ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

DATA LEAKAGE CONTROL MECHANISM FOR ATTRIBUTE BASED ENCRYPTION TECHNIQUE

Ms. D. SUGANYA,II[nd] ME (CSE),
MS.S.M.KARPAGAVALLI, ME , Assistant Professor/CSE
Al-Ameen Engineering College, Erode, Tamilnadu, India
dsuganya55@gmail.com, Karpagam.ration@gmail.com

Abstract

The public key cryptosystems are used to provide data confidentiality features. The access control mechanisms are not supported by the public key cryptography methods. The Attribute Based Encryption (ABE) schemes are applied to provide data confidentiality with access control policies. User privileges are assigned with separate key values and encryption process.

Ciphertext-policy attribute-based encryption (CP-ABE) enables fine-grained access control to the encrypted data for commercial applications. CP-ABE has two properties called traceability and large universe. Traceability is the ability of ABE to trace the malicious users or traitors who intentionally leak the partial or modified decryption keys for profits. The property of large universe in ABE enlarges the practical applications by supporting flexible number of attributes. In CP-ABE the number of attributes is not polynomially bounded and malicious users who leak their decryption keys could be traced. The storage overhead for traitor tracing is constant and suitable for commercial applications.

The CP-ABE scheme is adapted to secure the patient health record (PHR) in healthcare applications. User identity based security mechanism is integrated with the system. The Distributed Attribute Based Encryption (DABE) scheme is constructed with multi server access support. Dynamic role management mechanism is integrated with the system.

1. Introduction

Cryptography is the study of message secrecy. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of Automated Teller Machine (ATM) cards, computer passwords, and electronic commerce, which all depend on cryptography. The modern field of cryptography can be divided into several areas of study. The chief ones are discussed here;

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. This was the only kind of encryption publicly known until 1976. One round of the patented idea cipher, used in some versions of Pretty Good Privacy (PGP) for high-speed encryption. The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. A block cipher is, in a sense, a modern embodiment of Alberti's polyalphabetic cipher block ciphers take as input a block of plaintext and a key, and output a block of ciphertext of the same size. Since messages are almost always longer than a single block, some method of knitting together successive blocks is required. Several have been developed, some with better security in one aspect or another than others. They are the mode of operations and must be carefully considered when using a block cipher in a cryptosystem.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government. Despite its deprecation as an official standard, DES remains quite popular; it is used across a wide range of

applications, from ATM encryption to e-mail privacy and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken. Stream ciphers, in contrast to the 'block' type, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the output stream is created based on an internal state which changes as the cipher operates. That state's change is controlled by the key, and, in some stream ciphers, by the plaintext stream as well. RC4 is an example of a well-known stream cipher; Cryptographic hash functions do not necessarily use keys, but are a related and important class of cryptographic algorithms. They take input data, and output a short, fixed length hash, and do so as a one-way function. For good ones, collisions are extremely difficult to find. Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key is used to authenticate the hash value on receipt.

Symmetric-key cryptosystems typically use the same key for encryption and decryption, though this message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret. The difficulty of establishing a secret key between two communicating parties, when a secure channel doesn't already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world.

2. Related Works

Attribute Based Encryption (ABE) was first proposed as a fuzzy version of IBE. In CP-ABE [2], [3], [4], each user's private key is associated with a set of attributes and each ciphertext is encrypted by an access policy. To decrypt the message, the attributes in the user private key need to satisfy the access policy. The key difference between identity and attribute is that identities are many-to-one mapped to users while attributes are many-to-many mapped to users. Thus, to simulate a constant size conjunctive header, one needs to encrypt the message using each receiver's identity and the size of ciphertext is linearly increasing.

In [5], the authors proposed a CP-ABE scheme with constant size conjunctive headers and constant number of pairing operations. It must be noted that they did not seek to address the issues of recipient anonymity. One drawback of their scheme does not support wildcards in the conjunctive access policies. To decrypt a ciphertext, the decryptor's attributes need to be identical to the access policy. The model is still one-to-one, i.e., an access policy is satisfied by one attribute list or ID, which makes the number of access policies increase exponentially. Thus, their scheme can be simply implemented using IBE schemes with same efficiency by using each user's attribute list as his/her ID. We should note that in a system with attributes, the number of attribute combinations is 2^n. As the result, without using wildcards, there needs access policies to express all combinations. With wildcards, one can use a single access policy to express many combinations of attributes. Herranz et al. [1] proposed a more general construction of CP-ABE with constant ciphertext independently. Their proposed scheme achieves constant ciphertext with any monotonic threshold data access policy, e.g. n-of-n (AND), 1-of-n (OR) and m-of-n. Compared with our proposed PP-CPABE, their scheme does not consider recipient anonymity as one of the design goals.

To protect the privacy of the access policy, KSW scheme [2], NYO scheme, RC scheme [3] and YRL scheme were proposed, where the encryptor specified access policy is hidden. Specifically, the attribute names in both [3] are explicitly disclosed in the access policy, while only the eligible attribute

values are hidden. Also, YRL scheme was proposed in [7] based on BSW scheme [4] as a group key management scheme providing group membership anonymity.

We proposed a novel alternative to the hidden policy to preserve privacy efficiently. The main difference between our scheme and existing hidden policy attribute based encryption schemes is PP-CP-ABE significantly reduced the size of ciphertext to a constant size, while all existing hidden policy solutions requires ciphertext that is linearly increasing on the number of attributes in the hidden policy. It must be noted that the construction in this paper is developed from one of our earlier construction [4], where we proposed an ABE scheme with constant size ciphertext. The major improvements of in this paper are in 3 folds: 1) we introduce the privacy-preserving requirements for ABE and incorporate the privacy-preserving solutions into the previous approaches; 2) we present a PP-AB BE with an information theoretical analysis to address its complexity; and 3) we conduct a comprehensive performance evaluation.

ABE can be used as a perfect cryptographic building block to realize Broadcast Encryption (BE), which was introduced by Fiat and Naor. The encrypter in the existing BE schemes need to specify the receiver list for a particular message. In many scenarios, it is very hard to know the complete receiver list and it is desirable to be able to encrypt without exact knowledge of possible receivers. Also, existing BE schemes can only support a simple receiver list. It is hard to support flexible, expressive access control policies. A broadcast encryption with an attribute based mechanism was proposed in [8], where an expressive attribute-based access policy replaces the flat receiver list. Also, in [9] and [5], the authors proposed to use a CP-ABE and flat-table mechanism to minimize the number of messages and support expressive access policies. Compared with these works, our proposed scheme significantly reduces the size of ciphertext from linear to constant.

3. Chipertext-Policy Attribute Based Encryption(CPABE) Scheme

In traditional public key encryption, a user is privileged to share his/her data with others in a private manner. The access of a targeted user or device to the shared data is all or nothing. In other words, one can get the entire access capability to the shared data if given the secret key;nothing will be revealed. In many cases, this may not be enough. For example, a user may expect to share his/her data through a more general and expressive way based on the targeted user or a device's credentials. Sahai and Waters introduced the notion of Fuzzy Identity-Based Encryption (FIBE). Goyal et al. proposed two complementary forms of Attribute-Based Encryption (ABE): Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In the KP-ABE, users' decryption keys are issued according to an access policy and the ciphertexts are annotated by attributes. In the CP-ABE, users' decryption keys are issued according to the attributes they possess and the encrypting party specifies an access policy for the ciphertexts. A series of KP-ABE and CP-ABE schemes have been proposed, aiming at better expressiveness, efficiency or security. In particular, large universe and traceability are the two significant progresses in ABE.

Rouselakis and Waters proposed a new construction and proof method for Large Universe Attribute-Based Encryption (LU-ABE). In general, an ABE system can be classified to "small universe" and "large universe" constructions. In the "small universe" construction, the attributes are fixed at system setup and the size of the attributes is polynomially bounded and furthermore the size of public parameters grows linearly with the number of attributes. While in the "large universe" construction, the attributes need not be specified at system setup and the size of the attribute universe is unbounded. The "large universe" construction for ABE system brings an obvious advantage that the designer of the ABE system need not bother to choose a particular bound of the attributes at system setup.

Several CP-ABE systems supporting traceability have been proposed. In CP-ABE, each user possesses a set of attributes and can decrypt the ciphertext if his/her attributes satisfy the ciphertext's

access policy. This results in an obvious consequence that the encryptor or system does not know who leaks the decryption key to others intentionally. Due to the fact that the attributes are shared by multiple users and different users may have the same subset of attributes, the encryptor or system has no feasible method to trace the suspicious receiver if the decryption key is leaked. We take Alice (with attributes {Alice, Assistant Professor, Computer Science}) and Bob (with attributes {Bob, Assistant Professor, Computer Science}) as an example. They both have the same decryption keys corresponding to attributes {Assistant Professor, Computer Science} and can decrypt such a ciphertext encrypted by the attributes {Assistant Professor, Computer Science}. Suppose no other receiver in the system has both attributes ({Assistant Professor} and {Computer Science}) at the same time. If it happens to exist a user who can decrypt the ciphertext except Alice and Bob, it is significant to find out who leaks such decryption key to him, Alice or Bob? This drawback should be fixed in practice in case of leaking decryption key. It is necessary to add the property of traceability to the original ABE scheme, to identify who exactly leaks the decryption key. The above traceability is called white-box traceability, which means that any user who leaks his/her decryption key to the third user or device intentionally or unintentionally will be identified. Also note that there exists a relatively stronger notion named black-box traceability: the leakage of the user is the decryption equipment instead of its decryption key.

Up to now, there exists no practical traceable CP-ABE system supporting the property of large universe as the CP-ABE system. Large universe CP-ABE system with white-box traceability is not yet achieved in practice: (1) The CP-ABE systems supporting traceability proposed do not support the property of large universe, the attributes need to be fixed at system setup and the size of the attributes is polynomially bounded. Besides, public parameters' size grows linearly with the number of attributes. (2) The large universe CP-ABE system proposed is the first large universe CP-ABE system secure in the standard model; it does not support the property of traceability.

A Motivating Story: Consider a commercial application such as a pay-TV system with huge number of users for example. Each user is labeled with lots of related attributes, which are defined as TV channels that the user has ordered. As a versatile one-to-many encryption mechanism, CP-ABE system is quite suitable in this scenario. The pay-TV system provides several TV channels for users and those who have paid for the TV channels could satisfy the access policy to decrypt the ciphertext and enjoy the ordered TV channels. CP-ABE enables fine-grained access control to the encrypted data according to attributes in users' ordered lists. There are two problems with this approach. First, if someone illegally buys the decryption key from the Internet at a lower cost, she/he could also get access to the TV channels. It is necessary to find out who is selling the decryption key. Second, as the TV channels of the pay-TV system expand, an increasing number of new attributes need to be added to the system to describe the new channels. If the number of the attributes exceeds the bound set during the initial deployment of the pay-TV system, then the entire system has to be re-deployed and possibly all its data will have to be re-encrypted, which would be a disaster to the pay-TV in the commercial applications.

The problems, as described above, are the main obstacles when CP-ABE is implemented in commercial applications such as pay-TV systems and social networks. Due to the nature of CP-ABE, if a malicious user leaks its decryption key to others for profits, it is difficult to find out the original key owner from an exposed key since the decryption key is shared by multiple users who have the same attributes. As such, the pay-TV company will suffer severe financial loss. Thus, it is necessary for the pay-TV system to trace the malicious users who intentionally leak the partial or modified decryption keys. Also, as the pay-TV system expands, an increasing new attributes have to be added into the system. In previous CP-ABE constructions, the attributes are fixed at system setup and the number of the attributes is bounded. If the bound is not specified large enough, the attributes may exhaust if the number of the users exceeds the threshold and the entire system needs to be completely re-built. If the bound is specified

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

too large, it will increase the storage and communication burden of the entire system due to the corresponding increase of the public parameters' size. Thus, it is necessary for the pay-TV system to support flexible number of attributes. Lastly, since the number of users in a pay-TV system could grow fast, the storage for traceability should not increase linearly with the number of users. The storage for traceability will become relatively huge and exhaust if the users increase dramatically. Thus, the storage cost for traceability needs to be at a constant level in an ideal case.

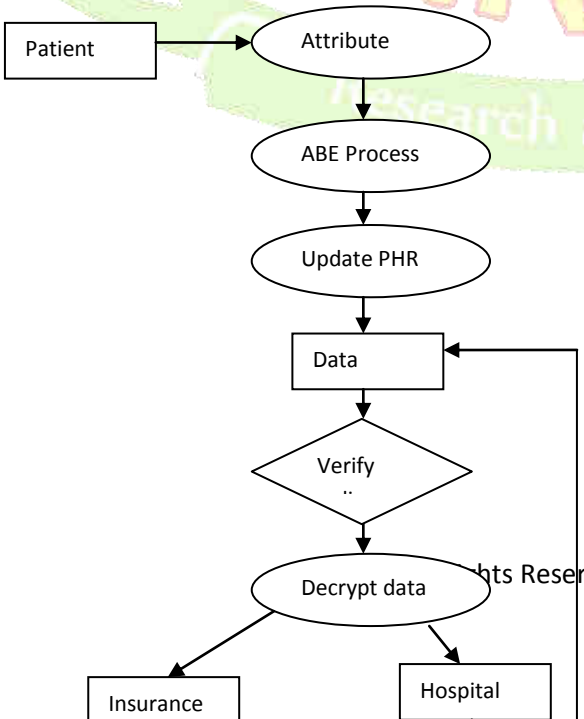
4. Problem Statement

Single owner based encryption model uses only one key value for the encryption process. In multiple owner model the data values are encrypted with multiple key values. The Central Authority (CA) handles the key management for all users. User-centric, secure sharing model is designed for semi-trusted server environment. Attribute-based Encryption (ABE) model is adopted to encrypt user data values. A users has the rights to selectively share their data among a set of users by encrypting the file under a set of attributes. Ciphertext-policy attribute-based encryption (CP-ABE) enables fine-grained access control to the encrypted data for commercial applications. CP-ABE has two properties called traceability and large universe. Traceability is the ability of ABE to trace the malicious users. Large universe property in ABE enlarges the practical applications by supporting flexible number of attributes. Large Universe Attribute-Based Encryption (LU-ABE) increases the attributes in the data sharing process. Traceable and large universe properties are integrated in the T-LU-ABE. The following problems are identified from the current security methods.

- User identity based access control mechanism is not supported
- Dynamic policy management model is not provided
- Attribute based encryption is tuned for single server environment
- Complex key distribution process

5. Data Leakage Control Mechanism for CPABE

The PHR security system is adapted to policy based and identity based security systems. The distributed ABE model is adopted to support multiple server frameworks. The data owners can change the access policies dynamically. The system reduces the key management and revocation complexity. The system is designed to manage patient health records under data centers. Multi party based data ownership and access mechanism is used in the system. Different key values are used to secure different attributes. The system is divided into six major modules. They are data owner, data provider, key management, security process, authority analysis and client.



ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Figure No: 5.2. Data Leakage Control Mechanism for CPABE

The data owner module is designed to handle data update process. The data provider module is designed to store and maintain the patient health records. The key management module is designed to handle the key update and distribution process. The security process module is designed to perform the attribute based encryption process. The authority analysis module is designed to verify the data access. The client module is designed to perform the data retrieval process.

5.1. Data Owner

The data owner module is designed to maintain the patient details. The attribute selection model is used to select sensitive attributes. Patient Health Records (PHR) is maintained with different attribute collections. Data owner assigns access permissions to various authorities.

5.2. Data Provider

The data provider module is used to store the PHR values. The PHR values are stored in databases. Data owner uploads the encrypted PHR to the data providers. User access information's are also maintained under the data provider.

5.3. Key Management

The key management module is designed to manage key values for different authorities. Key values are uploaded by the data owners. Key management process includes key insert and key revocation tasks. Dynamic policy based key management scheme is used in the system.

5.4. Security Process

The security process handles the Attribute Based Encryption operations. Different encryption tasks are carried out for each authority. Attribute groups are used to allow role based access. Data decryption is performed under the user environment.

5.5. Authority Analysis

Authority analysis module is designed to verify the users with their roles. Authority permissions are initiated by the data owners. Authority based key values are issued by the key management server. The key and associated attributes are provided by the central authority.

5.6. Client

The client module is used to access the patients. Personal and professional access models are used in the system. Access category is used to provide different attributes. The client access log maintains the user request information for auditing process

6. Conclusion

The patient health records are maintained in a data server. Public and personal access models are designed with security and privacy enabled mechanism. The attribute-based encryption model is enhanced to support distributed ABE operations. The system is improved to support dynamic policy

management model. Patient health records are maintained with security and privacy. User choice based security model is constructed with multiple data access authority support. Central key management model supports data owners and users.

References

[1] J. Herranz, F. Laguillaumie and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," in Proc. Public Key Cryptography (PKC), 2010, pp. 19-34.
[2] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Proc. Adv. Cryptology (EUROCRYPT), vol. 4965, 2008.
[3] S. Roy and M. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Tech. Rep., 2009.
[4] Z. Zhou and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption," in Proc. 17th ACM Conf. Comput. Commun. Security, 2010, pp. 753-755.
[5] K. Emura, A. Miyaji, K. Omote and M. Soshi, "A ciphertext policy attribute-based encryption scheme with constant ciphertext length," in Proc. 5th Int. Conf. Inf. Security Practice Experience. Springer-Verlag, 2009..
[6] Zhibin Zhou, Dijiang Huang and Zhijie Wang, "Efficient Privacy-Preserving Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption", IEEE Transactions On Computers, Vol. 64, No. 1, January 2015
[7] S. Yu, K. Ren, and W. Lou, "Attribute-based on-demand multicast group setup with membership anonymity," Comput. Netw., vol. 54, no. 3, pp. 377-386, 2010.
[8] D. Lubicz and T. Sirvent, "Attribute-based broadcast encryption scheme made efficient," in Proc. 1st Int. Conf. Cryptology Africa (AFRICACRYPT). Springer, 2008, pp. 325-342.
[9] L. Cheung, J. Cooley and C. Newport, "Collusionresistant group key management using attribute-based encryption," in Proc. 1st Int. Workshop Group-Oriented Cryptographic Protocols, 2007.