International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600

http://www.ijcsjournal.com Volume 4, Issue 2, No 3, 2016. ISSN: 2348-6600
Reference ID: IJCS-129 PAGE NO: 762-765

Personal Health Records in Cloud Computing Using Multi Authority Attribute-based Encryption

[1,] V.Ankayarkanni, [2,] Dr.V.Jayaraj

[1] Research Scholar , Bharathidasan University ,Trichy

[2] Assistant Professor, School of CSE & Applications, Bharathidasan University ,Trichy

Abstract— A PHR service allows a patient to create, manage, and control her Personal health data storage, retrieval and sharing of the medical information in web. The patient could actually control the sharing of their sensitive Personal health information's are stored on a third party server which people may not fully trusted. To ensure patient centric privacy control over their own PHR have fine-grained access control mechanisms that work in the semi trusted servers and the PHR owner encrypt her file should only be available decrypt it. Each attribute authority (AA) in it governs disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt PHR file under its data attributes MA-ABE by putting forward an efficient on demand user/attribute revocation scheme, and prove its security under standard security assumptions

Keywords- Hybrid wireless Network, Three-Hop, Distributing, Throughput, Overhead.

1. INTRODUCTION

Personal Health Record (PHR) is emerged as 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 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 health care 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 In security based 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 (MAABE) scheme is used to provide multiple authority based access control mechanism. 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. Delineation and implementation of accepted standards for health-care data, accurate patient identification and record matching, and the definition of incentives for accelerated deployment of health information technology. In response to these challenges, we present in this paper an alternative option, the Health Record Banking (HRB) system. Emulating commercial banking, this approach uses health-record banks to serve the need for immediately accessible and secure data for diverse stakeholders.

2. LITERATURE SURVEY

In[1] Ming Li clients usually outsource their independence for these banks and a mechanism for fostering medical research. We conclude with 10 critical issues associated with the development and implementation of an HRB system, which require public data to the cloud storage servers to reduce the management costs. While those data may contain sensitive personal information, the cloud servers cannot be fully trusted in protecting them. Encryption is a promising way to protect the confidentiality of the outsourced data, but it also introduces much difficulty to performing effective searches over encrypted information. Most existing works do not support efficient searches with complex query conditions, and care needs to be taken when using them because of the potential privacy leakages about the data owners to the data users or the cloud server. Personal Health Record (PHR) as a case study, we first show the necessity of search capability authorization that reduces the privacy exposure resulting from the search results, and establish a scalable framework for Authorized Private Keyword Search (APKS) over encrypted cloud data. We then propose two novel solutions for APKS based on a recent discussion. This paper describes the technology namely Health Record Banking (HRB). In [3] Liu, Z proposed the scheme called Clinical Document Architecture (CDA). Here X-PAT, a platform-independent software prototype that is able to manage patient referral multimedia data in an intranet network scenario according to the specific control procedures of a healthcare institution. It is a self- developed storage framework based on a file system, implemented in extensible Markup Language (XML) and PHP Hypertext Preprocessor Language, and addressed to the requirements of limited-dimension healthcare entities (small hospitals, private medical centers, outpatient clinics, and laboratories). In X-PAT, healthcare data descriptions, stored in a novel Referral Base Management System (RBMS) according to Health Level 7 Clinical Document Architecture Release 2 cryptographic primitive, Hierarchical Predicate (CDA R2) standard, can be easily applied to the Encryption (HPE). Our solutions enable efficient multi- dimensional keyword searches with range query, allow delegation and revocation of search capabilities. Moreover, we enhance the query privacy which hides users' query keywords against the server. We implement our scheme on a modern workstation, and experimental results demonstrate its suitability for practical usage. In this paper the technology used is Hierarchical Predicate Encryption (HPE). In [2] van den describes that the No unified, functioning system currently exists for the exchange of comprehensive health-care information across the wide spectrum of health-care networks. Regional health information organizations (RHIOs) and a national health information network (NHIN) have been proposed as vital building blocks in providing such a system, but these face many challenges, including specific data and organizational procedures of a particular healthcare working environment thanks also to the use of standard clinical terminology. Managed data, centralized on a server, are structured in the RBMS schema using a flexible patient record and CDA healthcare referral document structures based on XML technology. A novel search engine allows defining and performing queries on stored data, whose rapid execution is ensured by expandable RBMS indexing structures. Healthcare personnel can interface the X-PAT system, according to applied state-of-the-art privacy and security measures, through friendly and intuitive Web pages that facilitate user acceptance.

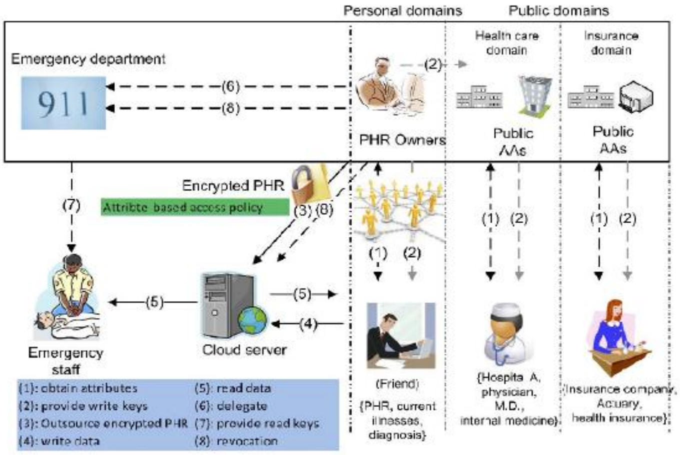
3. EXISTING SYSTEM

In Existing the Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

4. PROPOSED SYSTEM

The proposed system is a novel patient-centric framework and a suite of mechanisms for data access control to 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. Different from previous works in secure data 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 analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

5. SYSTEM MODEL



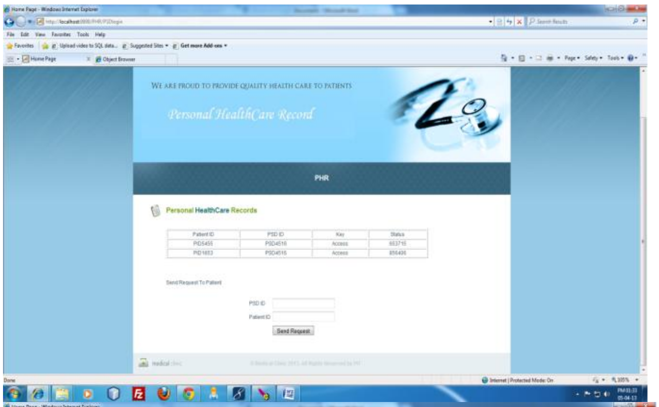
IJCS International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SK Research Group of Companies SKRGC Since 2012

http://www.ijcsjournal.com Volume 4, Issue 2, No 3, 2016. ISSN: 2348-6600
Reference ID: IJCS-129 PAGE NO: 762-765

6. CONCLUSION AND FUTURE WORK

In this paper System is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy. In future, to provide high security and privacy for Personal Health Record (PHR), the existing Multi authority attribute based encryption could be further enhanced to proactive Multi authority attribute based encryption Data Confidentiality and Integrity is a major concern. We mainly concentrate on business cloud where various organizations store their data about their project in the cloud. We have analyzed the security of our algorithm and also the efficiency.

7. SCREENSHOTS

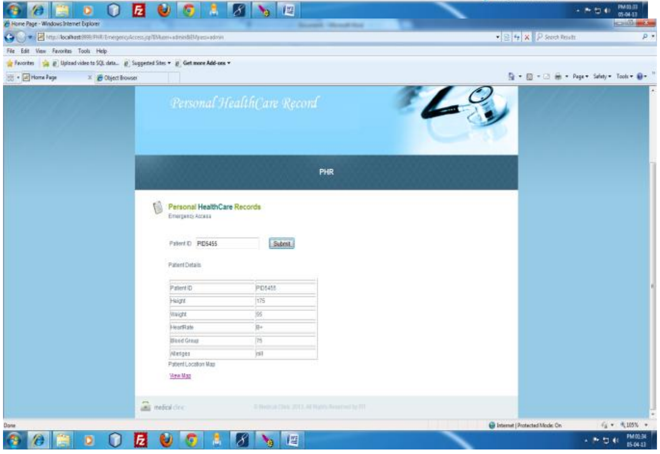

WE ARE PROUD TO PROVIDE QUALITY HEALTH CARE TO PATIENTS
Personal HealthCare Record
PHR
Send Request

Personal HealthCare Records

Patient ID	PSD ID	Key	Status
PID5455	PSD4516	Access	653716
PID1683	PSD4516	Access	856406

Send Request To Patient

PSD ID
Patient ID



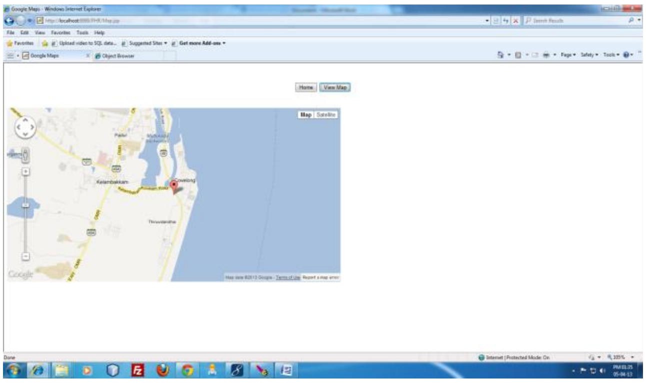
Personal HealthCare Records
Emergency Access

Patient ID PID5455

Patient Details

Patient ID	PID5455
Height	175
Weight	55
HeartRate	B+
Blood Group	75
Allergies	nil

Patient Location Map



REFERENCES

[1] Ming Li "Authorized private keyword search over encrypted personal health records in cloud computing" [2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010. [3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private KeywordSearch over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems(ICDCS '11), June 2011.

[4]"The Health Insurance Portability and AccountabilityAct,"http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp,2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply toThem," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] "At Risk of Exposure - in the Push for Electronic Medical Records,Concern Is Growing About How Well Privacy Can Be Safeguarded," http://articles.latimes.com/2006/jun/26/health/ he-privacy26, 2006.

[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, pp. 283-287, Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.