Secure and Scalable Sharing Of Personal Health Records (PHR) In Cloud Computing Using Multi Authority Attribute Based Encryption

Gadwala Rakesh[1] Venkata Subramanian D[2]
[1]U.G. Student [2]Professor
[1,2]Department of Computer Science and Engineering
[1,2]Saveetha School of Engineering, Saveetha University Chennai, India.

Abstract— Personal health records (PHR) is an emerging centric patient model of health information exchanges, which is often stored at a third party. Such as cloud providers so there is been better privacy provided by considering the personal health information's so that, they will no longer be accessible to the third party servers and other parties .So some specific issues like privacy exposure, scalability in key management, flexible access and efficient user revocation these process can be achieved. The stored data will be in the form of cryptography so here in the existing system it uses attribute based encryption (ABE) in order to maintain each patient's PHR file .so here we focus on multi authority attribute based encryption (MABE) to maintain the PHR for every clients in making modification of access policies or file attributes, supports efficient on demand user/attribute revocation and emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

Key words: Cloud computing,Personal Health record,Cloud server,Data

I. INTRODUCTION

A. General

The consistent help from the present measure of film information has changed the critical must construct keen approaches to schema notwithstanding draw out this motion picture content material. Normal capacities where displaying and also taking out film content material are exceptionally significant hold motion picture security, feature on-interest projects, ambush recognizable proof, outer screening, games capacities, criminal dissection investigation items, and numerous different styles.

B. Objective

The ABE based framework for patient-centric secure sharing of PHR in cloud computing is done under the multi-owner settings. To address the key management challenge's and conceptually divides the users in the system into two types of domains namely public and personal domain.

C. Existing approach

Personal health record (PHR) has emerged as a patient-centric model of health information exchange. PHR service allows patient to create ,manage of personal health data in one place through the web, which has made the storage ,retrieval and sharing of medical information in an efficient way. Especially, security was provided in high way to control of medical records and health data with wide range of users, including health care providers, family members and friends. Due to high cost building and maintaining specialized data centers, many PHR services are outsourced and provided to third party server due to this client many not trust fully because the personal health information(PHI) are sensitive, the third party servers often targets of various malicious methods which may lead to the exposure of the PHI without any authorization.

D. Proposed approach

Despite of these problems by third party server we propose ABE frame work for patient-centric secure, sharing of PHR in cloud computing environments. So addressing of key management challenges, we conceptually divide the user in the system in two types of domain .Such as, public domain and personal domain. In majority professional users are managed distributive by attribute authorities here owner's needs only small number of keys for users in personal domain. In this way framework can simultaneously handle different types of PHR sharing applications requirements by causing minimal key management over head for both owners and users in the system and can handle dynamic policy updates by accessing PHR in emergency scenarios. In public domain we use multi-authority ABE (MA-ABE) to improve the security and key escrow problems. Each attribute authority (AA) in it governs the disjoint subset for user role attributes and we propose the mechanism for the key distribution and encryption so that PHR owners can specify personalized role based access policies during the file encryption. In the personal domain, owners directly access privileges for personal users and encrypt PHR file under its data attributes. We enhance MA-ABE by keeping forward an efficient and demand user attribute revocation scheme and prove its security under standard security assumptions.

Abstraction Process:

II. ANALYSIS MODEL

There are four types of phases in spiral model

- Planning
- Evolutions
- Risk Analysis
- Engineering

A. Planning

In this phase, the aims, option and constraints of the project are determined and are documented. The aims and other specifications are fixed so as to determine the strategies/approaches to go after during the project life cycle.

B. Evolution:

The evolutionary process begins at the center position and moves in a clockwise direction. Each traversal of the spiral typically results in a deliverable. For example, the first and second spiral traversals may result in the production of a product specification and a prototype, respectively. Subsequent traversals may then produce more sophisticated versions of the software.

III. Modules

– PHR Owner Module
– Cloud Server Module
– Attribute based Access Policy Module
– Data confidentiality Module

A. PHR Owner Module

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains (PUDs) and personal domains (PSDs)) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.

B. Cloud Server Module

Means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

C. Attribute based Access Policy Module

In our framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition, two ABE systems are involved. We term the users having read and write access as data readers and contributors, respectively

D. Data confidentiality Module

The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PHR files, excluding the server.

Reference

[1] Priyanka Korde, Vijay Panwar, Sneha Kalse Computer Eng.Dept.Pimpri Chinchwad colleage of Engineering, Pune, India. "Focus on multiple owner on PHR owner scenario and division of personal health records users into multiple security domains "on April 2013.

[2] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou members of IEEE" content on Novel patient -centric frame network and suite of mechanisms for data acess controllto PHR stored semi trusted servers".

[3] H.Lohar, A-R.Sadeghi, M.winady," Securing the e-healtth cloud"in preceedings of the 1st ACM International Health Informatics Symposium, ser.IHI'10, 2010, pp.220-229.

[4] Josh Benaloh, Melissa Chase, Eric Horvitz and Kristin Lauter Microsoft Research Redmond, WA, USA"Enabling patients to generate and store encryption keys for protecting the patientce privacy".

[5] V.Goyal, O.Pandey, A.Sahi and B.Waters,"Attribute based encryption for free grained access control of encrypted data", in CCS'06, 2006, PP.89-98.

[6] Selim G.Akl and Peter D.Talyor"Cryptographic Solution to a problem of access control in hierarchy"ACM Trans.Comput.Syst., 1(3):239-248,1983.