ACCESS POLICY BASED PATIENT INFORMATION EXCHANGE PROTOCOL

PHR
Anugrah CP
MCA
Information Security Management Systems
Jain University Bangalore, India

Abstract: **We consider the problem of patient self-controlled access privilege to highly sensitive Personal Health Information (PHI), where PHI is expected to be securely stored in cloud storage for uninterrupted anytime, anywhere remote access. In order to assure the privacy of PHI, we propose Efficient and Secure Patient-centric Access Control (ESPAC) scheme which allows data requesters to have different access privileges based on their roles, and then assigns different attribute sets to them. Extensive security and performance analyses demonstrate that the ESPAC scheme is able to achieve desired security requirements with acceptable communication delay outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytically and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.**

I. Introduction

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing PHRs in cloud computing have been proposed.

While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates. Cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization. To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers.

A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the PHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary.

2.Scope of the Product

Enhanced PHR is a web-based application developed in MVC three tier architecture. The technology used in this system is J2EE which as My-SQL as back-end database. This system is developed with cloud computing technology. Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network.

Cloud computing entrusts remote services with a user's data, software and computation. End users access cloud-based applications through a web browser on a light- weight desktop while the ENHANCED PHR software and user's data are stored on servers at a remote location. In this system there are three type of end user Admin, Data Owner & Data Consumer.

3. Related works

Existing research works related to proposed ESPAC includes

- secure and privacy preserving eHealth care system
- Attribute-Based Encryption
- Access control over untrusted cloud storage.

Hybrid security policy for WBANs with Quality of Services (QoS) have recently been proposed for secure eHealth care system in Barua et al. (2011). Public key cryptography is used for session key management and private key cryptography is used for regular data encryption in WBANs environment. Due to the nature of the real-time traffic, emergency health application traffic is given high priority compare to other applications traffic. Lu et al. (2010) propose a mobile health care social network, where two patients can communicate each other if they have the same symptoms. Performance analyses demonstrate that emergency response time can be minimized by using proposed mobile health care social network. Lin et al. (2009) present a privacy preserving scheme for health care that can effectively works against global adversary. Both content and contextual privacy can be achieved by the proposed work.

Attribute-Based Encryption (ABE), a novel extension from identity based encryption by enabling expressive access policy to control the decryption process is first presented in Sahai and Waters (2005). Key Policy Attribute-based Encryption (KP-ABE) and Cipher text Policy Attribute-based Encryption (CP-ABE) are the two main variants of ABE proposed so far. In both cases, user has a set of attributes that associate with user’s private key. The attribute set is used to describe a user’s credentials. In KP-ABE, user’s private key is embedded with an access policy, whereas cipher text is encrypted by a pre-defined access policy in CP-ABE (Goyal et al., 2006; Bethencourt et al., 2007). Liang et al. (2010) present a patient self-controllable access policy so that patients would have the primary control of the access to their own PHI.

Health records sharing and integrating in health care cloud is discussed in Zhang and Liu (2010). The paper describes the security reference model for managing different security issues in health care clouds. Yu et al. (2010) propose a fine gained data access control in cloud computing based on KP-ABE. Confidentiality of user access privilege and user secret key accountability can be achieved by the work. A mandatory access control model to protect patient’s metadata with privacy is presented in Luna et al. (2010). It is shown that the use of fragmentation after encryption greatly improves overall security because potential attackers need to compromise more data file to gain access. Without disclosing the data contents, data owner delegates most of the computation tasks involved in fine-grained data access control to untrusted cloud server by combining techniques of ABE, proxy re-encryption, and lazy re-encryption. An efficient cloud storage sharing scheme is presented in Liu et al. (2010). The scheme works on hierarchical identity based encryption, where intended recipients can share the file by using their private keys. Wang et al. (2010) combine hierarchical identity-based encryption and CP-ABE to achieve fine-grained access control in cloud storage services.

4. System model and security requirements

In this section, define the system model and then describe the security requirements of the proposed ESPAC scheme.

4.1 System model

In this system model, define the following entities:

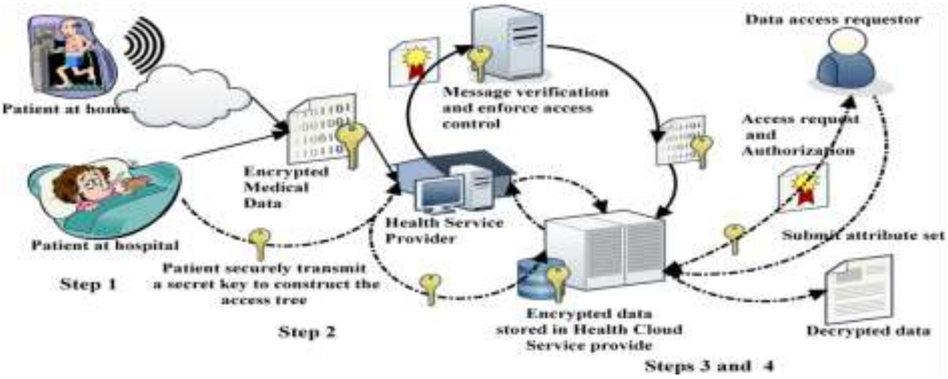
- Trusted Authority (TA): It generates the public and secret key parameters for the ESPAC. The trusted authority is responsible for attributes’ keys issuing, revoking, and updating. It grants differential access rights to individual users based on their attributes and roles. Trusted authority also maintains an index-table, where it stores the location of distributed data storage server. Authorized health service providers (e.g., Hospital, urgent care) are denoted as trusted parties.

- Cloud service provider: It provides data outsourcing services and consists of data servers and data service manager. The main responsibility of the data storage server is to serve and retrieve data according to authorized users’ request. Data service manager negotiates with health care service provider to control the access from outside users to the stored encrypted data.

- Registered user: Patient who is registered to the trusted authority is considered as registered user. A registered user is responsible for defining attribute-based access policy and encrypting the sensitive PHI under the predefined policy before storing at the cloud-storage.

- Data-access requester: Cloud users who request to access some specific PHI are called the data-access requester. The ESPAC scheme ensures that any data-access requester can only decrypts the encrypted data if and only if he can successfully complete the access-policy.

The encrypted data is stored in a centralized storage, health-cloud, for future access. Based on the major operations, the proposed scheme can be classified into four major steps, as shown in Figure 1.


Data access requestor
Patient at home
Message verification and enforce access control
Access request and Authorization
Encrypted Medical Data
Health Service Provider
Patient at hospital
Submit attribute set
Patient securely transmit a secret key to construct the access tree
Step 1
Step 2
Encrypted data stored in Health Cloud Service provide
Decrypted data
Steps 3 and 4

Step 1 (PHI collection): In this initial step, using different body sensors, PHI is sensed and ready to be transmitted to the trusted eHealth care service provider.

Step 2 (Secure data communication): In this step, public key cryptography is used to securely transfer collected PHI to the eHealth care service provider. Patient securely transfer a secret key to the trusted eHealth care provider, if he authorized the service provider to build-up the access tree.

Step 3 (PHI processing at eHealth care provider): After receiving the PHI securely, eHealth care service provider classifies the PHI based on the attributes set chosen by the patient. It then makes different privacy levels of data requesters based on their roles (e.g., level-1: general users, level-2: pharmacist, level-3: doctors, etc.) and assigns different set of attributes to these different levels.

Step 4 (Transfer PHI to the cloud storage and control access): After the data classification, encrypted data securely transfers to the cloud storage, shows as ‘Health Cloud’ in Figure 1. EHealth care service providers may operate either real-time or periodically based on the existing infrastructures. Data-access requester sends request to the cloud storage with a data block identity. They may also request for the corresponding attribute sets.

5 .Security requirements

Aim at achieving the following security objectives.

1 Patient-centric access control: The system should provide patient-centric access control, where a patient can decide who can get the access to his or her stored PHI.

2 Message integrity, source authentication and non-repudiation: All accepted messages should be delivered unaltered, and the origin of the messages should be authenticated by the eHealth care service provider. To ensure the non-repudiation, the patient cannot refute the validity of a PHI afterward.

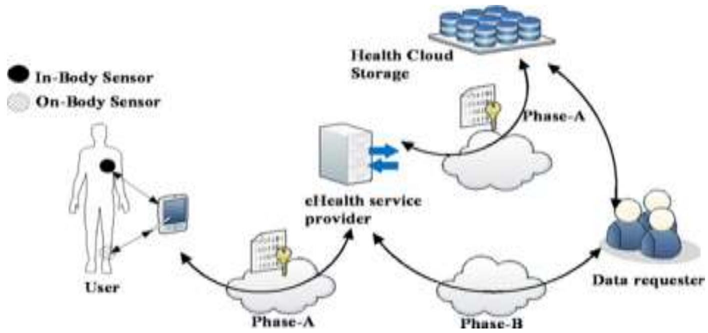
3 Prevention of Cipher text-only attack: The system should be secured enough to prevent recover of the plaintext from a set of stored cipher texts.

4 Provide patient privacy: Privacy is one of the important concerns from a patient perspective. Illegal disclosure and improper use of patient PHI can cause legal disputes and undesirable damaging in patient’s personal life.

5 Resistant to collusion attack: If multiple users collude, generally they may be able to decrypt a cipher text by combining their attributes. Users can not get any access to the encrypted data even by sharing information in a group.

6 Resistant to Denial-of-Service (DoS) attack: The DoS attack may be caused due to the large groups of legitimate users access the eHealth care service provider at the same time, or the attacker continuously launch false traffic with a High Data Rate (HDR). The system should ensure acceptable QoS level to resist the DoS attack.

6. Proposed ESPAC scheme



Setup (1t): The Probabilistic Polynomial Time (PPT) setup algorithm takes as input a security parameter 1t. It outputs the public parameters P K and a master key M K which is known only to the private key generator.

Encrypt1(PKs, m, PKr): The encryption algorithm takes the public parameters of the sender and receiver and encrypt the message ‘m’ by doing mapping and XOR operations. We use Encrypt2(P K, M, A) function to encrypt the message M and store in the health cloud. This encryption algorithm takes the system public parameters PK, a message M, and an access structure A over the universe of health attributes. The encrypted cipher text CT can only be decrypted if and only if the user possesses the set of health attributes that satisfy the access tree structure.

Decrypt1(PK, C, d): The decryption algorithm take’s as input the public parameter PK, cipher text C, and the product of the receiver’s secret key and sender PK’s hash value. The health care provider uses this function to decrypt the encrypt message sent by the user for further processing. Another decryption function Decrypt2(P K, CT , SK) takes as input the public parameters PK, a cipher text CT, which contains the access policy A, and a secret key SK, which is a private key for a set S of health attributes. If the set S of attributes satisfies the access structure A, the algorithm will decrypt the cipher text and return the message M.

7. Security analysis

In this section, evaluate the security and privacy issues of the proposed scheme.

The ESPAC scheme ensures user and eHealth agent’s identity privacy: User and health agent use pseudo identity instead of their unique identity, and these pseudo identities are generated by a strong one-way hash function. The construction of the hash function is easy to sample and compute but hard to invert. Therefore, the privacy is ensured by the proposed scheme.

The scheme is secure to chosen cipher text-only attack: Data transmissions from user to health agent, as well as from health agent to health cloud service provider are done with proper encryption schemes (Encryption1 and Encryption2). The processes are indistinguishable under chosen cipher text attack based on the BDH problem hardness and this hardness ensures there is no PPT algorithm that can decrypt the message from a set of chosen cipher text.

The scheme is resistant to the eavesdropping and collusion attacks: An eavesdropping attacker aims at accessing the private and sensitive patient’s medical data. This attack may be happened during the patient to eHealth care provider or eHealth care provider to the health cloud data communication. The BDH hardness ensures that the proposed scheme is resistant to this eavesdropping attack. To access the data at the health cloud server, an attacker needs to have sufficient attributes to complete the access tree. Here the random number‘s’ is divide into multiple shares based on the attributes set. For the non-privacy dataset, he may get access and it’s allowed in our scheme. But he cannot modified the data due to the verification bindings. However, for the patient sensitive data, a unique random number is embedded into both ‘C’ and ‘D’ of the equation shown in the Decrypt2(CT , SK) function. Without knowing that secret number, it is impossible to access the data in a PPT. This hardness also demonstrates our scheme as a resistant to the collusion attack. Therefore, any attacker cannot successfully launch the eavesdropping or collusion attack to our proposed scheme.

The scheme ensures message integrity, non-repudiation, and source authentication: We use the patient’s secret key and the session identity to generate the signature ‘S’

ESPAC ensures backward and forward secrecy: The scheme prevents user to access the plaintext before providing the required attributes that satisfy the access policy. On the other hand, any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other attributes that he is holding satisfy the access policy. Thus, ESPAC ensures backwards and forward secrecy.

8. Conclusion

In this paper, the have proposed a scheme, ESPAC, to achieve patient-centric access control with security and privacy by exploiting attribute-based encryption. Moreover ESPAC enables the eHealth care service provider to reduce the overall maintaining cost by moving data to a centralized storage or cloud storage for further processing and long-term storage. Moreover, storing PHIs in the cloud storage provides anytime, anywhere access to stored patient's health information. The proposed scheme also preserves user privacy with data integrity. Through detailed security and performance analyses, it has been demonstrated that the proposed scheme is highly efficient to resist various possible attacks and malicious behavior. In our future work, we will extend the proposed scheme to support encrypted keyword search in cloud computing.

Acknowledgment

THIS RESEARCH IS PARTLY SUPPORTED BY DEPARTMENT OF COMPUTER SCIENCE & INFORMATION SECURITY OF JAIN UNIVERSITY JAYANAGAR, 9TH BLOCK, BENGALURU, KARNATAKA, INDIA.

References

I. Diffie, W., and Hellman, M.E., New Directions in Cryptography, IEEE Transactions on Information Theory, vol. 22, no. 6, November 1976, pp.

II. Garret, Paul. Making, Breaking Codes: An Introduction to Cryptology. Upper Saddle River, NJ: Prentice-Hall, 2001

III. http://grouper.ieee.org/groups/1363/lattPK/submissions.html#NTRU1

IV. Kurose, James F., Ross, Keith W., Computer Networking: A top Down Approach Featuring the Internet. 2nd edition. Addison Wesley 2002.

V. Barua, M., Alam, M.S., Liang, X. and Shen, X. (2011) 'Secure and quality of service assurance scheduling scheme for wban with application to ehealth', Wireless Communications and Networking Conference (WCNC), 2011 IEEE, Cancun, Quintana-Roo, Mexico, pp.1–5.

VI. Bethencourt, J., Sahai, A. and Waters, B. (2007) 'Ciphertext-policy attribute-based encryption', Security and Privacy, 2007. SP '07. IEEE Symposium on, Washington DC, USA, pp.321–334.

VII. Bethencourt, J., Sahai, A. and Waters, B. (2011) Advanced Crypto Software Collection, Ciphertext-Policy Attribute-Based Encryption, http://acsc.cs.utexas.edu/cpabe/

VIII .Boneh, D. and Franklin, M.K. (2001) 'Identity-based encryption from the weil pairing', CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, Springer-Verlag, London, UK, pp.213–229.

BIOGRAPHY

SUBARNA PANDA.
M.Tech (CSE)
Working as Professor Jain University Jayanagar, 9th block, Bengaluru, Karnataka, India

Department of Computer Science & Information Security

ANUGRAH CP
MASTER OF COMPUTER APPLICATION. (Information Security & Management Service)
Jain University Jayanagar, 9th block, Bengaluru, Karnataka, India