Secure and Scalable Sharing of Personal Health Record in Cloud Using ABE

Prabhakar Singh
Shri Shankaracharya Technical Campus
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
yadavprabhakar89@gmail.com

Prof. Samta Gajbhiye
Shri Shankaracharya Technical Campus
Dept. of Computer Science and Engineering
Bhilai, Chhattisgarh, India
samta.gajbhiye@gmail.com

Abstract

Personal health record (PHR) is a developing patient-driven model of health data trade, which is frequently outsourced to be put away at an outsider, for example, cloud suppliers. Be that as it may, there have been wide security worries as personal health data could be presented to those outsider servers and to unapproved parties. To guarantee the patients' control over access to their own particular PHRs, it is a promising strategy to scramble the PHRs before outsourcing. However, issues, for example, dangers of protection presentation, adaptability in key administration, adaptable access, and productive client disavowal, have remained the most imperative difficulties toward accomplishing fine-grained, cryptographically authorized information get to control. In this paper, we propose a novel patient-driven system and a suite of components for information get to control to PHRs put away in semi trusted servers.

Keywords**—** *PHR, Cloud, Encryption, Personal Health Record, Hospital, Patients.*

I. INTRODUCTION

Electronic health care system is a promising innovation that has drawn broad consideration from both scholarly community and industry as of late [6]. It portrays the utilization of data and correspondence advancements over the entire scope of capacity that influence the PHI. The eHealth system demonstrates a high potential to enhance the nature of analysis, lessen medicinal expenses and help address the dependable and on-request health care challenges postured by the maturing society. Late advances in Wireless Body Area Networks (WBANs) have made it conceivable to send bio-sensors on, in, or around the patient body and permit to ceaseless checking of physiological parameters (e.g., electrocardiogram (ECG), blood oxygen levels) with physical exercises [7,8,9]. It has loaned incredible powers to the movement of health care system from doctor's facility or care unit to the patient's habitation.

Incorporating this innovation with the current remote advancements allows constant portable and perpetual checking of patients, notwithstanding amid their day by day ordinary exercises. In such a heterogeneous remote condition, secure correspondence of the patient PHI with respectability and classification is a fundamental piece of a solid eHealth care system.

Electronic health care system is a promising innovation that has drwan broad consideration from both scholarly world and industry as of late. It portrays the utilization of data and correspondence advances over the entire scope of capacity that influence the PHI. The eHealth system demonstrates a high potential to enhance the nature of determination, diminish therapeutic expenses and help address the solid and on-request health care challenges postured by the maturing society. Late advances in Wireless Body Area Networks (WBANs) have made it conceivable to send bio-sensors on, in, or around the patient body and permit to consistent observing of physiological parameters (e.g., electrocardiogram (ECG), blood oxygen levels) with physical exercises.

It has loaned extraordinary powers to the relocation of health care system from doctor's facility or care unit to the patient's living arrangement. Coordinating this innovation with the current remote advances allows continuous versatile and changeless observing of patients, notwithstanding amid their day by day ordinary exercises. In such a heterogeneous remote condition, secure correspondence of the patient PHI with honesty and classification is a fundamental piece of a solid eHealth care system [10, 11].

What's more, the eHealth care system needs to guarantee the accessibility of PHI in electronic shape sticks to an indistinguishable levels of protection and revelation strategy from appropriate to display day paper-based patient-records available just from the doctor's office. Rather than putting away the PHI locally, the current headway of distributed computing enables us to store all PHI midway and guarantees accessibility with decreases the capital and operational consumptions. Moving patients PHI into a cloud or in a focal stockpiling offers gigantic accommodations to the eHealth care suppliers, since they don't need to care about the complexities of direct equipment administration [14]. Notwithstanding, patient's protection with appropriate access control of this accessible PHI is a developing worry in the eHealth care industry because of its immediate association to human [12, 13].

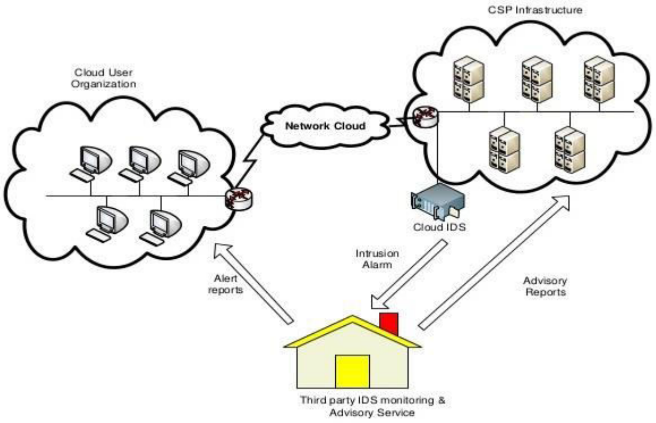


Fig.1. shows the architecture of PHR system

II. LITERATURE SURVEY

Mrinmoy Bar et. al [1], Author propose an efficient and secure patient-centric access control (PEACE) scheme for the emerging electronic health care (eHealth) system. In order to assure the privacy of patient personal health information (PHI), we define different access privileges to data requesters according to their roles, and then assign different attribute sets to the data requesters. By using these different sets of attribute, we construct the patient-centric access policies of patient PHI. The PEACE scheme can guarantee PHI integrity and confidentiality by adopting digital signature and pseudo-identity techniques. It encompasses identity based cryptography to aggregate remote patient PHI securely. Extensive security and performance analyses demonstrate that the PEACE scheme is able to achieve desired security requirements at the cost of an acceptable communication delay.

Luan Ibraimi et. al [2], Here author describe a new approach which enables secure storage and controlled sharing of patient's health records in the aforementioned scenarios. A new variant of a ciphertext-policy attribute-based encryption scheme is proposed to enforce patient/organizational access control policies such that everyone can download the encrypted data but only authorized users from the social domain (e.g. family, friends, or fellow patients) or authorized users from the professional domain (e.g. doctors or nurses) are allowed to decrypt it.

Shucheng Yu et. al. [3], addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in finegrained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

Melissa Chase et. al [4], In this paper, author propose a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice.

Vipul Goyal et. al [5], As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for flne-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

.

III. METHODOLOGY

In this section the proposed methodology is discussed in details. The proposed workflow is presented in fig. 2. It consists of several different modules.

a. Doctor Modules

b. Patient Details

c. Cloud Server

d. Patient Access

e. Remote User

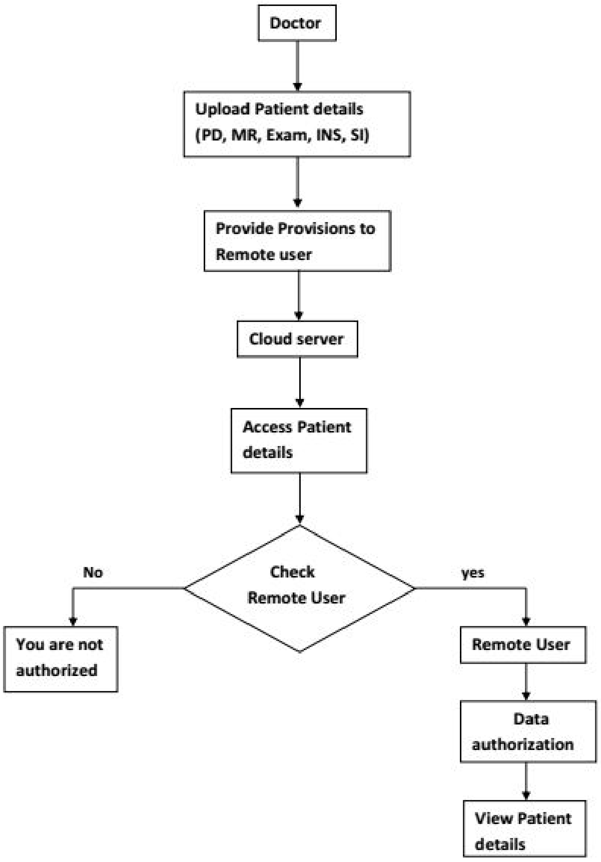


Fig. 2. Proposed workflow

A. Doctor Module

The doctor in PHR is responsible for entering patient details and modifying the details.

B. Patient Details

The patient details are modified and filled either by the doctor or by the data entry operators in the hospitals. The details of patient such as:

- Personal Details
- Medical Record
- Examination
- Insurance Details
- Sensitive Information

C. Cloud Server

Cloud server is the area where all the details of the patients are stores and accessed. It is semi trusted server that's why the hospital cannot totally trust over the cloud storage. It might got stolen or tempered.

D. Patient Access

The Patient relatives are given username and password foer accessing the patient details. It is invoked on demand by the relatives.

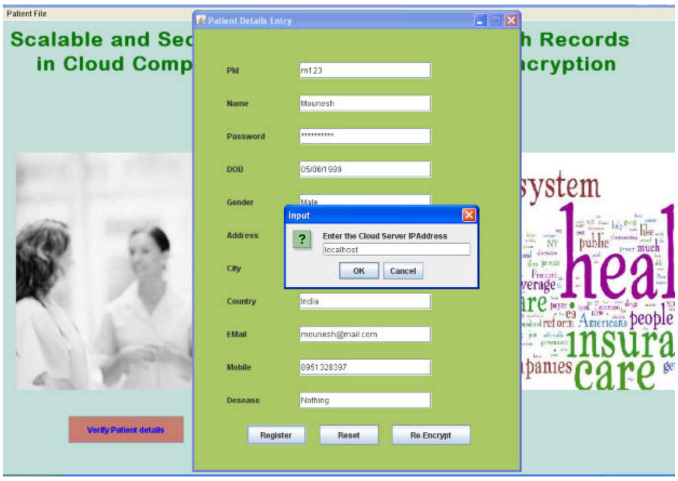
E. Remote User

The Remote user can connect to the cloud server and can request for the patient details. Its request are granted by the doctor.

IV. RESULTS

This section deals with the various outcomes of the cloud based security of patients.

The screenshot experiments are showed in below figures.


Patient File

Scalable and Sec h Records
in Cloud Comp ncryption

Patient Details Entry

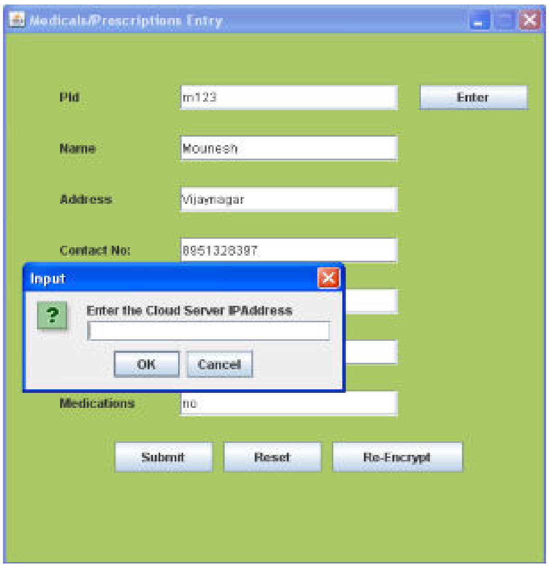
PId	m123
Name	Mounesh
Password	**********
DOB	05/06/1989
Gender	Male
Address	
City	
Country	India
EMail	mounesh@mail.com
Mobile	8951328397
Desease	Nothing

Input

Enter the Cloud Server IPAddress

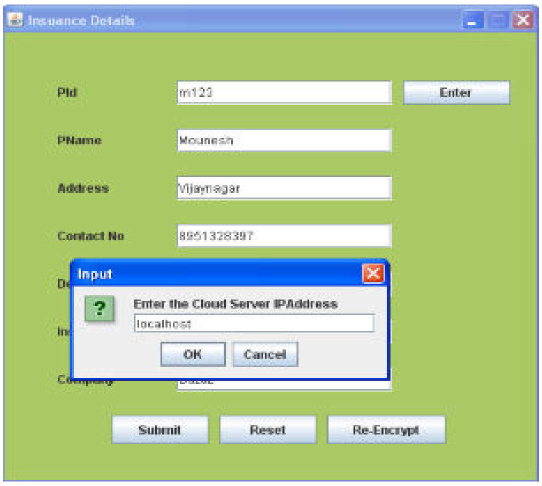
localhost

Fig. 3. Shows the Patient Details Registration



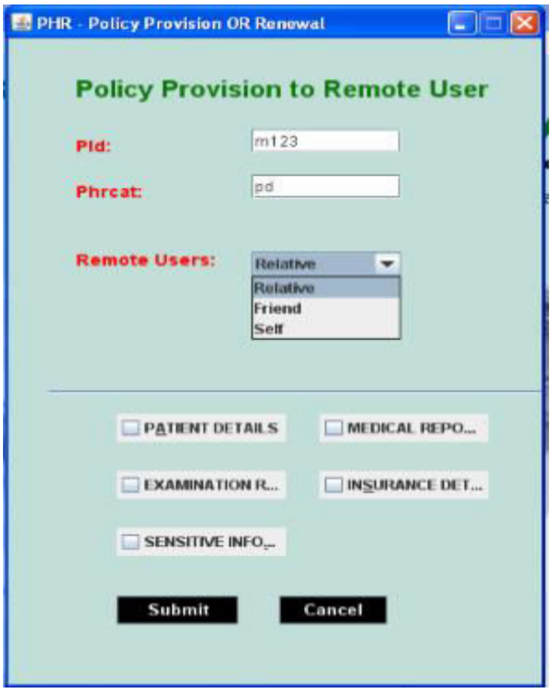
Pid: m123
Name: Mounesh
Address: Vijaynagar
Contact No: 8951328397
Medications: no
Enter the Cloud Server IPAddress

Fig. 4. Shows the Medical Prescription Details



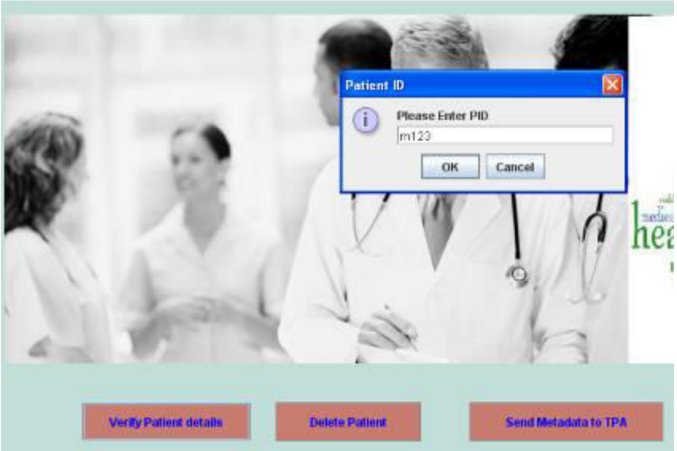
Pid: m123
PName: Mounesh
Address: Vijaynagar
Contact No: 8951328397
Enter the Cloud Server IPAddress: localhost

Fig. 5. Shows the Insurance Details


PHR - Policy Provision OR Renewal
Policy Provision to Remote User
Relative
Friend
Self
Submit
Cancel

Pid: m123
Phrcat: pd
Remote Users: Relative
□ PATIENT DETAILS
□ MEDICAL REPO...
□ EXAMINATION R...
□ INSURANCE DET...
□ SENSITIVE INFO...

Fig. 6. Shows the Policy Provisioning of Patient Detials



Please Enter PID: m123

Fig. 7. Verifying and Sending Metadata to TPA

- In this module the system first defines a common universe of data attributes shared by every PSD (Personal Domain), such as “basic profile”, “medical history”, “allergies”, and “prescriptions”. An emergency attribute is also defined for break-glass access.
- Each PHR owner’s client application generates its corresponding public/master keys. The public keys can be published via user’s profile in an online healthcare social-network (HSN). There are two ways for distributing secret keys.
- First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in GoogleDoc.
- Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, and the owner will grant her a subset of requested data types.

V. CONCLUSION

In this paper, we have proposed a novel structure of secure sharing of personal health records in distributed computing. Considering somewhat reliable cloud servers, we contend that to completely understand the patient-driven idea, patients should have finish control of their own security through encoding their PHR documents to permit fine-grained get to.

The structure tends to the interesting difficulties brought by numerous PHR proprietors and clients, in that we significantly lessen the multifaceted nature of key administration while upgrade the protection ensures contrasted and past works. We use ABE to scramble the PHR information, so patients can permit get to by personal clients, as well as different clients from open areas with various expert parts, capabilities, and affiliations.

REFERENCES

[1] M. Barua, X. Liang, R. Lu and X. Shen, "PEACE: An efficient and secure patient-centric access control scheme for eHealth care system," 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Shanghai, 2011, pp. 970-975.

[2] L. Ibraimi, M. Asim and M. Petković, "Secure management of personal health records by applying attribute-based encryption," Proceedings of the 6th International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health, 0slo, 2009, pp. 71-74.

[3] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," 2010 Proceedings IEEE INFOCOM, San Diego, CA, 2010, pp. 1-9.

[4] J. Han, W. Susilo, Y. Mu, J. Zhou and M. H. A. Au, "Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 665-678, March 2015.

[5] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. 2006. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA, 89-98.

[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.

[13] A. Boldyreva, V. Goyal, and V. Kumar, “Identity-Based Encryption with Efficient Revocation,” Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[14] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes,” 2009.