Survey Of Management Of PHR By Secure Cipher Text Policy Attribute Based Encryption Scheme

Abel Joy, Akhila H, Annie Chacko

Abstract: The PHR enables patients to manage their medical records in a centralized way which greatly facilitate the storage, access and sharing of personal health data. These details are locked by a central server in the hospital. But the security over the data is loosed while the data is sent to a requester. In this paper, we describe a new scheme for the secure data handling. The CP-ABE scheme is used for this purpose. In this scheme each user's private key is associated with set of attribute representing these capabilities and an encrypted cipher text such that only users whose attribute satisfy a certain policy can decrypt.

Index Terms: Cipher text Policy Attribute Based Encryption, Identity Based Encryption, Public Key Infrastructure,Personal Health Record Trusted Third Part

1 INTRODUCTION

There are number of access control mechanisms are available to outsourcing data to a third party. But the traditional encryption techniques are not suitable to be used in this scenario. Because the security over the data is loosed when the data is sent to a requester. So this can be overcome by using the technique CP-ABE. This paper presents a new approach for secure management of personal health records which are stored and shared from an un-trusted web server. The CP-ABE scheme has shown to be more useful in a healthcare setting since the access policy is enforced by virtually associating the access control policy to the protected data. This removes the need for involving a trusted entity which has to enforce access policies. The proposed scheme allows patients to encrypt the data according to an access policy over a set of attributes issued by two trusted authorities. The scheme does not require the presence of a central authority to coordinate the work of the trusted authorities. A possible future work is to formally provide a security proof for the proposed scheme.

2. SURVEY

2.1. ATTRIBUTE BASED ENCRYPTION

Traditionally, this type of expressive access control is enforced by employing a trusted server to store data locally. The server is entrusted as a reference monitor that checks that a user presents proper certification before allowing him to access records or files. However, services are increasingly storing data in a distributed fashion across many servers. Replicating data across several locations has advantages in both performance and reliability. The main disadvantage of this scheme is regarding the security; when data is stored at different and several locations, the chances that one of them has been compromised increases dramatically. For these reasons we would like to require that sensitive data is stored in an encrypted form so that it will remain private even if a server is compromised. Most existing public key encryption methods allow a party to encrypt data, but are unable to efficiently handle more expressive types of encrypted access control. In our system, a user's private key will be associated with number of attributes expressed as strings. On the other hand, when a user encrypts a message in our system, they specify an associated access structure over attributes. A user will only be able to decrypt a cipher text if that user's attributes pass through the cipher text's access structure. At a mathematical level, access structures in our system are described by a monotonic "access tree", where nodes of the access structure are composed of threshold gates and the leaves describe attributes. In the work of, collusion resistance is insured by using a secret-sharing scheme and embedding independently chosen secret shares into each private key. Because of the independence used in each invocation of the secret sharing scheme, collusion-resistance follows. In our scenario, users' private keys are associated with sets of attributes instead of access structures over them, and so secret sharing schemes do not apply. Instead, we devise a novel private key randomization technique that uses a new two-level random masking methodology. This methodology makes use of groups with efficiently computable bilinear maps, and it is the key to our security proof, which we give in the generic bilinear group model.

2.2 PUBIC-KEY CRYPTOGRAPHY

It is an asymmetric scheme that uses a pair of keys for encryption - a private key which is kept secret and a public key which is widely distributed. In a Public-Key Infrastructure (PKI), a public key must be obtained from, or the Trusted Third Party

- *Abel Joy is currently pursuing BTech Degree in Computer Science and engineering in Mahathma Gandhi university kottayam,India,PH-9895219874*
  E-mail: abeljoydasan@gmail.com
- *Akhila H is currently pursuing BTech Degree in Computer Science and engineering in Mahathma Gandhi university kottayam, India, PH-9961285288.*
  E-mail: akhilah81@yahoo.in
- *Annie Chacko currently working as assistant professor in Computer Science and Engineering department in MBCCET,Peermede,Idukki,PH-,9497791233*
  E-mail: nnievargh@gmail.com

(TTP) of the PKI. In Identity-Based Encryption (IBE) any string can be used to generate a public key without involvement of the TTP thus creates a degree of flexibility that a PKI cannot offer. Public-Key encryption is a most powerful mechanism for protecting the confidentiality of both stored and transmitted information. Traditionally, encryption is used for a user to share data to another user or any device.But in this method the sender knows the credentials of the receiver. In particular, they proposed two complementary forms of ABE. In the first, Key-Policy ABE, attributes are used to interpret the cipher texts and formulas over these attributes are credited to users' secret keys. The second type, Ciphertext-Policy ABE uses attributes to describe user's credentials and this is used by the encryptor for cipher text.

2.3CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION WITH REVOCATION

Revocation is a vital open problem in almost every cryptosystem dealing with malicious behaviors. In cipher text policy attribute based encryption, different users may hold the same functional secret keys related with the same attribute set leading to additional difficulties in designing revocation mechanism. This scheme uses linear secret sharing and binary tree techniques as the underlying tools. Along with the attribute sets each user is also assigned with a unique identifier so, the user can be easily access the data or information very easily. . There are some difficulties occurred in this scheme while considering the following conditions:-first, problem occurs while associating user secret keys with different sets of attributes instead of individual characteristics; second, users' individuality are taken place by several common attributes, and thus revocation on attributes or attribute sets cannot accurately exclude the users with misbehaviors; third, the system must be secure against collusion attack from revoked users even though they share some common attributes with non-revoked users.

2.4CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION ON BOUNDED SIZE

This Cipher text Policy Attribute Based Encryption scheme mainly based on number of theoretic assumptions and supporting advanced access structures. The earlier schemes support only the limited access structures. But in this scheme the access structures are represented by a bounded size access tree with threshold gates as its nodes. The size of the access tree is chosen at time of system setup and the security is handled by standard Decisional Bilinear Diffie-Hellman assumption. The main condition is that any access tree satisfying the upper bounds on the size can be dynamically chosen by the encryptor. In this technique we introduce many copies of each attribute for every position in the access structure tree where it can occur. This set of programs includes four command line tools performing various operations:

- Setup-which generates public parameter and a master key given a security parameter and access bound.
- Key generation-which takes as input a set of attributes and outputs a decryption key.
- Encrypt-which takes as input a plain text and a bounded access policy, and generate the corresponding ciphertext.
- Decrypt- the input is ciphertext produce the plaintext by using key. The plaintext is correct if and only if the attributes satisfies the access policy.

3. FIELD OF APPLICATIONS

The public key encryption method was the most traditional method applied to the PHR for the security of the data. But it made the high key-management problems and also this method was very less scalable. The user revocation or break glass access and other advanced techniques were not possible with these one-to-one. The attributes can define an object very efficiently just as the identity of an object works. The attribute based encryption provides the security to the database. In this system both the cipher text and secret key will be associated with the attributes. The user who is having a minimum number of attributes only can decrypt the data. So while applying this method the owner doesn't want to know about the entire list of users instead of that they can encrypt the data according to some attributes only. Using ABE, access policies expressed based on the attributes of user data which enable the patient to selectively share the PHR among a set of users by encrypting the file under a set of attributes, and so the owner don't want to know the complete list of users.It provides data confidentiality and write access control. But the on-demand user revocation and other techniques were not adaptable with this encryption method. In the revocation technique we use a unique identifier. By using the ciphertext policy attribute based encryption with revocation scheme in which malicious users can be efficiently revoked. This technique uses a linear secret sharing scheme and binary tree techniques. In CP-ABE model, each user is assigned with a unique identifier, this identifier can be later re-randomized, and it does not change. The bounded CP-ABE is based on a standard number theoretic assumption and supporting advanced access structures. In which uses a bounded size access tree with threshold gates as node. The bound depends on the depth, d of the access tree and maximum number of children in each non leaf node, num. The encryptor uses the access tree that satisfies the tuple (d, num). The Decisional Bilinear Diffie-Hellmann assumption support non-monotonic access policies. In this scheme uses a fixed "universal" tree access structure as CP-ABE scheme. In which each attribute is associated with number of copies and causes a significant increase in private key size, but it does not affect the ciphertext size. The encryption and decryption use these feature.

4. CONCLUSION

We created a system for Cipher text-Policy Attribute Based Encryption. Our system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. Our system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. Finally, we provided an implementation of our system, which included several optimization techniques.

ACKNOWLEDGMENTS

We would like to thanks all the reference authors for the completion of this paper.

REFERENCES

[1]. Amit Sahai UCLA CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION, John Bethencourt Carnegie Mellon University,Brent Waters, SRI International.

[2]. Luan Ibraimi, Qiang Tang, Pieter Hartel, Willem Jonker,EFFICIENT AND PROVABLE SECURE CIPHER TEXT-POLICY ATTRIBUTE-BASED ENCRYPTION SCHEMES, Faculty of EWI, University of Twente, the Netherlands, Philips Research, the Netherla

[3]. Xiaohui Liang, Rongxing Lu, Xiaodong Lin, and Xuemin (Sherman) Shen, CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION WITH POLICY ATTRIBUTE BASED ENCRYPTION WITH EFFICIENT REVOCATION, Department of Electrical and Computer Engineering, University of Waterloo,Canada Faculty of Business and Information Technology, University of Ontario Institute of Technology, Canada

[4]. Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai, BOUNDED CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION, Department of Computer Science,UCLA