IPHV8I107X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION FOR SECURE AND SHARING OF PERSONAL HEALTH RECORDS

[#1]K. AJAY KUMAR RAJU – Pursuing M.Tech,
[#2]SUBBA RAO POLAMURI –Asst. Professor,

Dept of CSE, AMALAPURAM INSTITUTE OF MANAGEMENT SCIENCES AND COLLEGE OF ENGINEERING, MUMMIDIVARAM, WEST GODAVARI, A.P., INDIA.

Abstract: — Attribute based encryption determines encryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to user and encryptor can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Personal Health Record (PHR) is maintained in the centralized server to maintain the patient's information. The patient records should be maintained with high privacy and security. The security schemes are used to protect the personal data from public access. Patient data can be accessed by many different people. Each authority is assigned with access permission for a particular set of attributes. The access control and privacy management is a complex task in the patient health record management process. Cloud computing is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers that are connected through a real-time communication network. It is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. Data owners update the personal data into third party cloud data centers. In this paper, we propose a novel patient-centric framework and a suite of data access mechanisms to control PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage Attribute Based Encryption (ABE) techniques to encrypt each patient's PHR file. Multiple data owners can access the same data values. The proposed scheme could be extended to Multi Authority Attribute Based Encryption (MA-ABE) for multiple authority based access control mechanism.

Index Terms- *Personal Health Records, Cloud Computing, Data Privacy, Fine-grained access control, Multi-authority Attribute Based Encryption..*

I. INTRODUCTION

a patient-centric model of health information exchange. It enables the patient to create and control their medical data which may be placed in a single place such as data center. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to third-party service providers, for example, Microsoft Health Vault, Google Health. While it is exciting to have convenient PHR data 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. Although there exist health care regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. 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 [1]. "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" [2]. To ensure privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. Hence we move to a new encryption pattern namely Attribute Based Encryption (ABE). In ABE, it is the attributes of the users or the data that selects the access policies, which enables a patient to selectively share their PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. As a result, the number of attributes involved determines the complexities in encryption, key generation and decryption. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism. A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the PHR owner them self should decide how to encrypt their 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. The goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc. We refer to the two categories of users as personal and professional users, respectively.

II. RELATED WORK

The paper is mostly related to work in cryptographically enforced access control for outsourced data and attribute based encryption. To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used [1]. A fundamental property of ABE is preventing against user collusion. In addition, the encryptor is not required to know the ACL. A. Trusted authority A number of works used ABE to realize fine-grained access control for outsourced data [3], [4]. Recently, Narayan et al. proposed an attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE [5] that allows direct revocation. There are several common drawbacks of the above works. First, they usually assume the use of a single Trusted Authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys [1]. B. Attribute Based Encryption It is a well-known challenging problem to revoke users/attributes efficiently and on-demand in ABE. Traditionally this is often done by the authority broadcasting periodic key updates to unrevoked users frequently [6], [7], which does not achieve complete backward/forward security and is less efficient. This paper bridges the above gaps by proposing a unified security framework for patient-centric sharing of PHR in a multi-domain, multi-authority PHR system with many users. The framework captures application level requirements of both public and personal use of a patient's PHR and distributes users' trust to multiple authorities that better reflects reality.

III. PROBLEM DEFINITION

The problem is being extended to a wider range, where a number of PHR owners and users are involved. The owners refer to patients whose medical related data are being controlled and the users are those who try to access them. There exists a central server where owners place their sensitive medical data, and attempted by users to gain access. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data. This leads to the need of Multi-Authority Attribute Based Encryption (MA-ABE). A. Prevention of Unauthorized Users An important requirement of efficient PHR access is to enable "patient-centric" sharing. This means that the patient should have the ultimate control over their personal health record. They determine which users shall have access to their medical record. User controlled read/write access and revocation are the two core security objectives for any electronic health record system. Users controlled write access control in PHR context entitles prevention of unauthorized users to gain access to the record and modifying it. B. Fine Grained Access Control Fine grained access control should be enforced in the sense that different users are authorized to read different sets of documents. The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute. C. Attribute Revocation This is usually called attribute revocation. The PHR system should support users from both the personal domain as well as public domain. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners' efforts in managing users and keys should be minimized to enjoy usability.

IV. SOLUTION FRAMEWORK

The main goal of the system is to provide secure access of PHR in a patient-centric manner and efficient key management. First, the system is divided into multiple security domains like Personal domain (PSD) and Public domain (PUD). Each domain controls only a subset of its users. For each security domain, one or more authorities are assigned to govern the access of data. For personal domain it is the owner of the PHR itself who manages the record and performs key management. This is less laborious since the number of users in the personal domain is comparatively less and is personally connected to the owner. Public domain consists of a large number of professional users and therefore cannot be managed easily by the owner herself. Hence it puts forward the

new set of public Attribute Authorities (AA) to govern disjoint subset of attributes.

A. Multi-Authority ABE

A Multi-Authority ABE system is comprised of k attribute authorities and one central authority. Each attribute authority is also assigned a value, dk. The system uses the following algorithms:

1) Set up: A random algorithm that is run by the central authority or some other trusted authority. It takes as input the security parameter and outputs a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key which will be used by the central authority.
2) Attribute Key Generation: A random algorithm run by an attribute authority. It takes as input the authority's secret key, the authority's value dk, a user's GID, and a set of attributes in the authority's domain and output secret key for the user.
3) Central Key Generation: A randomized algorithm that is run by the central authority. It takes as input the master secret key and a user's GID and outputs secret key for the user.
4) Encryption: A randomized algorithm runs by a sender. It takes as input a set of attributes for each authority, a message, and the system public key and outputs the cipher text.
5) Decryption: A deterministic algorithm runs by a user. It takes input a cipher-text, which was encrypted under attribute set and decryption keys for that attribute set.
This algorithm outputs a message m. Using ABE and MA-ABE which enhances the system scalability, there are some limitations in the practicality of using them in building PHR systems. For example, in workflow based access control scenarios, the data access right could be given based on users' identities rather than their attributes, while ABE does not handle that efficiently. In those scenarios one may consider the use of attribute-based broadcast encryption [9]. In addition, the expressibility of encryptor access policy is somewhat limited by that of MA-ABE's, since it only supports conjunctive policy across multiple AAs.

V. SECURITY ANALYSIS OF THE PROPOSED SYSTEM

<element name="PGPData" type="ds:PGPDataType"/> <complexType name="PGPDataType"> <choice> <sequence> <element name="PGPKeyID" type="base64Binary"/> <element name="PGPKeyPacket" type="base64Binary" minOccurs="0"/> <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> </sequence> <sequence> <element name="PGPKeyPacket" type="base64Binary"/> <any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> </sequence> </choice> </complexType>

Some of the security analyses of the proposed system are as follows:
1) Fine-grainedness of Access Control: In the proposed scheme, the data owner is able to define and enforce expressive and flexible access structure for each user. Specifically, the access structure of each user is defined as a logic formula over data file attributes, and is able to represent any desired data file set.
2) Data Confidentiality: The proposed scheme discloses the information about each users access on the PHR among one another. For eg, the data revealed to a research scholar may be unknown to a lab technician.
3) User Access Privilege Confidentiality: The system does not reveal the privileges of one user to another. This ensures user access privilege confidentiality. This is maintained for public domain as well as private domain.
A. Secure Sharing Of Personal Health Records
The system is designed to manage Personal Health Records (PHR) with different user access environment. The data values are maintained under a third party cloud provider system. The data privacy and security is assured by the system. The privacy attributes are selected by the patients. The data can be accessed by different parties. The key values are maintained and distributed to the authorities. The system is enhanced to support Distributed ABE model. The user identity based access mechanism is also provided in the system. The system is divided into six major modules. They are data owner, cloud provider, key management, security process, authority analysis and client.
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.
2) Cloud Provider: The cloud provider module is used to store the PHR values. The PHR values are stored in databases. Data owner uploads the encrypted PHR to the cloud providers. User access information's are also maintained under the cloud provider.
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.

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) 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.

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.

VI. CONCLUSION & FUTURE WORK

A framework of secure sharing of personal health records has been proposed in this paper. Public and Personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced. The attribute-based encryption model is enhanced to support operations with MAABE. The system is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy. As future study, it will be interesting to enhance the HSN with a third party auditor to verify the cloud server that stores and process the PHRs homomorphic Split key Encryption can become additional enhancement to verify the trustworthiness of the TPA.

REFERENCES:

[1] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions On Parallel And Distributed Systems 2012.

[2] "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.

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

[4] 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.

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

[6] Melissa Chase, "Multi-authority Attribute Based Encryption", TCC, volume 4392 of LNCS, pages 515–534, Springer, 2007.

[7] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," Technical Report, University of Waterloo, 2010.

[8] 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.

[9] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," Pairing-Based Cryptography– Pairing 2009, pp. 248–265, 2009.

[10] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.

[11] "Privacy-preserving personal health record system using attribute-based encryption," Master's thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011.

[12] S. M¨ uller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption,"Information Security and Cryptology–ICISC 2008, pp. 20–36, 2009.

AUTHORS PROFILE:

[1]. K. AJAY KUMAR RAJU M.Tech, CSE Dept, Amalapuram Institute of Management Sciences & College Of Engineering, Mummadivaram, AP.

[2]. SUBBA RAO POLAMURI, Asst.Prof is currently heading the department of Computer Applications, AIMS College Of Engineering. He is a postgraduate in Computer Science and Technology and had 7 years of teaching and research experience. His research interests include spatial data mining, web mining and data warehousing.