservation of not only data but user information. Therefore, the field of ABE schemes is vast with different ABE schemes designed for different application scenarios. In this paper, while focusing on application of ABE to cloud and mobile devices, various ABE schemes will be introduced along with its limitations that needs to be overcome. In particular, ABE schemes and concepts from papers that can be considered as mainstream will be introduced, followed by concepts more important for cloud and mobile.

The rest of this paper is organized as follows: In Section 2, the first ABE scheme as well as two main types of ABE schemes will be introduced as background of ABE. In Section 3, other ABE schemes and concepts from mainstream papers will be introduced as they are important in the research field of ABE and has many places for application. In Section 4, ABE scheme considerations for cloud and mobile applications will be introduced as well as some application of ABE. In Section 5, we will briefly summarize the various ABE schemes and in Section 6, we will give our conclusion.

2. Background on Attribute-Based Encryption

In this section, the background on ABE will be provided. In Section 2.1, the first ABE scheme, Fuzzy ID-based Encryption, will be introduced. In Section 2.2, the two main types of ABE, Key-Policy ABE and Ciphertext-Policy ABE, will be introduced.

2.1 Fuzzy ID-based Encryption

The first attribute-based encryption scheme, called Fuzzy ID-based encryption (Fuzzy IBE), was introduced in 2005 by Sahai and Waters [1]. Fuzzy IBE is an encryption scheme made by combining secret sharing and ID-based encryption. In Fuzzy IBE, data are encrypted with set of attributes while the user's decryption key consists of a set of attribute keys such that users with at least certain number of matching attribute keys, called threshold, can decrypt the encrypted data.

For example, if five attributes are assigned to encrypted data with threshold of three, then any three attributes out of the five attributes needs to match the user's attributes in order to decrypt the data. Fig. 1 shows an example of Fuzzy IBE scheme. As shown in Fig. 1, Data 1 and 2 are encrypted with different attribute sets {A, B, C, D} and {B, C, D, E} with different threshold of two and three respectively. User 1, 2 and 3 are given different attributes, {A, B}, {B, C}, and {C, D, E} respectively. In the example, all users are able to decrypt Data 1 since their attributes satisfy the threshold condition of at least two attributes matching. Similarly, only User 3 is able to decrypt Data 2 as it is the only user that satisfies the threshold condition of three.

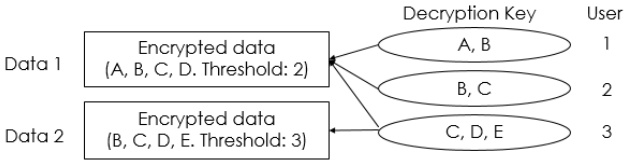

Fig. 1. Fuzzy ID-Based Encryption

This scheme, however, does not provide fine-grained access control, which refers to a differential access rights, as the decryption is based on a threshold. Therefore, the user who encrypted the data cannot exert control over who are able to

† 早稲田大学 Waseda University

decrypt the data and thus insufficient for systems such as cloud that requires fine-grained access control. Therefore, to achieve higher fine-grained access control, various ABE schemes were proposed over the years which will be introduced in the later subsections

2.2 Two main types of ABE

In Fuzzy IBE, the decryption is decided based on the threshold of the encrypted data, resulting in a lack of fine-grained access control. Therefore, in order to provide a different method to associate attributes to data and users so that decryption is not decided based on threshold, two variants of ABE were proposed: Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE). In these two schemes, an access structure of attributes, sometimes called policy, that can be expressed as a Boolean formula of AND and OR operations is used. The access structure is a tree structure of attributes, where leaves are attributes and nodes are Boolean operations in which AND and OR is expressed as n out of n and 1 out of n threshold respectively. In KP-ABE and CP-ABE, this access structure is used to define the decryption condition of the user decryption key or the ciphertext, respectively. Fig. 2 shows an example of a tree structure defined as {A AND (B OR C)} in which the nodes are the Boolean operations and leaves are the attributes.

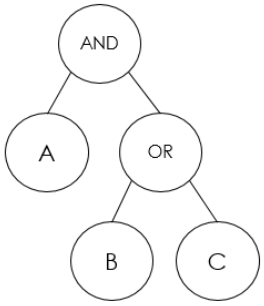

Fig. 2. Access Structure

2.2.1 Key-Policy Attribute-Based Encryption

Key-Policy Attribute-Based Encryption (KP-ABE) was first introduced in 2006 by Goyal et al. [2] in order to achieve more expressive access control in terms of AND, OR operations than Fuzzy IBE. KP-ABE is an encryption scheme in which the ciphertext is encrypted with set of attributes while the decryption key is given an access structure that defines the decryption condition. In this scheme, users are able to decrypt only the data that satisfy the access structure defined in their decryption key.

An example of KP-ABE is shown in Fig. 3. In Fig. 3, Data 1 and 2 is given attribute set {A, B} and {B, C} respectively, and User 1, 2, and 3 are given access structure {B OR D}, {B AND C}, {A OR D} respectively. As shown in the figure, Data 1 can be decrypted only by User 1 and 3 as the encrypted data attributes satisfy the OR condition of the user access structure while not satisfying the {B AND C} condition of User 2. Similarly, Data 2 can decrypted only by User 1 and 2 as User 1's {B OR D} condition, and User 3's {B AND C} condition is satisfied.

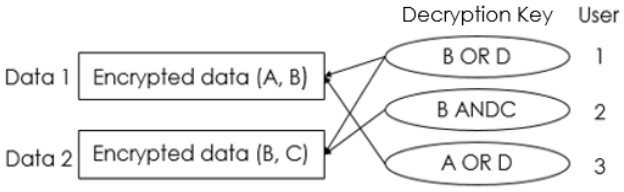

Fig. 3. Key-Policy Attribute-Based Encryption

Compared to Fuzzy ID-based encryption, KP-ABE provides more expressive access control as an access structure is defined for the decryption key. This KP-ABE scheme provides fine-grained access control to decrypting users in the sense that users choose which data to decrypt. However, it may be undesirable for some application as the encryptor cannot exert control over who are able to decrypt the data after encryption since the encrypted data only holds attributes [3].

2.2.2 Ciphertext-Policy Attribute-Based Encryption

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) was first introduced in 2007 by Bethencourt et al. [3] which was later improved to be secure under the standard model by Waters [4]. CP-ABE is the opposite of KP-ABE in the sense that in CP-ABE, the ciphertext is encrypted with an access structure while the decryption key consists of attribute keys. In this scheme, decryption of data is possible when the user's attributes satisfy the access structure defined in the encrypted data. Fig. 4 shows an example of CP-ABE. Data 1 and 2 are given access structure {A OR B} and {B AND C} respectively while User 1, 2, and 3 are given attributes {B, D}, {B, C} and {A, C} respectively. All users are able to decrypt Data 1 as they all satisfy the {A OR B} condition whereas only User 2 is able to decrypt Data 2 as it is the only attributes that satisfies {B AND C} condition.

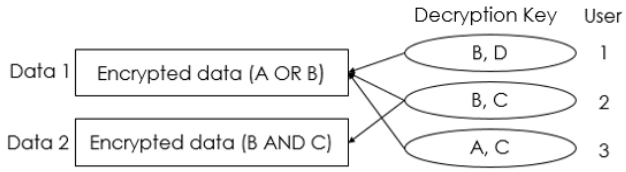

Fig. 4. Ciphertext-Policy Attribute-Based Encryption

This scheme achieves the desired fine-grained access control of data since the data is encrypted with an access structure that defines the decryption condition, enforcing stronger access control compared to Fuzzy IBE or KP-ABE. Therefore, CP-ABE is more often considered for application than KP-ABE. However, the main drawback to this scheme is the computation time during encryption and ciphertext size that increases linearly with respect to the size of the access structure. In KP-ABE, the encryption time and ciphertext size is O(n) where n is the number of attributes to be encrypted. While in CP-ABE, the encryption time and ciphertext size is O(A) where A is the size of the access structure (number of nodes). Thus, although both KP-ABE and CP-ABE has a linear growth, the CP-ABE requires more computation.

2.3 Collusion Resistant

In any ABE scheme, it is important that the encryption scheme is collusion resistant, meaning that users are not allowed to combine their attribute keys to decrypt data. In most ABE schemes, collusion resistance is achieved by using different exponent for each user when distributing the decryption key based on the concept of bilinear map. In some ABE schemes, such as multi-authority ABE, which is to be introduced in the later section, a unique identifier is given to users to avoid collusion attacks.

3. ABE Schemes

In this section, several important ABE schemes that were proposed over the years will be introduced. In Section 3.1, ABE scheme with negative attributes within its access structure, called non-monotonic access structure, will be introduced. In Section 3.2, two types of hierarchical ABE (HABE), hierarchical authority and hierarchical attribute, will be introduced. In Section 3.3, ABE scheme proposed for system with different entities, called Multi-Authority ABE, will be introduced. Finally, in Section 3.4, ABE with revocation, particularly how users or attributes are revoked, will be introduced.

3.1 Non-monotonic Access Structure

In the three ABE schemes described in Section 2, only monotonic access structures, an access structure containing only positive attributes, are supported. In case that we do not want certain attribute holders to access data, we can specify negative attributes explicitly such as "NOT:D" within the ciphertext. However, if there are many attributes that needs to be negated, it becomes necessary to define a new negative attribute for each attribute. In which case, the access structure will grow linearly, resulting in a ciphertext size and computation time that also grows linearly.

In order to address such issues, Ostrovsky et al. [5] introduced an ABE scheme that supports non-monotonic access structures (access structure with negative values) in 2007. Their proposed scheme achieved non-monotonic access structure that supports AND, OR, NOT and threshold for KP-ABE by implicitly specifying negative attributes in a way that a share of the secret sharing is available only if a given attribute does not exist in the set of attributes of the ciphertext. Thus, the need of defining a new negative attribute is eliminated. However, their proposed scheme was constructed for key-policy, needing to be adapted for more expressive access systems. Following their proposal, various papers were introduced such as [18], [19], and [20]. Lewko et al. [18] proposed a different KP-ABE with non-monotone access structure but also under a selective security model. Okamoto and Takashima [19] proposed KP-ABE and CP-ABE with non-monotone structure under full security. Attrapadung et al. [20] proposed KP-ABE with a non-monotone access structure and a constant-size ciphertext but under security of selective adversaries and non-interactive assumption.

3.2 Hierarchical Attribute-Based Encryption

In order to improve the performance and efficiency of the system Hierarchical Attribute-based Encryption (HABE) was introduced. In HABE, the system is organized in a tree structure, constructing a hierarchical relationship. However, as confusing as it is, there are two types of HABE scheme: hierarchical authority and hierarchical attribute. In most cases, the hierarchical authority type is applied as hierarchical attribute scheme is effective only when attributes can be organized into a tree structure.

3.2.1 Hierarchical Authority

The first HABE in which the authority is organized in a hierarchical manner was proposed by Wang et al. [6]. Their scheme is a combination of CP-ABE and Hierarchical Identity-Based Encryption (HIBE) [7]. Their scheme was proposed considering an enterprise that shares data using cloud servers. In their scheme, by having multiple domains that can fully delegate key generation, creation of attribute keys based on the attributes it has, the potential bottleneck at one single authority is reduced, resulting in high performance. This type of HABE is composed of a root master (RM), domain masters (DM) and users as shown in Fig. 5.

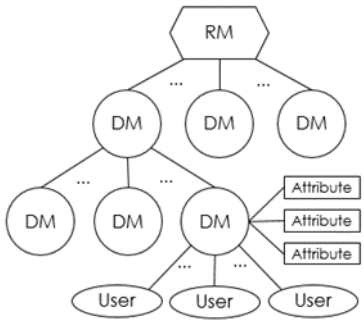

Fig. 5. Hierarchical Authority

The root master acts as the third trusted party that generate and distribute system parameters and domain keys to the domain masters and also mark the domain masters and attributes with an identifier to denote its position within the system. Then, the domain masters can act as the authority of the users under its domain, and generate keys for the users. In this scheme, rather than one single authority to generate and distribute all keys to users within the system, the process can be handled for a smaller number of users by creating different domains, improving the overall performance. However, the main drawback to their scheme is that it lacks expressivity as it uses disjunctive normal form policy and the attributes that a domain master manage is in one conjunctive clause, resulting in a performance-expressivity tradeoff.

3.2.2 Hierarchical Attribute

The first HABE scheme in which the attributes are organized in a hierarchical manner was proposed by Jin et al. [8]. In their scheme, the attributes are organized in a tree hierarchy structure such that the ancestral node can derive its descendant's key but the reverse is not possible. Fig. 6 shows a simple example of hierarchical attributes. In this example, attribute A is able to derive attribute keys of all attributes within its subtree. Similarly, Attribute C is able to derive attribute keys of D and E as they are a subtree of attribute C.

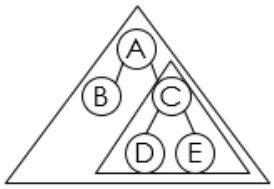

Fig. 6. Hierarchical Attribute

Their proposed scheme is a combination of HIBE and secret sharing technique utilized in Fuzzy IBE, resulting in an ABE scheme with attribute hierarchy in which certain number of attributes needs to match the attributes within the ciphertext in order to decrypt it. Therefore, the main drawback to their proposed HABE is the lack of access control.

3.3 Multi-Authority Attribute-Based Encryption

In all ABE schemes introduced so far, there is always one central authority that manages the entire system. In which case, if a system involves different entities, and a user has attributes distributed by different entities, the central authority will have to monitor all attributes within the system. Not only will the central authority become a potential bottleneck, the central authority needs to be absolutely trusted as well. To avoid such problems, it is more desirable to have the different entities manage their own attributes while users being able to use attributes from different entities together to decrypt data without involving the central authority.

The concept of Multi-Authority Attribute-Based Encryption (MA-ABE) was first introduced by Chase [9] as an ABE scheme that allows management of attributes by different entities without letting the central authority know the user's attributes. In her proposed scheme, a global identifier is issued to each user by the central authority so that the user’s identity is verifiable and no user can claim another user’s identity, and also to avoid collusion attacks from multiple users. The main drawback to her proposed scheme is that the decryption requirement is based on a threshold value and still requires one trusted central authority that will issue a setup key for user’s global identifier.

Although several MA-ABE schemes with no central authority were proposed, the MA-ABE proposed by Lewko and Waters [10] is applied by papers which considers multiple authorities. In their scheme, a global setup is run once to produce a global parameters to be used within the system. From there on, any party can become an authority and there is no need for global co-ordination except at the setup of the authority where it must take in the global parameters. In their proposed scheme, the concept of global identifier by Chase [9] is used to connect the attributes from different authorities, to identify users and to prevent collusion attacks.

3.4 ABE with Revocation

Revocation is one of the important concepts in not only cloud and mobile applications but in any general application. In real situations, users and their attributes within the system changes over time. A user’s position in the system may change, a user may leave the system, or a user was found out to be malicious and thus needs to be removed from the system. In such cases, it is crucial to be able to revoke the users or their attributes so that the users will no longer be able to user their keys to decrypt data that should now be inaccessible to them. Not only that, it is also important to revoke users or their attributes without affecting other users. Over the years, many ABE schemes were proposed with user and attribute revocation in mind. In general, there are two methods to achieve revocation.

3.4.1 Revocation List

One revocation method is usage of a revocation list introduced by Attrapadung and Imai [13]. In their proposed idea, user's private keys are associated with a user index ID, and ciphertext is associated with a list of user index in addition to the attributes or access structure depending on whether it is KP-ABE or CP-ABE such that users within the list will no longer be able to decrypt the data. By this method, no other users are affected by user revocation and re-encryption of ciphertext only is needed when the list is updated. For that reason, various ABE system such as [17], [22], and [23] adopts this method.

In [24] and [25], the revocation list is used differently than the above method. The alternate method is, rather than encrypting the data with a revocation list, to have the system check the revocation list when a user attempts to decrypt data. If the user is not within the revocation, the system allows the data to be decrypted. In [24], the cloud server checks the revocation list and calculates the decryption token for the user if the user is not within the revocation list. In [25], security mediator checks the revocation list and partially decrypts the data so that the user can fully decrypt it if the user is not within the revocation list. With this method, the re-encryption of ciphertext with updated revocation list becomes unnecessary but requires the user to trust the server that is checking the list.

3.4.2 Proxy Re-encryption

The method using revocation list efficient as the revocation of a user does not affect any other users. However, this method does not support attribute revocation of a user. A method to achieve individual attribute revocation was proposed by Yu et al. [12]. Their proposed scheme focused on attribute revocation for CP-ABE. CP-ABE has a master secret key for each attribute keys that is distributed to the user. Taking that into account they proposed re-encryption of the revoked attributes by updating the master secret key, ciphertexts and unrevoked users attribute keys such that the user with revoked attribute can no longer use the old attribute key to decrypt data. While it allows for attribute-level revocation, this method affects other users with the attribute as they need to compute their attribute keys.

4. ABE for Cloud and Mobile Devices

In this section, two important considerations when applying ABE to cloud and mobile devices will be introduced. In Section 4.1, outsourcing computation will be introduced as it is especially important when considering application of ABE to mobile devices. In Section 4.2, privacy-preservation for both user and recipient will be introduced. In Section 4.3, some application of ABE for cloud and mobile will be introduced.

4.1 Outsourcing Encryption and Decryption

Mobile devices are limited in resources in terms of battery and CPU. If an encryption requires long computation time, the encryption will also consume the limited amount of battery that the mobile devices have. Therefore, it is important that the computation time and energy consumption is low when applying ABE on mobile devices. With the emergence of cloud computing, outsourcing most of encryption and/or decryption has been considered by papers in order to have mobile devices compute as little as possible. However, of course, it is not secure to simply hand over the plaintext during encryption or the secret key during decryption. Therefore, when outsourcing encryption and/or decryption, the process is split between user and server in a way that user computes small part of encryption and decryption while the server computes the rest.

Green et al. [14] first proposed an ABE scheme in which the decryption of the ciphertext is outsourced to a server. In their proposed scheme, during decryption, the ciphertext is transformed into a short ElGamal ciphertext by the server which is then decrypted by the user to obtain the plaintext. Zhou et al. [15] proposed an ABE scheme in which both encryption and decryption is outsourced to a server. During encryption, the access structure is made of two subtree such that the user encrypts one subtree (usually smaller subtree with less nodes) and the server encrypts the other subtree. Finally, the server combines the two encrypted subtrees into one as shown in Fig. 7.

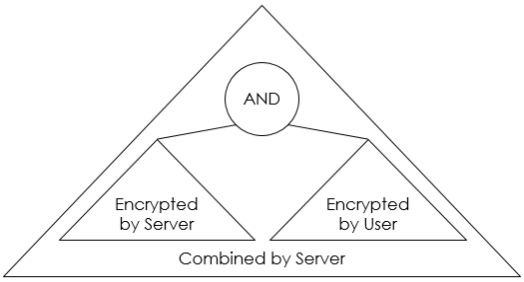

Fig. 7. Outsourced Encryption

During decryption, the user blinds its private key and sends it to the server such that the obtained message after the decryption is not yet the plaintext. The user obtains the plaintext by performing the last computation on the message.

Following their work, Lai et al. [26] and Li et al. [27] proposed outsourcing ABE schemes with verifiability of the outsourced decryption by introducing extra algorithms. In their scheme, the users are able to verify that the decryption conducted by the server is honest and no fraud activity has occurred.

As such, computation can be securely outsourced to servers while not disclosing any crucial information such as the plaintext and private keys to the servers. This greatly reduces the computation needed to be done by the users which is very desirable when considering application of ABE for mobile devices that is limited in resources.

4.2 Privacy-Preservation

In a cloud computing environment in which data are outsourced to be stored on a server that is outside the user's trust domain, privacy becomes a concern for many users. In ABE, attributes acts as the identifying feature of the users which can be considered as a sensitive information. Therefore, users may want to hide their attributes to the authority, or hide the access policy of the ciphertext as that discloses the attribute information of the intended recipients.

In Section 4.2.1, the concept of hiding attributes from authorities will be introduced. In Section 4.2.2, the concept of hiding the access policy of ciphertext will be introduced.

4.2.1 Hiding User Attributes

MA-ABE proposed by Chase [9] and Lewko and Waters [10] can be considered as a starting point for hiding attributes from authorities. Within the scheme by Chase, the central authority does not obtain any information about what attributes the user has obtained from entities whereas the scheme by Lewko and Waters does not have a central authority. Although all of the attributes that a user has is not known to the system, the attributes distributed by an authority is known to that same authority.

There are not many papers that considers privacy-preservation in this direction as most considers hiding the access policy. Rather recently, Jung et al. [11] proposed a method to allow users to obtain attribute keys from different authorities (MA-ABE) without disclosing the attribute. In their proposed method, 1-out-of-n Oblivious Transfer is used to distribute the attribute keys to users by categorizing attributes so that users are able to obtain only one key from each category. By this method, users are able to obtain attribute keys while not letting the authorities know which key the user received. The drawbacks to their proposed method is that it does not support revocation and also needs extra communication to conduct the 1-out-of-n oblivious transfer.

4.2.2 Hiding the Access Policy

The concept of hiding the access structure of a ciphertext was introduced by Nishide et al. [16]. In their proposed scheme wildcards are used to indicate that certain attributes are not relevant to the policy but in a hidden way in order to achieve hidden access policy of the ciphertext. Following their proposal, several schemes were proposed for hidden access policy. There are two ways to how the authors achieved hidden access policy. First method is, similar to Nishide et al., usage of wildcards when encrypting data. The other method is usage of composite order bilinear group [29], [30]. However, to the best of our knowledge, both methods of hiding access policy supports only access structure with AND operations [16], [28], [29], [30].

4.3 Application

Common application of ABE is to secure data that are to be stored in a cloud server. In fact, most ABE schemes proposed in the recent years are for cloud storage application so that users can encrypt and store data securely on cloud servers.

In [22], the authors proposed an MA-ABE scheme with identity-based user revocation using a revocation list for controlling data stored in cloud. In their proposed scheme, rather

than encrypting the whole message with ABE, the message is encrypted with a symmetric key. The symmetric key is encrypted with CP-ABE and then attached to the ciphertext. In [31], the authors proposed a cloud-based electronic health record (EHR) system by applying threshold ABE. In their proposed scheme, the personal health records of a user is encrypted with symmetric key, and the symmetric key is encrypted with ABE. Their proposed scheme also enable search, revocation and efficient decryption at local device by outsourcing. In [21], the authors proposed a different cloud-based EHR system using white-box traceable and revocable multi-authority ABE. White-box traceable refers to the capability of tracing users who has leaked their secret keys in which existing decryption equipment is used to decrypt using the leaked key. Therefore, by combining white-box traceable and revocation malicious physicians who leaked secret keys can be traced and revoked.

Aside from cloud storage, one interesting application of ABE exists for mobile devices using location. In [17], the authors proposed a location-enabled authentication system for mobile devices using ABE. In their proposed scheme, they use CP-ABE to encrypt messages using access structures based on location, services available for the user, and user attributes. Bluetooth Low Energy beacons are used to broadcast messages encrypted with access structure, and only mobile devices who are able to decrypt the message is able to engage in an automatic login process. With this method, users are able to log in to services provided at that specific location automatically.

Although outsourcing the computation to servers is considered often for applying ABE for mobile devices, there are also some research being done for handling all computation on mobile devices. In [32] and [33], the authors implemented KP-ABE and CP-ABE on Android smartphone devices to evaluate performance. In both papers, rather than directly encrypting a message with ABE, they encrypted the message using AES and then encrypted the symmetric key using ABE. Although [32] first considered usage of ABE on smartphone is challenging, the authors of [33] concluded that using ABE in this method for smartphone is feasible.

5. Summary

Many ABE schemes were proposed over the years for various situations and needs such as fine-grained access control and efficiency. Different ABE schemes has many areas for application that can be combined with other features such as revocation and outsourcing in order to satisfy the need of the system. Table 1 shows a brief summary of three ways of associating attributes to encrypted data and attributes. Table 2 shows usage, features and limitations of each ABE schemes. Similarly, Table 3 shows important concepts to ABE along with its method, feature and limitation.

Table 1: Association of Attributes to Data and Users

ABE scheme	Association of Attributes		Advantage	Limitation
	Data	User		
Fuzzy IBE [1]	List of attributes	Set of attribute keys	Computation time, ciphertext size and key size depend only on number of attributes	Based on threshold only so lacks fine-grained access control
KP-ABE [2]	List of attributes	Access structure	Smaller computation time and ciphertext size than CP-ABE	Encryptor cannot exert control over who can decrypt data
CP-ABE [3], [4]	Access structure	Set of attribute keys	Encryptor can specify the access structure of the data	Computation time and ciphertext size increase linearly with the size of the access structure

Table 2: ABE schemes

ABE Scheme	Feature	Usage	Advantage	Limitation
Non-Monotonic [5], [18], [19]	Can express negative attributes within the access structure	For more fine-grained access control by specifying NOT	Does not have to explicitly include negative attributes	Nevertheless increase in computation time for every negated attribute
HABE (Authority) [7]	Single system organized into a hierarchical structure	When system wishes to fully delegate key generation	Reduce burden on one central authority by distributing the system. Full delegation of key generation	Performance-expressivity tradeoff
HABE (Attribute) [8]	Attributes organized into a tree structure	Where attributes can be organized into a tree structure	Higher efficiency. Less keys to issue to users	Given only in threshold case
MA-ABE [10]	No central authority needed and any party can become an authority	When there are multiple entities within one system	No co-ordination needed between any authorities. Any party can become an authority	Uses random oracle

Table 3: Concepts to ABE

Concepts	Usage	Method	Advantage	Limitation
Revocation	To revoke users	Encrypting with Revocation List [13]	Does not affect other users	Requires re-encryption of ciphertext with updated revocation list
		Checking Revocation List [24], [25]	Does not affect other users. No re-encryption of ciphertext needed	Requires the user to trust the server
	To revoke attributes	Proxy Re-encryption [12]	Revocation at an attribute level rather than complete user revocation	Requires computation of a new master secret key and proxy key to change user attribute keys
Outsourcing	To lessen computation by users. Desirable for mobile devices.	Split up computation into user side and server side [14], [15], [26], [27]	Less computation needed by user side. Data and key privacy maintained	Computation server needs to be online
Privacy-Preservation	To preserve privacy of attributes from authority	1-to-n Oblivious Transfer [11]	Authority do not obtain any information of the user	No efficient revocation method
	To preserve privacy of recipients by hiding access policy	Wildcard [16], [28]	Supports negative attributes	Growth in access structure due to addition of wildcards. Only supports AND operations
		Composite Order [29], [30]	Only relevant attributes needed in the access structure	Does not support negative attributes. Only supports AND operations

6. Conclusion

ABE is an encryption scheme that achieves both data security and access control. Over the years, many various ABE schemes were proposed for higher fine-grained access control, efficiency and other needs such as revocation and privacy-preservation. In this paper, we introduced various important schemes from mainstream papers in the field of ABE and also introduced important considerations when applying ABE to cloud and mobile environment.

We conclude that for general application, research related to ABE is rather well-established as various applications could be constructed by the main ABE schemes and concepts depending on the needs as well as most systems are proven to be fully secure. Fine-grained access control can be achieved by using CP-ABE and multiple entities can collaborate in one system but without a central authority by using MA-ABE. Revocation of users or their attributes is also possible with two revocation methods to do so.

By taking advantage of cloud servers, most of computation can be outsourced to the servers to make ABE more applicable for mobile devices. Meanwhile, as these features can be realized, there are some tradeoffs between expressivity and performance regardless of what ABE scheme is used. In CP-ABE in particular, as the size of the access structure increase, the computation time and ciphertext size also increases linearly. Also, we believe that consideration and research towards user attribute privacy and access policy privacy is still in need. Currently, no efficient revocation method exists for attribute privacy and access policy privacy is supported only for access structures with AND operations. In order to protect the privacy of users in terms of both data and identity, addressing these two issues are important for application of ABE to cloud.

Acknowledgement

A part of this work was supported by CREST, JST.

Reference

[1] Amit Sahai, and Brent Waters, "Fuzzy identity-based encryption", Advances in Cryptology–EUROCRYPT 2005, LNCS, Vol. 3494, pp. 457-473, (2005).
[2] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, "Attribute-based encryption for fine-grained access control of encrypted data", Proc. of the 13th ACM Conf. on Computer and communications security, pp. 89-98, (2006).
[3] John Bethencourt, Amit Sahai, and Brent Waters, "Ciphertext-policy attribute-based encryption", Proc. of 2007 IEEE Symp. on Security and Privacy (SP'07), pp. 321-334, (2007).
[4] Brent Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization", Public Key Cryptography–PKC 2011, LNCS, Vol. 6571, pp. 53-70, (2011).
[5] Rafail Ostrovsky, Amit Sahai, and Brent Waters, "Attribute-based encryption with non-monotonic access structures", Proc. of the 14th ACM Conf. on Computer and communications security, pp. 195-203, (2007).
[6] Guojun Wang, Qin Liu, and Jie Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services", Proc. of the 17th ACM Conf. on Computer and communications security, pp. 735-737, (2010).
[7] Craig Gentry and Alice Silverberg, "Hierarchical ID-based cryptography", Advances in cryptology—ASIACRYPT 2002, LNCS, Vol. 2501, pp. 548-566, (2002).
[8] Jin Li, Qian Wang, Cong Wang, and Kui Ren, "Enhancing attribute-based encryption with attribute hierarchy", Mobile networks and applications, Vol. 16, No. 5, pp. 553-561, (2011).
[9] Melissa Chase, "Multi-authority attribute based encryption", Theory of cryptography, LNCS, Vol. 4392, pp. 515-534, (2007).
[10] Allison Lewko, and Brent Waters, "Decentralizing attribute-based encryption", Advances in Cryptology–EUROCRYPT 2011, LNCS, Vol. 6632, pp. 568-588, (2011).

[11] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption", IEEE Trans. on Information Forensics and Security, Vol. 10, No. 1, pp. 190-199, (2015).
[12] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "Attribute based data sharing with attribute revocation", Proc. of the 5th ACM Symp. on Information, Computer and Communications Security, pp. 261-270, (2010).
[13] Nuttapong Attrapadung and Hideki Imai, "Conjunctive broadcast and attribute-based encryption", Pairing-Based Cryptography–Pairing 2009, LNCS, Vol.5671, pp. 248-265, (2009).
[14] Matthew Green, Susan Hohenberger, and Brent Waters, "Outsourcing the Decryption of ABE Ciphertexts", Proc. of USENIX Security Symp. Vol. 2011, No. 3, (2011).
[15] Zhibin Zhou, and Dijiang Huang, "Efficient and secure data storage operations for mobile cloud computing", Proc. of the 8th Int'l Conf. on Network and Service Management, pp. 37-45, (2012).
[16] Takashi Nishide, Kazuki Yoneyama, and Kazuo Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures", Applied cryptography and network security, LNCS, Vol. 5037, pp. 111-129, (2008).
[17] Marcos Portnoi, and Chien-Chung Shen, "Loc-auth: Location-enabled authentication through attribute-based encryption", Proc. of 2015 Int'l Conf. on Computing, Networking and Communications (ICNC), pp. 89-93, (2015).
[18] Allison Lewko, Amit Sahai, and Brent Waters, "Revocation systems with very small private keys", Proc. of 2010 IEEE Symp. on Security and Privacy, pp. 273-285, (2010).
[19] Tatsuaki Okamamoto and Katsuyuki Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption", Advances in Cryptology–CRYPTO 2010, LNCS, Vol. 6223, pp. 191-208, (2010).
[20] Nuttapong Attrapadung, Benoît Libert, and Elie De Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts", Public Key Cryptography–PKC 2011, LNCS, Vol. 6571, pp. 90-108, (2011).
[21] Jun Zhou, Zhenfu Cao, Xiaolei Don, and Xiaodong Lin, "TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems", Prof. of 2015 IEEE Conf. on Computer Communications (INFOCOM), pp. 2398-2406, (2015).
[22] Máté Horváth, "Attribute-based encryption optimized for cloud computing", SOFSEM 2015: Theory and Practice of Computer Science, LNCS, Vol. 8939, pp. 566-577, (2015).
[23] Qiang Li, Dengguo Feng, and Liwu Zhang, "An attribute based encryption scheme with fine-grained attribute revocation," Proc. of Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 885-890, (2012).
[24] Xingbing Fu, and Zufeng Wu, "Ciphertext policy attribute based encryption with immediate attribute revocation for fine-grained access control in cloud storage", Proc. of 2013 Int'l Conf. on Communications, Circuits and Systems (ICCCAS), Vol. 2, pp. 103-108, (2013).
[25] Yuechen Chen, Zoe L. Jiang, S. M. Yiu, Joseph K. Liu, Man Ho Au, and Xuan Wang, "Fully secure ciphertext-policy attribute based encryption with security mediator", Information and Communications Security, LNCS, Vol. 8958, pp. 274-289, (2015).
[26] Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng, "Attribute-based encryption with verifiable outsourced decryption", IEEE Trans. on Information Forensics and Security, Vol. 8, No.8, pp. 1343-1354, (2013).
[27] Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang, "Securely outsourcing attribute-based encryption with checkability." IEEE Trans. on Parallel and Distributed Systems, Vol.25, No.8, pp. 2201-2210, (2014).
[28] Zhibin Zhou, Dijiang Huang, and Zhijie Wang, "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption." IEEE Trans. on Comput., Vol. 64, No. 1, pp. 126-138, (2015).
[29] Xiaohui Li, Dawu Gu, Yanli Ren, Ning Ding, and Kan Yuan, "Efficient ciphertext-policy attribute based encryption with hidden policy", Internet and Distributed Computing Systems, LNCS, Vol. 7646, pp. 146-159. (2012).
[30] Runhua Xu, Yang Wang, and Bo Lang, "A Tree-Based CP-ABE Scheme with Hidden Policy Supporting Secure Data Sharing in Cloud Computing", Proc. of 2013 Int'l Conf. on Advanced Cloud and Big Data (CBD), pp. 51-57, (2013).
[31] Fatos Xhafa, Jingwei Li, Gansen Zhao, Jin Li, Xiaofeng Chen, and Duncan S. Wong, "Designing cloud-based electronic health record system with attribute-based encryption", Multimedia Tools and Applications, Vol.74, No.10, pp. 3441-3458, (2015).
[32] Xinlei Wang, Jianqing Zhang, Eve M. Schooler, and Mihaela Ion, "Performance evaluation of attribute-based encryption: Toward data privacy in the IoT", Proc. of 2014 IEEE Int'l Conf. on Communications (ICC), pp. 725-730, (2014).
[33] Moreno Ambrosin, Mauro Conti, and Tooska Dargahi, "On the feasibility of attribute-based encryption on smartphone devices", Proc. of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, pp. 49-54, (2015).