A Framework for Accessing Control over the Personal Health Records Based on Attributes

B.V.P.V.Narasimha Murty[1], Ch.Sunil[2]
M.Tech Scholar[1], Assistant Professor[2]
[1,2]Dept of CSE in Kaushik College of Engineering,Visakhapatnam, Andhra Pradesh, India

Abstract: Personal health records (PHR) are the brief information about the patient. These are stored in the third party servers such as cloud servers. It has some complexities to preserve these records more secure and providing privacy to the PHR. To assure privacy and secure about the patient record we introduced a framework called attribute based encryption (ABE) technique. It is based on the user accessing providing by the PHR owner and service provider. It reduces key distribution complexity and enables fine grained access. Users are divided into two types such as Public and Personal users. Our framework improves the privacy and security to personal health records and it enables dynamic control of the health records to record owner and dynamic access controlling by the health record owner.

I.INTRODUCTION

E- health record is a clear summary of health check-up of an individual. It contains medical prescription and check-up done by doctor and their details. In this user can specify their blood group, haemoglobin etc. details are also included. Users store their records in third party resources for receiving better suggestions from the personal and medical people.

A)Management of E-Health Infrastructure

On a larger scale, the whole infrastructure of an e-healthcloud has several risks that threaten the privacy of healthdata. Both medical and administrative data of patients areprocessed at several places in the e-health cloud, and theusage of smartcards and access control mechanisms alonedoes not provide the necessary protection.

a.Cryptographic Key Management

Complex infrastructures must be managed and this com-prises additional security and privacy issues. The usageof encryption requires management of cryptographic keys,smartcards must be personalized and issued to their users. One question that is often insufficiently answered in this context concerns that is in control of the cryptographic keys. Anaive approach would way the patient of course. But howto handle lost or stolen cards when the encryption keys arelost as well? And do the card issuers or the EHR server havebackup copies of the keys? But backup strategies must alsotake into account the privacy requirements of health data.For example, in many European countries, and especially inGermany, it is required by law that the patients themselveshave the full data sovereignty over their health data. Thismeans no other party is allowed to circumvent privacy decisions and access rights definitions of the patient regardingEHR data. But if the card issuer or even the EHR serverproviders maintain backup copies of the cryptographic keysfor reasons of issuing backup smartcards in case of theft orloss, they could in principle decrypt and access the EHRdata directly.

b.Management of Certificates

As in any public key infrastructure, certificates must bemanaged to ensure authenticity of key holders (smartcards,connectors, server, etc.). This includes issuing and distributing certificates as well as updating revocation lists.Management of Hardware/Software Components.Besides the cryptographic infrastructure, other components must be managed and maintained as well. This includes the hardware and software components that are usedat EHR servers and billing servers and computing devices ofhealth care providers. Security-critical component those are smartcard readers or connectors to protected networks are should be certified and tested properly. The installationand update of software components requires a secure distribution mechanism. On the other side it must be possibleto allow changes in software configuration due to legitimateupdates. On the next side unauthorized and maliciouschanges (e.g., due to malware attacks) are must be detectableto stop further usage or to exclude the infected componentsfrom the e-health infrastructure.

II. RELATED WORK

An (Key-Policy) Attribute Based Encryption scheme consists of four algorithms.

Setup: This is a randomized algorithm that takes no input other than the implicit securityparameter. It results the public parameters PK and a master key MK.

Encryption: This is a randomized algorithm that takes as input a message m and the set of attributes γ and public parameters PK results ciphertext E.

Key Generation: This is a randomized algorithm that takes as input toan access structure A and master key MK and the public parameters PK results decryption key D.

Decryption: This algorithm takes as input { the ciphertext E that was encrypted under the set γ of attributes and decryption key D for access control structure A and the

publicparameters PK. It outputs the message M if γ belongs to A.We now discuss the security of an ABE scheme.

A)Fine-grained Access Control

Fine-grained access control systems facilitate grantingdifferential access rights to a set of users and allow flexibility in specifying the access rightsof individual users. There are so many techniques are known for implementing ¯ne grained accesscontrol.

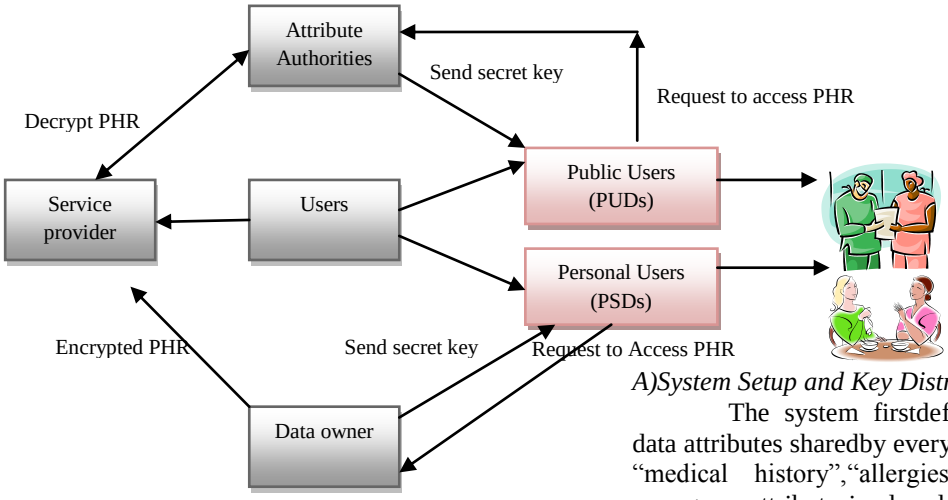
Common to the existing techniques and the referencestherein) is the fact that they employ a trusted server that stores the data in clear. The Accesscontrol depends on software checks to ensure that a user can access a piece of data only ifhe is authorized to do so. This resultant situation is not particularly appealing from a securitystandpoint. In the event of server compromise and for example the result of a softwarevulnerability exploit and potential for information theft is immense and in that always danger of insider attacks wherein a person having access to the server stealsand leaks the information and for example and economic gains. There are some techniques create user hierarchies and require the users to share a common secret key if they are ina common set in the hierarchy. The data is divided according to the hierarchy andencrypted under the public key of the set it is meant for and those methods have severallimitations. Consider that third party must access the data for a set of users of that set either needsto act as an intermediary and decrypt all relevant entries for the party or must give theparty its private decryption key thus let it have access to all entries. Most of the cases by using the user hierarchies it are not even possible to realize an access control equivalentto monotone access trees.In this paper, we introduce new techniques to implement ¯ne grained access control. Inour work data is stored on the server in an encrypted form while different users are still allowed to decrypt different pieces of data per the security policy. This eliminates the need to rely on the storage server for preventing unauthorized data access.

III. OUR APPROACH

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. Main idea is to divide the system into multiple security domains (namely, public users (PUDs) and personal users (PSDs)) according to the different users' data access requirements. The Public users consist of users who make access based on their professional roles they are doctors, nurses and medical researchers. In practical issues a public user can be mapped to an independent sector in the society and such as the health care and government or insurance sector. For each personal user its users are personally associated with a data owner (such as family members or close friends) and they make accesses to personal heal record based on access rights assigned by the owner. Which there are multiple attribute authorities(AAs), each governing a disjoint subset of attributes. Role attributes are defined for PUDs are representing the professional role or obligations of a PUD user. Users in public users obtain their attribute based secret keys from the AAs and without directly interacting with the owners. To control access from PUD users and the owners are free to specify role-based fine-grained access policies for her PHR files and while do not need to know the list of authorized users when doing encryption. Since the publicusers contain the majority of users and it is greatly reduces the key management overhead for both the owners and users.

In our framework, there are multiple SDs and multipleowners and the multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes areatomic file categories while internal nodes are compoundcategories. Dark boxes are the categories that a personal user'sdata readers have access to.The two attribute based systems are involved: for each PSD the YWRL'srevocable KP-ABE scheme [9] is adopted; We term the users having read and write access as datareaders and contributors.

Fig 1: Architecture of Key Policy Attribute Based Encryption



A)System Setup and Key Distribution

The system firstdefines a common universe of data attributes sharedby every PSD, such as "basic profile", "medical history","allergies", and prescriptions. The emergencyattribute is also defined for break-glass access. Each personal health recordowner's client application

generates its correspondingpublic or master keys. The public keys can be publishedvia user's profile in an online healthcare social-network(HSN) (which could be part of the PHR service; e.g., theIndivo system [27]). There are two ways for distributingsecret keys. Initially first using the PHR service aPHR owner can specify the access privilege of a datareader in her PSD and let him/her application generateand distribute corresponding key and in a wayresembling invitations in GoogleDoc. Next a readerin personal users could obtain the secret key by sending a request(indicating which types of files she wants to access) tothe PHR owner via HSN then the owner will grant hera subset of requested data types. Based on the request thepolicy engine of the application automatically derives anaccess structure and runs keygen of KP-

ABE to generatethe user secret key that embeds her access structure. Adding to that the data attributes can be organized in ahierarchical manner for efficient policy generation . When the user is granted all the file types undera category and his/her access privilege will be represented bythat category instead.For the public users the system defines role attributesthen the reader in a PUD obtains secret key from AAs andbinds the user to her claimed attributes/roles.

Now, if we want each authority to give out its own polynomials, one simplesolution might be to do an additive secret sharing to form the SW secrets (i.e.the values y such that every random polynomial p is chosen with p(0) = y).Thus, we pick a random value for the master secret y0 and for each authorityk = 1. . . K, y_k is a share of y_0 so $\sum y_k = y_0$. We can output $e(g, g)y_0$ as the entiresystems public key. Then to encrypt message m and a user gives $E = e(g, g)^{y0s}$mand $E_{k,i} = T^{s}_{k,i}$ for all i, k where they wish to allow a decryptor to use attribute. In addition, theAAs distribute write keys that permit contributors intheir PUD to write to some patients' PHR.

C)PHR Encryption and Access

The owners uploadABE-encrypted PHR files to the server. Each owner'spersonal health record file is encrypted both under a certain finegrainedand role-based access policy for users fromthe PUD to access control and under a selected set of dataattributes that allows access from users in the PSD. Onlyauthorized users can decrypt the personal health record files are excluding inthe server. Instantaneously improving efficiency data attributeswill include all the intermediate file types from a leafnode to the root.An "allergy" file'sattributes are *{PHR, medical history, allergy}*. The datareaders download PHR files from the server and theycan decrypt the files only if they have suitable attributebased keys. The data contributors will be grantedthe write access to someone's personal health record, if they present properwrite keys.

IV.CONCLUSION

Based on privacy and security of the personal health records we designed a framework it improves the control over the personal health records of the patient. The owners of the health record have full control over the health records. The framework includes multiple owners and multiple users, and attribute based encryption that reduces the complexity of the key management. It implementation works efficiently and sufficiently on the health records.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in *SecureComm'10*, Sept 2010, pp. 89–106.

[2] H. L¨ohr, A.-R.Sadeghi, and M. Winandy, "Securing the e-health cloud," in *Proceedings of the 1st ACM International Health Informatics Symposium*, ser. IHI '10, 2010, pp. 220–229.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in *ICDCS '11*, Jun. 2011.

[4] "The health insurance portability and accountability act." [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

[5] "Google, microsoft say hipaa stimulus rule doesn't apply tothem," http://www.ihealthbeat.org/Articles/2009/4/8/.

[6] "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded," 2006. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26

[7] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," *BMJ*, vol. 322, no. 7281, p. 283, Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in *CCSW '09*, 2009, pp. 103–114.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *IEEE INFOCOM'10*, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in *Journal of Computer Security*, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *CCS '06*, 2006, pp. 89–98.

[12] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEEWireless Communications Magazine*, Feb. 2010.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *ACM CCS*, ser. CCS '08, 2008, pp. 417–426.

[14] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ASIACCS'10*, 2010.

14

[16] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10 2010, pp. 47–52.

[17] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in *AHIC 2010*, 2010.
[18] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," *Technical Report, University of Twente*, 2009.
[19] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE S& P '07*, 2007, pp. 321–334.

BIOGRAPHIES

B.V.P.V.Narasimha Murty completed his MSc(Computer Science), and he is currently pursuing M.Tech in Department of CSE in Kaushik College of Engineering. His interested areas are data mining & data warehousing and Computer Networks.

Ch.Sunil is an Asst. Professor of the Department of CSE, Kaushik College of Engineering (Affiliated to JNTUK), Visakhapatnam, Andhra Pradesh, India. He obtained his M.Tech. in Computer Science & Engineering from AcharyaNagarjuna University. He is pursuing Ph.D. in Computer Science & Engineering from GITAM University, Visakhapatnam. His main research interests are Cryptography and Network Security.