ISSN No: - 2456- 2165

Different Methodologies Review for Secure Personal Health Record

Priyanka Bansal
Apex Institute of Engineering & Technology,
Jaipur, Rajasthan, India

Mohit Saxena
Apex Institute of Engineering & Technology,
Jaipur, Rajasthan, India

Abstract: - Personal health record is sustained in the centralize server to preserve patient's personal and diagnosis data. Personal health record (PHR) is a future patient-centric model of health data commutation, which is frequently outsourced to be stored at a third party, specified as cloud suppliers. However, there have been broad secrecy concerns as personal health information could be open to those third party servers and to unauthorized parties. The security systems are applied to protect personal information from public access. To secure the patients' control over access to their own PHRs, it is a promising technique to encode the PHRs before outsourcing. In this paper we are giving some methods review for the security of the information from the external attacks.

Keywords: *Attribute-based encryption, cloud computing, data privacy, fine-grained access control, Personal health records, revocation.*

I. INTRODUCTION

PHR is a service in which patient can manage , generate and control the heath records through a web service . This service make the connection in sharing the information , retrieval more securely and efficiently . In this service , patient have full authority to control , share to the PHR data from the family members and friends . Due to the high coast for building & management of data centers , commonly PHR services transferred to the third party e.g Microsoft Health vault. For recent storage of PHR data in cloud computing is given in [1][2].

The PHR data get stored in the third Party server so authorized person can share and check the PHR data of patient . So the main concern is, patient can control the sharing of the PHI(Personal Health Record) with the relevant person. Before outsourcing the PHR data, an individual approach is using for encrypting the data. The patient can self-decide that how to encrypt the PHR file. Corresponding that PHR data will be received only for that relevant person who have decryption key for the decryption.

The term "PHR" has been applied to both paper-based and computerized systems; current usage usually implies an electronic application used to collect and store health data. In recent years, several formal definitions of the term have been proposed by various organizations[3][4][5]. It is important to note that PHRs are not the same as electronic health records (EHRs). The latter are software systems designed for use by health care providers. Like the data recorded in paper-based medical records, the data in EHRs are legally mandated notes on the care provided by clinicians to patients. There is no legal mandate that compels a consumer or patient to store her personal health information in a PHR.
PHRs can contain a diverse range of data. These are :

- Allergies and Adverse Drug Reactions
- Chronic Diseases
- Family History
- Illnesses and Hospitalizations
- Imaging Reports (e.g. X-ray)
- Laboratory Test Results
- Medications and Dosing
- Prescription Record
- Surgeries and Other Procedures
- Vaccinations
- Observations of Daily Living (ODLs)

There are two methods by which data can arrive in a PHR[1]. A patient may enter it directly, either by typing into fields or uploading/transmitting data from a file or another website. The second is when the PHR is tethered to an electronic health record, which automatically updates the PHR. Not all PHRs have the same capabilities, and individual PHRs may support one or all of these methods[1].

In addition to storing an individual's personal health information, some PHRs provide added-value services such as drug-drug interaction checking, electronic messaging between patients and providers, managing appointments, and reminders[5].

ISSN No: - 2456- 2165

A. Benefits

PHRs grant patients access to a wide range of health information sources, best medical practices and health knowledge. All of an individual's medical records are stored in one place instead of paper-based files in various doctors' offices. Upon encountering a medical condition, a patient's health information is only a few clicks away.

Moreover, PHRs can benefit clinicians. PHRs offer patients the opportunity to submit their data to their clinicians' EHRs. This helps clinicians make better treatment decisions by providing more continuous data[1].

PHRs have the potential to help analyze an individual's health profile and identify health threats and improvement opportunities based on an analysis of drug interaction, current best medical practices, gaps in current medical care plans, and identification of medical errors. Patient illnesses can be tracked in conjunction with healthcare providers and early interventions can be promoted upon encountering deviation of health status. PHRs also make it easier for clinicians to care for their patients by facilitating continuous communication as opposed to episodic. Eliminating communication barriers and allowing documentation flow between patients and clinicians in a timely fashion can save time consumed by face-to-face meetings and telephone communication. Improved communication can also ease the process for patients and caregivers to ask questions, to set up appointments, to request refills and referrals, and to report problems. Additionally, in the case of an emergency a PHR can quickly provide critical information to proper diagnosis or treatment.

II. LITERATURE REVIEW

In 2014 RaseenaM [et.al] presented a paper for Personal Health Record (PHR) service, a method that allows patients share their medical information with other family and friends, as well as health care providers. Generally, PHR data is hosted to the third party service providers for interoperability and accessibility. However, this convenience poses serious security and privacy challenges as data is stored in third party servers mostly in cloud storage.To improve on security, the data is encrypted before storing in third party servers. Still many issues such as risk of privacy, scalability in encryption key management, and organized user access and revocation, are persistent. This pose as a challenge in achieving fine-grained, cryptographically enforced data access control. In order to achieve this, the paper proposes a novel patient-centric framework. The framework is based on multiple data owner scenario, instead of commonly used single owner scenario. In this framework, a high degree of privacy is assured by using multi authority attribute based encryption (ABE). ABE allows dynamic modification of access policies or file attributes, and on demand user/attribute revocation. Though ABE is promising, it does not efficiently handle workflow based control scenario, which is based on users' identity rather than attribute. To overcome these issues, this paper proposes an Attribute Based Broadcast Encryption (ABBE) [1].

In 2015 KanchanHadawale[et.al]presented a paper for Personal health record (PHR). With PHR is patient's personal and diagnosis information is managed, and is stored at a third party service providers, mostly in Cloud. With PHR, patient manages and creates her own health record and control the sharing of it. By the very nature, PHR poses high security and privacy risks. This advocates for PHR to be rightfully protected and secured, so that the patient's personal health information (PHI) from unauthorized users. Such protection scheme is easier said than done, as it is the patient who has control over access to their own PHR. This paper focuses on PHR, and outlines the security, and privacy aspects of PHR. This paper suggests ABE, and looks into the benefits, such as scalable key management, multiple data owners, and protection against unauthorized access. It emphasizes that that multiple data owners can access same type of patients' data from third party servers and guarantees high degree of privacy. [2]

In 2013 Susheel R. Deshmukh[et.al] presented a paper for healthcare industry which is rapidly growing its digital world pushing for an increase in need for online exchange of medical data among healthcare providers. A personal healthcare record (PHR) is a patient-driven model for such an exchange of healthcare information. In this method, the patient holds the access and coordinates personal healthcare information (PHI) and shares this information with healthcare providers, family and friends. For better interoperability, PHR is hosted by third party storage service providers, mostly in Cloud. However, outsourcing patient PHR to storage servers pose major privacy concerns, and they are not covered entities under HIPAA. This has led to increasing number of security attacks in recent years. As a common practice, patient encrypts PHR before storing it thus guarantees the patients' control over access to their own PHR. The main challenge with encryption is that it does not offer granularity and it is not scalable solution. To achieve granular and scalable data access control for PHR, an attribute based encryption (ABE) is proposed in the paper. ABE provide more scalable and interoperable options for better access to information between the different healthcare entities. ABE supports more efficient and on-demand revocation of users/attribute, and emergency access in critical scenarios [3].

In 2014 Mr.Prasad P S[et.al] presented a paper for Personal health record (PHR). With PHR is patient's personal and diagnosis information is managed, and is stored at a third party service providers, mostly in Cloud. This comes with the cost of exposing personal health information (PHI) to third party servers and to unauthorized parties. Encryption of PHR before being storage in third party server is a method

ISSN No: - 2456- 2165

commonly used, which assures the patients' control over approach to her PHR. However, encryption does not mitigate the risks of privacy exposure and poses key management challenges as we scale up the model. Encryption also lacks the flexible access control and is not efficient in user revocation. This calls for an improved method in accomplishing fine-grained and cryptographically imposed data access control. This is an improvisation without affecting the core functionality of the patient to have good control over accessibility and distribution to her PHR. In order to have control for data access to PHRs stored in semi trusted severs, this paper proposes a novel structure of providing a wholesome solution for PHR and at the same time retaining the patient-centric aspects of PHR. It proposes to leverage attribute-based encryption (ABE) practices to achieve scalable and granular data access control for PHR. In this paper, the author concentrates on the multiple data owner scenario, which is different from commonly used method of using encryption in secure data storage. ABE allows using multiple data owner scenario, by this it divides the users in the PHR system into several security domains. Such segregated module of security domains decreases the key management complexity for owners and users, when the system is scaled up in growth. Along with multiple security domains, ABE offers benefits of patient confidentiality and guarantees multi authority ABE. This method is immensely helpful in an emergency scenario, ABE scheme provides break-glass access to dynamic change of access policies or file attribute, and supports on-demand user/attribute revocation. Intense analytical and test results show improved security, scalability, and efficiency of with this ABE scheme [4].

In 2013 Priyanka Korde[et.al]presented a paper for the design and implementation of Personal Health Records (PHR). PHR is online application that enables people to access and manage their personal health information (PHI). The patients have control over access to PHI. Since the data is stored online in third party servers, security need to be implemented. This is achieved by using the attribute based encryption (ABE) to encrypt the data before move it online. With ABE, uses multiple owner scenarios and keeps the PHR in multiple security domains. This reduces the overhead associated with key management for owners and users. ABE also promises a high degree of privacy for patients' records. This ABE scheme gives PHR owner with full control of data. Performance and security analysis tests conducted with ABE shows that the scheme is highly efficient [5].

Paper Write	Year	Methodology	Description
Raseena M[et.al][1]	2014	Secure Sharing of Health monitoring by ABE(attribute Based Encryption)	ABE algorithm is describe for ABE encryption
Kanchan Hadawale[et.al] [2]	2015	Secure Sharing of Health monitoring by ABE(attribute Based Encryption)	Paper is working for ABE health monitoring based algorithm.
Susheel R. Deshmukh[3]	2013	Attribute based Encryption for personal Health monitoring	Results are showing in terms of time for Key generation
Mr.Prasad P S [4]	2014	ABE encryption based Health Monitoring	They show flow chart for the PHR(Personal Health Record) by use ABE(Attribute based Encryption)
PriyankaKorde[et .al] [5]	2013	ABE, AES and MD5 cryptographic based health monitoring	In this paper , they describe the algorithm of the ABE , AES(Advanced Encryption Standard) and MD5 cryptographic algorithm for show the security .

Table 1. Review of Different Papers

ArpanaMahajan et al. (2012) reviewed the safe access to this new, promising model of health information exchange, the PHR which is focused on the patients. For storing of this data, however, subcontractors are commonly employed, and to guarantee the patients' power over entry to their own PHRs, it is therefore a good idea to encode the PHRs prior to

subcontracting. In this review paper, they offer a new patient-focused agenda and a horde of machinations to manage access to data of the PHRs kept in halfway reliable servers. They also propose attribute-based-encryption (ABE) techniques to codify individual PHRs as a means to obtain finely encrypted and flexible data access management for the PHR's. They concentrate on having a multitude of data holders, and separate the PHR users into several security fields and this diminishes the difficulty significantly in the main organization for both owners and users. Moreover, this allows the active changing of access procedures or of file characteristics and backs up capable on-demand user/attribute cancellation and break-glass entry if urgent [6].

III. CONCLUSION

The PHRs are taken as unfolded tradition in the field of exchanging personal health information. And further cloud computing storage & sharing services are used by users over a very high pace. In this paper we, give the Review of the different papers for Person Health Record.

References

[1]. Raseena M, Harikrishnan G R," Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Broadcast Encryption", in International Journal of Computer Applications (0975 8887) Volume 102 - No. 16, September 2014.

[2]. KanchanHadawale, NikamManoj B1, KadamJayesh D2, Salgar Vijay L3, GhogareSagar R," Scalable and Secure Sharing of Personal Health Records in centralized Database Using Attributebased encryption", in International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2015.

[3]. Susheel R. Deshmukh," Attribute-Based Encryption And Interoperability Of Personal Health Records In Cloud Computing ", in International Journal of Recent Advances in Engineering & Technology (IJRAET), Volume-1, Issue - 2, 2013.

[4]. Mr.Prasad P S, Dr. G F Ali Ahammed, "Attribute-Based Encryption for Scalable and Secure Sharing of Personal Health Records in Cloud Computing", in (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014.

[5]. Priyanka Korde, Vijay Panwar, Sneha Kalse," Securing Personal Health Records in Cloud using Attribute Based Encryption ", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[6]. Arpana Mahajan, Yask Patel," Enhancing PHR services in cloud computing: Patient-centric and fine grianed data access using ABE",*IRACST* - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.6, December 2012.