IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 11-13

Privacy-Enhancing Patient Profile Management

[1]sri Devi. R Me Cse [2]v.Vimala [3]t.Kujani
Dept. Of Computer Science &Engg.
[1,2,3]Skr Engineering College, Agarmel, Chennai-600 123.

Abstract : *Collaborative healthcare environments offer potentialbenefits, including enhancing the healthcare quality deliveredto patients and reducing costs. As a direct consequence, sharing ofElectronic Health Records (EHRs) among healthcare providershas experienced a noteworthy growth in the last years, sinceit enables physicians to remotely monitor patients' health andenables individuals to manage their own health data more easily.However, these scenarios face significant challenges regardingsecurity and privacy of the extremely sensitive informationcontained in EHRs. Thus, a flexible, efficient and standardsbasedsolution is indispensable to guarantee selective identity informationdisclosure and preserve patient's privacy. We proposea privacy-aware profile management approach that empowers thepatient role, enabling him to bring together various healthcareproviders as well as user-generated claims into an uniquecredential. User profiles are represented through an adaptiveMerkle Tree, for which we formalize the underlying mathematical model. Furthermore, performance of the proposed solution isempirically validated through simulation experiments.*

I Introduction

Fast access to health data enables better healthcare service provisioning, improves quality of life, and helps saving life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in our daily life. Services supported by mobile devices, such as home care and remote monitoring, enable patients to retain their living style and cause minimal interruption to their daily activities. In addition, it significantly reduces the hospital occupancy, allowing patients with higher need of in-hospital treatment to be admitted. While these e-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are involved, and people start to realize that they would completely lose control over their personal information once it enters the cyberspace. According to the government website, around 8 million patients' health information was leaked in the past two years. There are good reasons for keeping medical data private and limiting the access. An employer may decide not to hire someone with certain diseases. An insurance company may refuse to provide life insurance knowing the disease history of a patient. Despite the paramount importance, privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short. This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an urgent need for the development of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information. Outsourcing data storage and computational tasks becomes a popular trend as we enter the cloud computing era. A wildly successful story is that the company's total claims capture and control (TC3) which provides claim management solutions for healthcare payers such as medicare payers, insurance companies, municipalities, and self-insured employer health plans. TC3 has been using Amazon's EC2 cloud to process the data their clients send in (tens of millions of claims daily) which contain sensitive health information. Outsourcing the computation to the cloud saves TC3 from buying and maintaining servers, and allows TC3 to take advantage of Amazon's expertise to process and analyze data faster and more efficiently. The proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the cloud-based data/computation outsourcing paradigm. We introduce the private cloud which can be considered as a service offered to mobile users. The proposed solutions are built on the service model shown in. A software as a service (SaaS) provider provides private cloud services by using the infrastructure of the public cloud providers (e.g., Amazon, Google). Mobile users outsource data processing tasks to the private cloud which stores the processed results on the public cloud. The cloud-assisted service model supports the implementation of practical privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks.

II Problem Description:

Collaborative healthcare environments offer potential benefits, including enhancing the healthcare quality delivered to patients and reducing costs. As a direct consequence, sharing of Electronic Health Records (EHRs) among healthcare providers has experienced a noteworthy growth in the last years, since it enables physicians to remotely monitor patients' health and enables individuals to manage their own health data more

easily. However, these scenarios face significant challenges regarding security and privacy of the extremely sensitive information contained in EHRs. Thus, a flexible, efficient and standardsbased solution is indispensable to guarantee selective identity information disclosure and preserve patient's privacy. We propose a privacy-aware profile management approach that empowers the patient role, enabling him to bring together various healthcare providers as well as user-generated claims into an unique credential. User profiles are represented through an adaptive Merkle Tree, for which we formalize the underlying mathematical model. Furthermore, performance of the proposed solution is empirically validated through simulation experiments.

III Existing System

In theexisting system, Personal health record (PHR) is an emerging patient-centric in Cloud Computing Servers. However, there is no Security in keeping privacy concerns of the Patient & could be exposed to those third party servers and to unauthorized parties.

Disadvantages of existing system:

- Security is very less.
- Trustworthiness between the Users and the Cloud Service Providers can't be maintained properly.

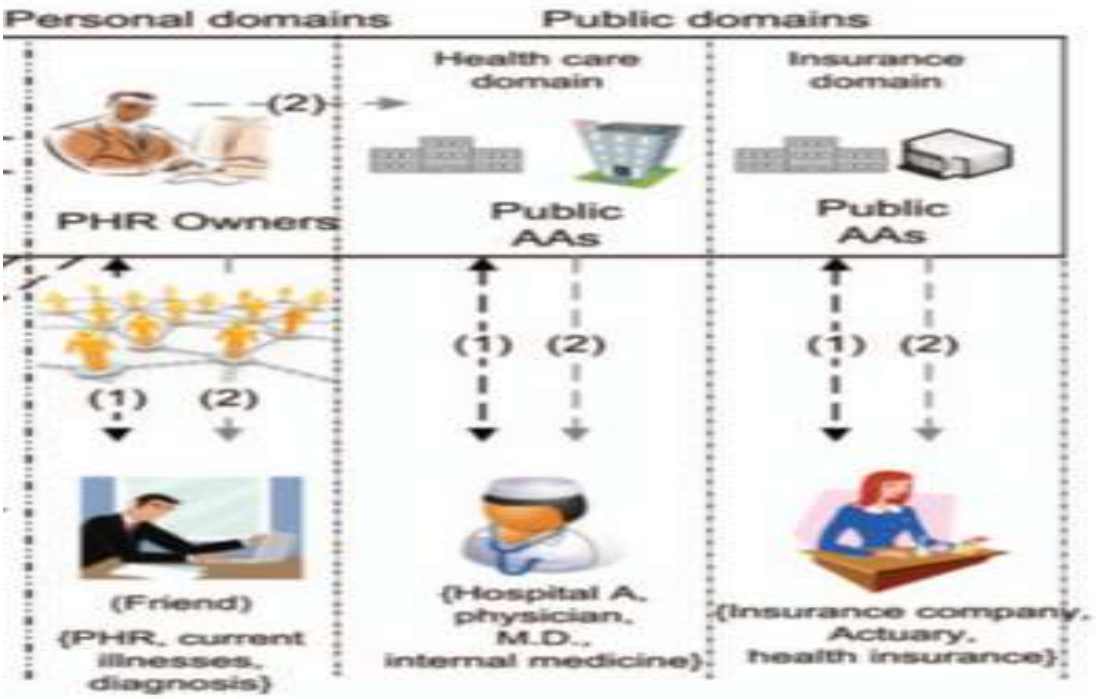
IV Proposed System

 In the proposed model, a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. We leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. 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.

Advantages of the proposed system

- Security level will be increased.
- Trustworthiness will also be maintained properly.

V Architecture Diagram



VI Conclusion

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and

users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient.

References

[1]. Li M., Yu S., Ren K., Lou W. (2010) Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings. In: Jajodia S., Zhou J. (eds) Security and Privacy in Communication Networks. SecureComm 2010. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 50. Springer, Berlin, Heidelberg

[2]. Yan-Cheng Chang and Michael Mitzenmacher. 2005. Privacy preserving keyword searches on remote encrypted data. In Proceedings of the Third international conference on Applied Cryptography and Network Security (ACNS'05), John Ioannidis, AngelosKeromytis, and Moti Yung (Eds.). Springer-Verlag, Berlin, Heidelberg, 442-455. DOI=http://dx.doi.org/10.1007/11496137_30

[3]. Reza Curtmola, Juan Garay, Seny Kamara, and RafailOstrovsky. 2006. Searchable symmetric encryption: improved definitions and efficient constructions. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA, 79-88. DOI=http://dx.doi.org/10.1145/1180405.1180417

[4]. Eu-Jin Goh. 2003. Secure Indexes. Cryptology ePrint Archive, Report: 216.

[5]. Lv Z., Hong C., Zhang M., Feng D. (2014) Expressive and Secure Searchable Encryption in the Public Key Setting. In: Chow S.S.M., Camenisch J., Hui L.C.K., Yiu S.M. (eds) Information Security. ISC 2014. Lecture Notes in Computer Science, vol 8783. Springer, Cham