International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 8 –NOVEMBER 2016.

SHARING PERSONAL HEALTH RECORDS IN CLOUD WITH SCALABLE AND SECURE USING ABE

SHAIK SHAHINA[#1] ,GUNTAPALLI MINNI[*2] and SAYEED YASIN[*3]

[#] *M.Tech (CSE) Student, Nimra College of Engineering & Technology, A.P., India.*

[*2] *Assistant Professor, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

[*3] *Associate professor & Head, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

***Abstract*— 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. The main concern is about diagnosis information. The patient records should be whether the patients could actually control the sharing 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. The 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 (MAABE) for multiple authority based access control mechanism.**

Index Terms*— Cloud computing, Personal health records, data privacy, fine-grained access control, attribute-based encryption.

I. INTRODUCTION

Cloud computing provides shared processing environment for data storage and accessing also known as internet based computing. It is a model which provides configurable computing resources such as networks, servers, storage, applications and services. Cloud computing has a high computation power, lowest cost of services, higher performance, scalability, accessibility and availability for that reason it is highly demanded. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing PHRs in cloud computing have been proposed in .While it is exciting to have convenient PHR 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. On the one hand, although there exist healthcare 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 behaviours which may lead to expo- sure of the PHI. 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. To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. A feasible and promising approach would be to en- crypt the data before outsourcing. Basically, the PHR owner herself should decide how to encrypt her 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. However, 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. The latter has potentially large scale; should each owner herself be directly responsible for managing all the professional users, she will easily be overwhelmed by the key management overhead. In addition, since those users‟ access requests are generally unpredictable, it is difficult for an owner to determine a list of them. On the other hand, different from the single data owner scenario considered in most of the existing works in a PHR system, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner whose PHR she wants to read would limit the accessibility since patients are not always online. An alternative is to employ a central authority (CA) to do the key management on behalf of all PHR owners, but this requires too much trust on a single authority (i.e., cause the key escrow problem). In this paper, we endeavor to study the patient-centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her 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. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved.

II. EXISTING SYSTEM

A. *Existing System:*

Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft Health Vault.

While it is exciting to have convenient PHR 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.

B. *Disadvantages Of Existing System:*

There have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

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.

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 since the TA can access all the encrypted files, opening the door for potential privacy exposure. 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.

III. PROPOSED SYSTEM:

To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. In this paper, we propose 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.

- To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers.

- In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her 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.

A. *Advantages Of Proposed System:*

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.

In this paper, we bridge the above gaps by proposing a unified security framework for patient-centric sharing of PHRs 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 PHRs, and distributes users' trust to multiple authorities that better reflects reality.

IV. LITERATURE SURVEY

A. *Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings*

AUTHORS: M. Li, S. Yu, K. Ren, and W. Lou

Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which

greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to enjoy the elastic resources and reduce the operational cost. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Under encryption, it is challenging to achieve fine-grained access control to PHR data in a scalable and efficient way. For each patient, the PHR data should be encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios.

In this paper, we propose a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained and scalable access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR data. To reduce the key distribution complexity, we divide the system into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically. Our proposed scheme is also flexible, in that it supports efficient and on-demand revocation of user access rights, and break-glass access under emergency scenarios

B. Securing the e-health cloud

AUTHORS: H. L¨ohr, A.-R. Sadeghi, and M. Winandy

Modern information technology is increasingly used in healthcare with the goal to improve and enhance medical services and to reduce costs. In this context, the outsourcing of computation and storage resources to general IT providers (cloud computing) has become very appealing. E-health clouds offer new possibilities, such as easy and ubiquitous access to medical data, and opportunities for new business models. However, they also bear new risks and raise challenges with respect to security and privacy aspects.

In this paper, we point out several shortcomings of current e-health solutions and standards, particularly they do not address the client platform security, which is a crucial aspect for the overall security of e-health systems. To fill this gap, we present a security architecture for establishing privacy domains in e-health infrastructures. Our solution provides client platform security and appropriately combines this with network security concepts. Moreover, we discuss further open problems and research challenges on security, privacy and usability of e-health cloud systems.

C. Authorized private keyword search over encrypted personal health records in cloud computing

AUTHORS: M. Li, S. Yu, N. Cao, and W. Lou

In cloud computing, clients usually outsource their 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. In this paper, using on line 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 cryptographic primitive, Hierarchical Predicate 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.

D. Public standards and patients' control: how to keep electronic medical records accessible but private

AUTHORS: K. D. Mandl, P. Szolovits, and I. S. Kohane

A patient's medical records are generally fragmented across multiple treatment sites, posing an obstacle to clinical care, research, and public health efforts.1 Electronic medical records and the internet provide a technical infrastructure on which to build longitudinal medical records that can be integrated across sites of care. Choices about the structure and ownership of these records will have profound impact on the accessibility and privacy of patient information. Already, alarming trends are apparent as proprietary online medical record systems are developed and deployed. The technology promising to unify the currently disparate pieces of a patient's medical record may actually threaten the accessibility of the information and compromise patients' privacy. In this article we propose two doctrines and six desirable characteristics to guide the development of online medical record systems. We describe how such systems could be developed and used clinically.

E. Patient controlled encryption: ensuring privacy of electronic medical records

AUTHORS: J. Benaloh, M. Chase, E. Horvitz, and K. Lauter

We explore the challenge of preserving patients ' privacy in electronic health record systems. We argue that security in such systems should be enforced via encryption as well as access control. Furthermore, we argue for approaches that enable patients to generate and store encryption keys, so that the patients ' privacy is protected should the host data center be compromised. The standard argument against such an approach is that encryption would interfere with the functionality of the system. However, we show that we can build an efficient system that allows patients both to share partial access rights with others, and to perform searches over their records. We formalize the requirements of a Patient Controlled Encryption scheme, and give several instantiations, based on existing cryptographic primitives and protocols, each achieving a different set of properties.

V. REALATED WORK

The past and current information about health is collect, store and track, for this purpose we used toll called as PHR. By using this we can save our time and money as well as repetition of medical test should be avoided. A PHR is health record where all data about health is manipulated by patient itself. PHR is totally opposite to the current used electronic medical record. The electronic medical record is operated by different hospital and institution. The main purpose of PHR is to give the complete, good and correct summary of each patient's medical history and all this data is access via internet. PHR report mainly consists of lab result data from wireless result of patient data and patient data is collected from different hospital's computer. A personal Health Record, or PHR, is a health record where health data and information related to the care of a patient is maintained by the patient. This stands in contrast to the more widely used electronic medical record, which is operated by institutions, such as hospitals and contains data entered by clinicians or billing data to support insurance claims. The intention of a PHR is to provide a complete and accurate summary of an individual's medical history which is accessible Online. The health data on a PHR might include patient reported outcome data, lab results, and data from devices such as wireless electronic weighing scales or collected passively from other devices like Hospital's computers. To realize the potential of PHRs and PHR systems to improve health and healthcare, significant steps are needed in the areas of privacy, security. Security is a critical component of a PHR system especially if it is accessible via the Internet. so according to survey of previous systems n health records can conclude that new systems are very well efficient and easy to accessible for patients use. In cloud computing we can combine the lot of technology. The main problem in cloud is security, for that purpose security is required when data is present in cloud. Handling the medical records in cloud is a very complex one. There is the security threat in cloud computing. So overcome the security threat while maintaining the medical records we need to improve the security level of the PHR system in cloud computing. A Survey on Improving the Security of Public Health Record System in Cloud Computing.

A. PHR Solution Types

A] Paper-based PHRs Personal health information is recorded and stored in paper format. Paper-based PHR consist of Printed laboratory reports, Hospital notes, and health data of each individual patient. Cost required is less, access without use of computer. The paper-based PHR is developed in 1980 and used for pregnancy record. It is difficult to update, share with other. Paper-based PHRs are concern to physical loss.

B] Electronic device-based PHRs Personal health information is recorded and saved in personal computer-based software that may have the capability to encrypt, and import data from other authority such as a hospital. PHR software can provide more sophisticated features such as data encryption, data importation, and data sharing with health care providers. Device such as a CD-ROM, DVD, smart card, or USB flash drive used for copying health record.

C] Web-based PHR solutions Web-based PHR solutions are similar electronic device PHR solutions. The advantage of web-based solutions is that it can be easily combine with other services. For e.g. Medical data imported from other sources. Patients allow for data sharing with external authority .

D] Present System In previous systems PHR is available publically. That means anyone can access data without taking any type of permission from patient. Patients don't have any type of control over his records. Technique used now is not reliable and secure because reporting is done by third party companies. In this system PHRs are stored publically no security is there so there are number of resources that can access patients record easily because no privacy and security is there[6]. Resources are from which patient's information can get easily like hospitals, school nurse, specialist doctor, payer data center, primary doctor, lab, pharmacy, LIC policies etc. so these are the resources from which patients data can be misplaced.

VI. CONCLUSION

This system is fully patient-centric concept. Patients have full control of its privacy through encrypting their PHR files to allow particular access to other. The system we has develop is able to cater both statistical reports and ad-hoc reporting in the client- server platform as well as web based platform. Because of cloud Data availability, Data security is more .This system has scalable database as we are using cloud. 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.

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," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[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 Keyword Search 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 Accountability Act," http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp, 2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," 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.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[12] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.

SHAIK SHAHINA is a student of Nimra college of engineering and Technology, Jupudi, NimraNagar, VIJAYAWADA. She is presently pursuing her M.Tech degree from JNTU, Kakinada.She has obtained B.Tech degree from JNTU, Kakinada.

G.MINNI is presently working as Assistant professor in CSE department in Nimra college of Engineering and Technology, Jupudi, Nimra Nagar,VIJAYAWADA. She has obtained M.Tech degree from JNTU, Kakinada. She is pursuing Ph.D., in A.N.U, GUNTUR. She has published several research papers in various national and international Journals. She has more than Ten years of experience in teaching field, her area of interests are networks & Web Designing.

SAYEED YASIN received his M.TECH in Computer Science & Engg from JNTU Hyderabad. He is pursuing Ph.D., in Rayalaseema University, Kurnool. He is currently working as an Associate Professor & Head in Nimra College of Science & Technology the Department of Computers Science and Engineering & Technology, Jupudi, Ibrahimpatnam,Vijayawada-521456. He has more than Eight years of experience in teaching field. His area of interests are wireless networks & programming, & Mobile Computing.