ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Improving Security and Efficiency in Distributed Data Sharing and Data Leakage Detection System

A.Rani
Shadan Engineering College, India
rani.smily123@gmail.com

Abstract

Many data hiding techniques have recently been analyzed as they could help to manage part of the security rights. The randomization is expected to increase the security of the system and also increase the capacity. One of the most challenging issues in data sharing systems is the enforcement of access policies and the support of policies updates. Cipher text policy attribute-based encryption (CPABE) is becoming a promising cryptographic solution to this issue. Among the general framework of data hiding, key generation plays an vital role with trusted key generation center in order to select keys and transport those keys to all communication entities secretly. In key generation the major drawback which is called as the key escrow problem and in my proposed system it is overcome by Free key issuing protocol which is constructed using the secure two-party computation between the key generation center and the data storing center. The confidentiality of this transformation in data will be theoretically secured by providing authentication for transferring keys which are being generated. In my proposed system by applying encryption in the data sharing system introduces another challenge with regard to the user revocation, since the access policies are defined only over the attribute universe. The efficiency and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.

Keywords: Key escrow protocol, revocation, CP-ABE, KP-ABE, Data sharing, attribute-based encryption, access control.

Introduction

Development of the network and computing technology enables many people to easily share their data with others uses online external storages. People can share their lives with friends by uploading their private photos or messages into the online social networks such as Face book and MySpace; or upload highly sensitive personal health records (PHRs) into online data servers such as Microsoft Health Vault, Google Health for ease of sharing with their primary doctors or for cost saving. As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. The original solution by Chase employs a trusted central authority and the use of a global identifier for each user, which means the confidentiality, depends critically on the security of the central authority and the user-privacy depends on the honest behavior of the attribute-authorities. The proposed attribute-based encryption scheme with the trusted authority and the anonymous key issuing protocol works for the existing schemes and for the new construction. In particular, no group of users should be able to combine their keys in such a way that they can decrypt a cipher text that none of them alone could. The primary technique is that to construct a user's private key as a set of private key components, one for each attribute in the user's identifier.

Attribute based Encryption

ABE comes in two flavors called key-policy ABE (KPABE) and cipher text-policy ABE(CP-ABE)(fig(C)).In KPABE, attributes are used to describe the encrypted data and policies are built into users' keys; while in CP-ABE, the attributes are used to describe users' credentials, and an encrypt or that determines a policy on who can decrypt the data. Between the two approaches, CP-ABE is more appropriate to the data sharing system because it puts the access policy decisions in the hands of the data owners.

Generating Key

For the given password, hashing technique is applied to generate the Key. Here in my thesis work for

ISSN: 2277-9655
Impact Factor: 1.852

hashing technique, to generate the key SHA1 algorithm is used.

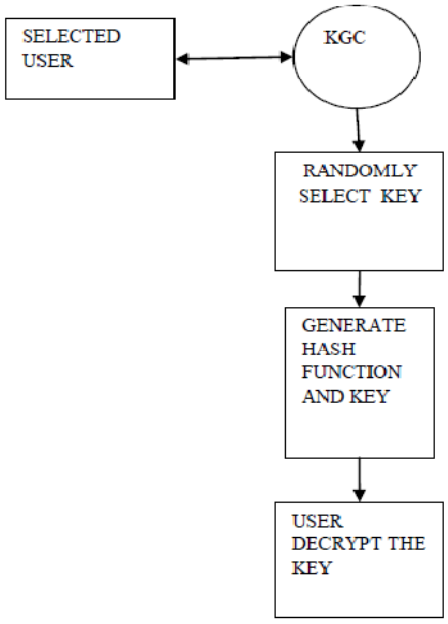

Fig 1.0 Generating key by KGC.

A.Hash Function

A hash function H is a transformation that takes a variable size input m and returns a fixed-size string, which is called the hash value h (that is, h = H(m)). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties. The basic requirements for a cryptographic hash function are: the input can be of any length and the output has a fixed length. H(x) is relatively easy to compute for any given x also H(x) is one-way and H(x) is collision-free. SHA-1 is a cryptographic message digest algorithm. SHA1, also known as SHA160, is a hash algorithm. SHA-1 is commonly used to verify the integrity of software archives, as a unique identifier, and for digital signatures. The SHA takes a message of less than 264bits in length. It is based on design with a few key differences.

Remove Key Escrow in ABE

Key escrow is an inherent property in the current proposed attribute based encryption. In this paper, a scheme which Removes the key escrow and maintaining some important properties of the ABE [3][4][5]. Also some cryptosystems are introduced based on variant including an authenticated key agreement (fig.1).The KGC and the data storing center are involved in the user key issuing protocol. In the protocol, a user is required to contact the two parties before getting a set of keys. The key generation center is responsible for authenticating a user and issuing attribute keys to him if the user is entitled to the attributes.

A Escrow-Free Key Issuing Protocol for CP-ABE The KGC and the data storing center are involved in the user key issuing protocol. In the protocol, a user is required to contact the two parties before getting a set of keys. The KGC is responsible for authenticating a user and issuing attribute keys to him if the user is entitled to the attributes. The secret key is generated through the secure 2PC protocol between the KGC and the data storing center. They engage in the arithmetic secure 2PC protocol with master secret keys and issue independent key components to a user. Then, the user is able to generate the whole secret keys with the key components separately received from the two authorities. The secure 2PC protocol deters them from knowing each other's master secrets so that none of them can generate the whole secret keys of a user alone. The data storing center probabilistically outputs the public and private key pair. The KGC and the data storing center are involved in the key generation protocol. The value is personalized and unique secret to the user, which should be consistent for any further attribute additions to the user. Then, the KGC and the data storing center engage in a secure 2PC protocol. When one member is compromised, the group can still continue with its secure communication by excluding the compromised member. The final property is the dynamic compromised property, which means the group key agreement scheme property, retains both accuracy and efficiency even if the group key retains agreement scheme involves dynamic membership events, agreement confidentiality, meaning that the communication data among a group of authorized members are secure and inaccessible to group outsiders. To offer data privacy, an effective approach is to require all group members to establish a common secret group key, which is held only by group members, but not outsiders, for encrypting the transmitted data.

Proposed CP-ABE Scheme

Since the first CP-ABE scheme proposed by Bettencourt et al. [5], dozens of the subsequent CP-ABE schemes have been suggested which are mostly motivated by more rigorous security proof in the standard model. However, most of the schemes failed to achieve the expressiveness of the Bettencourt et al.'s scheme, which described an efficient system that was expressive in that it allowed an encryptor to express an access predicate in terms of any monotonic Formula over attributes. Therefore, in this section, we develop a variation of the CP-ABE algorithm partially based on (but not limited to) Bethencourt et al.'s construction in order to enhance the expressiveness of the access control

ISSN: 2277-9655
Impact Factor: 1.852

policy instead of building a new CP-ABE scheme from scratch. Its key generation procedure is modified for our purpose of removing escrow. The proposed scheme is then built on this new CP-ABE variation by further integrating it into the proxy re-encryption protocol for the user revocation. To handle the fine-grained user revocation, the data storing center must obtain the user access (or revocation) list for each attribute group, since otherwise revocation cannot take effect after all. This setting where the data storing center knows the revocation list does not violate the security requirements, because it is only allowed to re-encrypt the cipher texts and can by no means obtain any information about the attribute keys of users. Since the proposed scheme is built on [5], we recapitulate some definitions in [5] to describe our construction in this section, such as access tree, encrypt, and decrypt algorithm definitions.

Encrypting Data

By encrypting the message (M) using AES algorithm, will produce Enc (M, K). In this implementation work the key K can be generated from a set of user passwords each with a specific key using simple XOR. This will add more security especially when it is necessarily to make the secret message available only if all the users present their passwords. AES is an iterated block cipher with a fixed block size of 128 and a variable key length. The different transformations operate on the intermediate results, called state. The state is a rectangular array of bytes and since the block size is 128 bits, which is 16 bytes, the rectangular array is of dimensions 4x4. The cipher key is similarly pictured as a rectangular array with four rows. The number of columns of the cipher key, is equal to the key length divided by 32.It is very important to know that the cipher input bytes are mapped onto the state bytes in the order a0,0, a1,0, a2,0, a3,0, a0,1, a1,1, a2,1, a3,1 ... and the bytes of the cipher key are mapped onto the array in the order k0,0, k1,0, k2,0, k3,0, k0,1, k1,1, k2,1, k3,1 ... At the end of the cipher operation, the cipher output is extracted from the state by taking the state bytes in the same order. AES uses a variable number of rounds, which are fixed: A key of size 128 has 10 rounds. A key of size 192 has 12 rounds. A key of size 256 has 14 rounds. During each round, the following operations are applied on the state:

1. Sub Bytes: every byte in the state is replaced by another one, using the Rijndael S-Box
2. Shift Row: every row in the 4x4 array is shifted a certain amount to the left
3. Mix Column: a linear transformation on the columns of the state
4. AddRoundKey: each byte of the state is combined with a round key, which is a different key for each round.

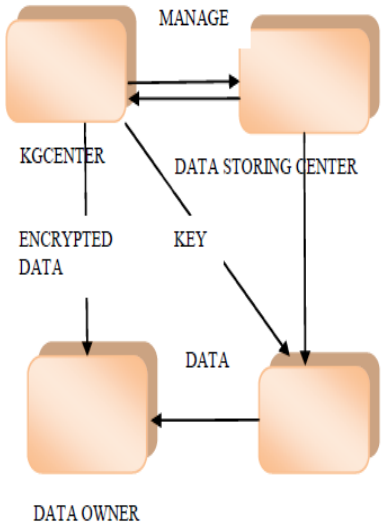

Fig 5.1 architecture of data sharing system

Scheme Analysis

In this section, we analyze and compare the efficiency of the proposed scheme with the previous CP-ABE schemes (that is, Bethencourt et al.'s scheme (BSW) [5], Attrapadung's scheme (BCP-ABE2) [9], and Yu et al.'s scheme (YWRL)) in theoretical and practical aspects. Then, the efficiency of the proposed scheme is demonstrated in the network simulation in terms of the communication cost. We also discuss its efficiency when implemented with specific parameters and compare these results with those obtained by the other schemes.

Conclusion

In our scheme the secure key exchange system overcome the security problem. It provides more security by giving the session keys and secret keys [1][2][3].The proposed scheme features a key issuing mechanism that removes key escrow during the key generation. The user secret keys are generated through a secure two-party computation such that any curious key generation center or data storing center cannot derive the private keys individually[5][6]. Thus, the proposed scheme enhances data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding credentials. The proposed scheme can do an immediate user revocation on each attribute set while taking full advantage of the scalable access control Provided by the cipher text policy attribute based encryption. Therefore, the proposed scheme achieves more secure in the data sharing system.

ISSN: 2277-9655
Impact Factor: 1.852

References

[1] Junbeom Hur," Improving Security and Efficiency in Attribute-Based Data Sharing"IEEE transactions on knowledge and data engineering, 2010 IEEE.
[2] G.Balaia, Dr.V.SrinivasaRao,"A Protocol for Authenticated Group Key Transfer Protocol Based on Secret Sharing" International journal of advanced engineering science and technology, Vol No: 8, Issue No.2, 256-260.
[3] J.Bethencourt,A.Sahai, B.Waters,"Cipher text-Policy Attribute-Based Encryption," Proc. IEEE Symposium on Security and Privacy 2007, pp. 321–334, 2007.
[4] C.Blundo, A.DeSantis, A.Herzberg, S.Kutten, "Perfectly Secure Key Distribution for Dynamic Conferences", Information and computation, vol.146, pp1-23, oct.1998.
[5] A. Lewko, A. Sahai, B. Waters, "Revocation Systems with VerySmall Private Keys,"Proc. IEEE Symposium on Security andPrivacy 2010, pp. 273–285, 2010.
[6] S. Yu, C. Wang, K. Ren, W. Lou, "Attribute Based Data Sharingwith Attribute Revocation,"Proc. ASIACCS '10, 2010.
[7] X. Liang, Z. Cao, H. Lin, D. Xing, "Provably Secure and EfficientBounded Ciphertext Policy Attribute Based Encryption,"Proc. ASIACCS, pp. 343–352, 2009.
[8] S.S.M. Chow, "Removing Escrow from Identity-Based Encryption,"Proc. PKC 2009, LNCS 5443, Pp.256–276,2009.