International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 11, November 2014)

Scalable and Securing the e-Health Records

Pottabathula Venu
M.Tech Scholar(CSE)
Sri Indu College of Engg&Tech
Ibrahimpatan, Hyderabad, TS

Konduru Arjun
M.Tech Scholar(CSE)
Sri Indu College of Engg&Tech
Ibrahimpatan, Hyderabad, TS

Juluru Ganesh
M.Tech Scholar(CSE)
Sri Indu College of Engg&Tech
Ibrahimpatan, Hyderabad, TS

K. Anuradha
Associate Professor
Sri Indu College of Engg&Tech
Ibrahimpatan, Hyderabad, TS

Abstract: **PHRs grant patients access to a good vary of health information sources, best medical practices and health knowledge. In patient centrical secure sharing, patients can produce, manage and management their personal health information from one place using the net. Before storing the records in cloud server, they are encrypted victimization cryptography rule that ensures the patient's full management over their PHR. additionally to PHR (Medical history, current exams), personal files, insurance details and sensitive info may also be hold on and shared. Patients only decide that set of users will access that set of files. All the files hold on in clouds that square measure semi-trusted servers are in the encrypted kind and square measure confidential to alternative users. We make use of Attribute primarily based cryptography (ABE) to code the files. In this theme, users square measure categorized into personal and skilled domains that greatly cut back the key management complexness.**
There is a structured thanks to access the files for private and professional functions. Patients square measure ready to dynamically modify the access policy and attributes.

Key words: **Attribute Based Encryption, Cipher, DES, Feistel.**

1. INTRODUCTION

A personal health record (PHR) makes it easy to gather and manage medical information in one accessible and secure location. Carrying paper records is a big drawback, rarely the patients have with them when they need. Personal health record systems overcome this problem by making the personal health record accessible anytime via a Web-enabled device, such as computer. Literally, having a personal health record can be a lifesaver. In an emergency patient can quickly give emergency personal vital information about disease, medications and drug allergies. Now a day, personal health record (PHR) has become a patient-centric model of health information exchange. A PHR service allows patients to create, manage and control their personal health data from one place through the web, which has made the storing, retrieving and sharing of the medical information more efficient. Especially, each patient will have full control of their medical records and can share their health data with different users from different domains which include healthcare providers, family members and friends. Due to high cost of building and maintaining separate data centers, many PHR services are outsourced and provided by third party service providers for example, Microsoft Health Vault (UK). The Health Vault Program of Microsoft will allow users including individuals, health centers, hospitals etc. to gain access to the information on health related issues. The user interface will be simple, that would allow anyone to operate the program easily. But on the other hand, many people do not wish to share their private health records and other information universally through the Health Vault. As the sensitive Personal Health Information (PHI) is highly valuable, the third-party storage servers are the targets of various malicious behaviors which may result in exposure of the PHI. Researches on PHR's using cloud computing is still underway.

The main concern is about whether the patients could actually control the sharing of their sensitive PHR and other information, especially when they are stored on a third-party server which people may not fully trust. To ensure patient-centric privacy control over their own PHRs, encryption of data is necessary prior storage. Basically, the PHR owners themselves should decide how to encrypt their files and to allow which set of users to obtain access to each file. The PHR and other files are available to only those users who are given the corresponding decryption key and are confidential to other users. Furthermore, the patient will always have the right to not only to grant, but also to revoke access rights when it is necessary.

We consider a PHR system where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners' PHRs. The users may come from various aspects; for example, a friend, a caregiver or a researcher. 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. A typical PHR system uses standard data formats.

For example, continuity-of-care (CCR) (based on XML data structure), which is widely used in representative PHR systems including Indivo, an open-source PHR system adopted by Boston Children's Hospital. Due to the nature of XML, the PHR files are logically organized by their categories in a hierarchical way. The main aim of the proposed system 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.

2. LITERATURE SURVEY

A personal health record (PHR) is simply a collection of information about a person's health. It is a tool for the excellent management of the health. J. Benaloh, "Patient

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 11, November 2014)

Controlled Encryption: Ensuring Privacy of Electronic Medical Records," has proposed a scheme in which a file can be uploaded without key distribution and it is highly efficient. But it is a single data owner scenario and thus it is not easy to add categories. C. Dong, "Shared and Searchable Encrypted Data for Untrusted Servers," has explored that the data encryption scheme does not require a trusted data server. The server can perform encrypted searches and updates on encrypted data without knowing the plaintext or the decryption keys. But in this scheme the server knows the access pattern of the users which allows it to infer some information about the queries.

A. Boldyreva, V.Goyal, and V. Kumar, "Identity-Based Encryption With Efficient Revocation," and X. Liang, R, "Ciphertext Policy Attribute Based Encryption With Efficient Revocation," resolved 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 but does not achieve complete backward/ forward security and is less efficient.

Recently J. Hur and D. K. Noh in "Attribute-Based Revocation in Data Outsourcing Systems," and S. Jahid, P. Mittal, and N. Borisov in, "Easier: Encryption-Based Access Control in Social Networks With Efficient Revocation," proposed two CPABE schemes with immediate attribute revocation capability, instead of periodical revocation. However, they were not designed for Multi Authority Attribute Based Encryption (MAABE).

S. Ruj, A. Nayak, and I. Stojmenovic in, "DACC: Distributed Access Control in Clouds," proposed an alternative solution for the same problem. The main advantage of the solution is each user can obtain secret keys from any subset of the Trusted Authorities (TAs) in the system. On the downside, the communication overhead of key revocation is still high, as it requires a data owner to transmit an updated ciphertext component to every non-revoked user.

M. Li, S. Yu, N. Cao and W. Lou in [3], "Authorized Private Keyword Search Over Encrypted Personal Health Records in Cloud Computing," address the problem of authorized private keyword searches over encrypted data in cloud computing, where multiple data owners encrypt their records along with a keyword index to allow searches by multiple users. The main advantage of schemes in this category is they obviate the overhead for users to acquire search capabilities. However, search authorization is intrinsically difficult to achieve since it is contradictory with user-generated capabilities.

Although there exist healthcare regulations such as Health Insurance Portability and Accountability Act (HIPAA) in United States 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.

3. EXISTING SYSTEM

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 on their personal health data, which makes it necessary for each patient to encrypt their 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. Disadvantages of Existing System: There is no policy management for file access, so that unauthorized users can also able to access the sensitive data. There is no encryption and decryption concept so the files stored in the semi-trusted cloud can able to leak the information to others. There is no structured way to access the file for personal & professional purpose.

4. PROPOSED SYSTEM

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. 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 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. Advantages of Proposed System are: There is policy management for file access, data access member can able to access the files which they have rights set by the policy. Files stored in the semi-trusted cloud are in encrypted form and there is no chance of others to view the file content. There is a structured way to access the file for personal & professional purpose through attribute policies and attribute based encryption and decryption.

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 11, November 2014)

5. ANALYSIS

Software Requirements Specification plays an important role in creating quality software solutions. Specification is basically a representation process. Requirements are represented in a manner that ultimately leads to successful software implementation.

Feasibility Study: Feasibility Study is a high level capsule version of the entire process intended to answer a number of questions like: What is the problem? Is there any feasible solution to the given problem? Is the problem even worth solving? Feasibility study is conducted once the problem clearly understood. Feasibility study is necessary to determine that the proposed system is Feasible by considering the technical, Operational, and Economical factors. By having a detailed feasibility study the management will have a clear-cut view of the proposed system.

The following feasibilities are considered for the project in order to ensure that the project is variable and it does not have any major obstructions. Feasibility study encompasses the following things:

- Technical Feasibility
- Economical Feasibility
- Operational Feasibility

In this phase, we study the feasibility of all proposed systems, and pick the best feasible solution for the problem. The feasibility is studied based on three main factors as follows.

6. DESIGN

Design is a meaningful engineering representation of something that is to be built. Software design is a process through which the requirements are translated into a representation of the software. Design is the place where quality is fostered in software engineering. Design is the perfect way to accurately translate a customer's requirement in to a finished software product. Design creates a representation or model, provides detail about software data structure, architecture, interfaces and components that are necessary to implement a system. This chapter discusses about the design part of the project. Here in this document the various UML diagrams that are used for the implementation of the project are discussed.

Design Principle: The Unified Modeling Language (UML) is a visual modeling language used to specify, visualize, construct and document a software intensive system. The embedded real-time software systems encountered in applications such as telecommunications, school systems, aerospace, and defense typically tends to be large and extremely complex. It is crucial in such systems that the software is designed with a sound architecture. A good architecture not only simplifies construction of the initial system, but also, readily accommodates changes forced by a steady stream of new requirements.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects. Using the UML helps project teams communicate, explore potential designs, and validate the architectural design of the software.

The primary goals in the design of the UML are: Provide users with a ready-to-use, expressive visual modeling language so they can develop and exchange meaningful models. Provide extensibility and specialization mechanisms to extend the core concepts. Be independent of particular programming languages and development processes. Provide a formal basis for understanding the modeling language. Encourage the growth of the OO tools market. Support higher-level development concepts such as collaborations, frameworks, patterns and components. Integrate best practices.

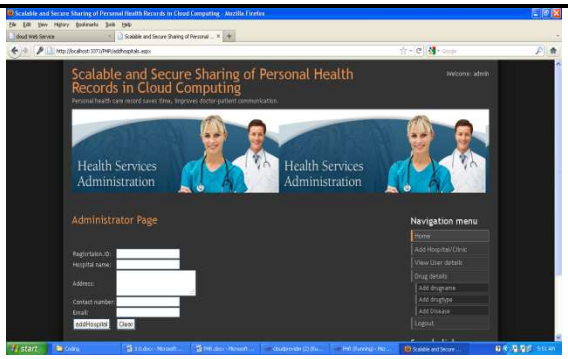
7. IMPLEMENTATION & RESULTS

The most crucial phase of any project is the implementation. This includes all those activities that take place to convert from the old system to the new system. It involves setting up of the system for use by the concerned end user. A successful implementation involves a high level of interaction between the analyst, programmers and the end user. The most common method of implementation is the phased approach, which involves installation of the system concurrently with the existing system. This has its advantage in that the normal activity carried out, as part of the existing system is anyway hampered. The end users are provided with sufficient documentation and adequate training in the form of demonstration/presentation in order to familiarize with the system.

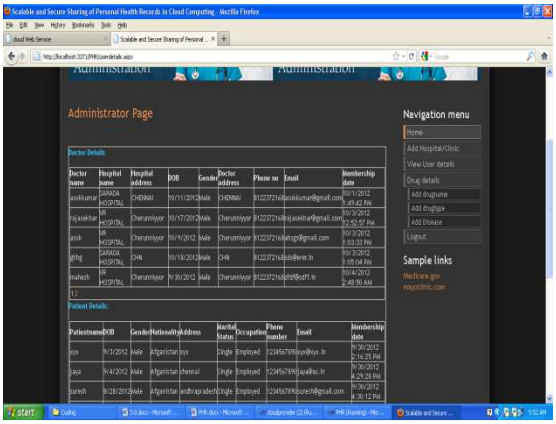
SS 1: Home Page

SS 2: Admin Login

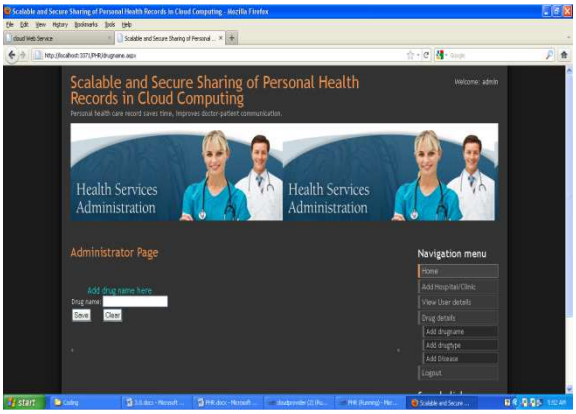
International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 11, November 2014)



SS 3 :Admin Home Page

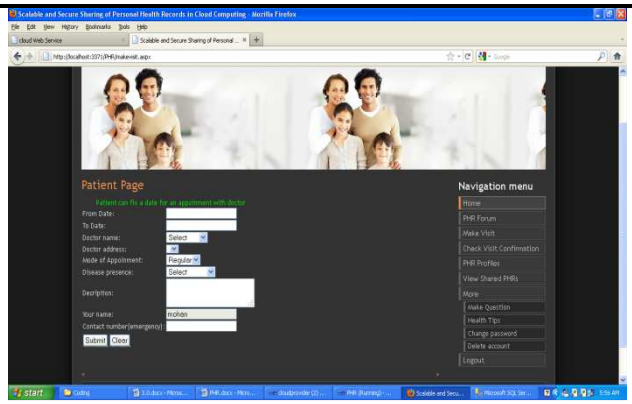


SS 4:View user details Page

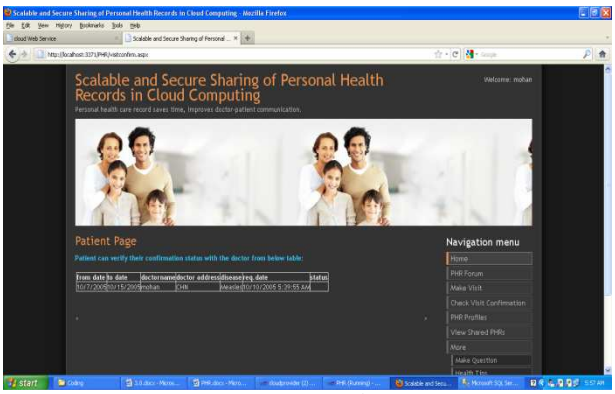


SS 5: Add drug page

SS 6: Patient home page



SS 7: Make visit



SS 8: Check visit confirmation

8. 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] 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," in SecureComm'10, Sept. 2010, pp. 89–106.

[2] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.
[4] "The health insurance portability and accountability act." [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp
[5] "Google, microsoft say hipaa stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.
[6] "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
[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, p. 283, Feb. 2001.
[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114.