Privacy Over PHR Using Attribute Based Encrtption

Akshaya Prarthana Selvaraj[1]
[1]Student
[1]Computer Science & Engineering Department
[1]Saveetha School Of Engineering

Abstract--- (PHR) Personal Health Record is often used in the information and data exchange, on the basis of storing the data such as the cloud providers. The threat is that these data's that are stored can be exposed to the third party or the unauthorized party. In order to ensure the control over the patient data, a promising encryption method is being followed. Yet, the flexible access and efficient user have remained the most important and challenging enforced data access control over the PHR. In this paper, we propose attribute based encryption over the patient data's by encrypting. In this, we focus on the multiple data owner scenario, and divide the users and also provide the multiple security domains that help in reducing the complexity for the owners and users. In we also use Pseudo random code algorithm for giving different id for the patient .As a part of security the data is protected by blocking the user if the user attempts a failure to login the id twice, the user will henceforth will not be allowed to login again with the same network. Thus security, scalability and efficiency of our proposed scheme also has the random code algorithm which blocks the third party access over the data and provide full privacy of the patient's personal health record.

Keyword: Personal health record, Attribute based encryption, Pseudo-Random code algorithm, Blocking, Cloud storage, Data privacy.

I. INTRODUCTION

Personal health record (PHR) has been a patient-centric model of health information and data exchange according to the recent year. This provides the control over the data of patient by storing the data and retrieving the info from the storage data base (PHR). This storage data is cloud storage. Even though the patient has the full control over the (PHR) they give the right or the authority to the consulting doctors, admin and family members to access the data even if the patient is off-line [1]. As the result the data's are access-able to all the viewers and thus they can retrieve the info about the patient details very easily ,so the data a be miss-used easily[2].This made us to adopt a new idea .This is to provide the security to the patients details and privacy for the data that is stored in the (PHR)[3] .Now, HIPAA becomes the major concept in this personal health record(PHR) [4].As of now the (PHR) is being used in many hospital but with the threat that the data can be used in the wrong way. Anyone who gets logged in to the website can be able to view all the details about the patients not only the data and also the medical concerns[5].This is the major problem faced by the patients and also the hospital i.e. the security over the data is very complex.

A patient-centric privacy control over their own PHR, it is essential to work with-in the semi-trusted server by providing the security feasible and promising and appropriate way to protect the is to encrypt the data before outsourcing (PHR)[6]. A patient who has the authority to operate the (PHR) has the access to change the setting in-order to have the privacy over the patients data (PHR)and give the accessibility to the specific people that the patient want to share[7].

The conflict between the patient-centric mode and the scalable becomes the major problem. This give raise to the scalable and secure sharing of data's from patient to the doctors and vice-versa.

Though it is a very huge process the storage is out sourced to the third party which again becomes a major problem .Thus the patient self has the authority to control and access and manage the data that is stored using the key management. Even with the secure key management the data is not fully protected as the patient is not always online .So, each owner encrypt the key in their own way in-order to enter in to the login of the user. Once the patient wants to limit the accessibility of the data only to the people this becomes the major draw-back in the previous paper. However the key management and the attribute based encryption is done the security becomes the major problem that let each user obtain keys from every owner. An alternative method to secure the data is to focus on how to have a central authority (CA) with the key management of all PHR owners, but this requires trust on a single authority (i.e., key escrow problem). In this paper, we propose an innovative idea of securing the data by protecting the data by using the attribute based encryption (ABE) with the random code algorithm. The main idea behind this is to not only provide security but also block the other users when they try to login the data without the patient permission. This also provide a selective user to enter in to the patient data .

Both the encryption and the decryption is done in this paper so that not all the users can login for the (PHR) unless the patient is willing to share the data. This is not only implemented in the small storage but also in the large storage.

Thus this provides the secure, dynamic, scalable implementation of (PHR).

Thus we contribute the ideas by implementing:

1. We propose a secure idea in sharing the data from the patient to the doctor because there are many challenging problems that occur during the transfer of data's. Since we are storing the data in the cloud storage the data can be retrieved from the cloud by the unknown user. Thus the data can be miss-used. In order to protect the data from the third party user we use (ABE) attribute based encryption. This attribute based encryption will encrypt the data once by hiding the patient detail.
2. In the recent papers the sharing of patient data is being done only with-in the same hospital For instance Apollo is a hospital where the patient details are stored .These details can be retrieved only with-in Apollo in any of the branch. But ,we have implemented an idea of

sharing the data not only with-in same server but also different server .i.e., the details of the patient in the Apollo hospital can be viewed by other hospital doctors(MIOT) when required.

3. Sharing the data not only in the same server but also different server has to face the security challenges. So, we encrypt the data again in order to share the details between the server. This encryption over the data will provide a secure sharing of details so that the third party access will not be 6allowed .This is done using the attribute based encryption. This will encrypt the detail so that the data cannot be viewed by others and will be secure
4. The patient can give the authority to family members to view the details whom the patient feel secure .The patient can choose to share the details with the family members if the patient wish to give the id and the password. There is an option of choosing the people whom the patient wants to give the id and the password.
5. In-spite of all this security there are possibilities that the third party access may still occur by giving the continuous id in the login page .In order to protect the patient details we use Pseudo-random code algorithm where the each patient will get the id in a random method. So, that the third party user cannot enter the login page, by just typing the id to view other patient details. Pseudo random code algorithm provides the security to the patient detail by not allowing the other user to login.
6. This paper also gives security by blocking the user when he/she tries to enter the login page without the permission of the patient. When the other user tries to login the page and put wrong id and password thrice the login page will automatically get closed and henceforth will not allow that user to get in the login page. This will automatically block the ip-address so that the person cannot enter in to the login page again in the same ip-address.
7. This paper is also done using the HMAC MD5 and ABE attribute based encryption with the M-ABE multiple -attribute based encryption in order to give the privacy over the data

II. Related Works

The recent works of the paper has the data privacy over attribute based encryption and fine grain access control and public key encryption and key management using different keys with different user. Each user had their own way to encrypt the key to view the details of the patient.

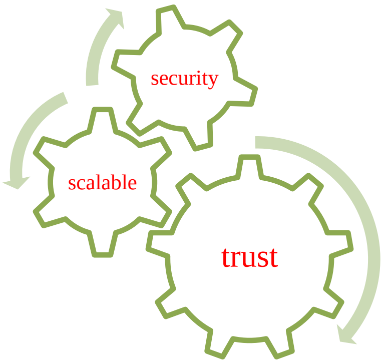

Fig. 1:

So, different user encrypted the key in their own ways .This gave raise to many security issues. Security over the detail of the patient was difficult .Though the attribute based encryption was used the security was the problem because the data was outsourced to the third party.

III. ABE (Attribute Based Encryption)

Recent number of works is done using attribute based encryption especially in the (EHR) electronic health records. The attribute based encryption is used here on the basis of providing security over the patient details. In ABE the details of the patient is first logged in and the data is been encrypted once so the data of the patient can be viewed only by the patient and the doctor. If the third party user wants to view the details of the patient the data will be in the form of encrypted way so that the third party user cannot understand the way in which the data is encrypted. This provides the direct revocation over the data. The following process of encryption not only happens in the EHR but also in the PHR (PERSONAL HEALTH RECORD).

This approach of using attribute based encryption is done by encrypting the key .each user will encrypt the key in their own way such data each encryption will differ one another. Key management is done by managing the data in a secure way by encrypting the data with multiple users.

In this we propose the idea of storing the data in the cloud storage and then retrieving the data when required from cloud. The patient details are first stored in to the cloud by logging the details of the patient in to the server. Once if the details of the patient are given the data of the patient is stored in the cloud, these details can be retrieved any time. Once the patient gets logged on to the website the patient has the option of hiding the data and giving the authentication only to the family members. These data and the medical details are shared with in the same hospital. If the patient wants to get the treatment in other hospital the data can be shared by the other hospital admin since there is an option of sharing the data in different server. This is the new idea that we have proposed.

IV. Personal Health Record And Its Frame-Work

In this paper we describe about the security over the personal health record using different algorithm and and storing in the cloud storage

A. Problem statement

There are different ways in which the data in the PHR is encrypted by different user for their convenience. The patient only has the right to make changes such as delete over their data .once the profile for the patient is created all the data and the information about the patient will be stored in the cloud so that the data can be retrieved from the cloud any time. In-order to provide the security for the patient data we are using the Attribute based algorithm, H MAC MD5 algorithm and blocking of data. For instance , patient data is stored in a Baby care hospital if the patient wish to visit a doctor in Vee care hospital the data can be retrieved from the cloud storage and the sharing of data with different servers can also be done in a secured manner .This type of storing the data and retrieving the data from the cloud using the above mentioned algorithm will provide security and scalability and usability over the data.PHR is not only accessed in the emergency cases it is also done in the normal case where the patient data base is created in the cloud so that the patient need not necessarly remember all the medical data instead the patient can store the data in the cloud and retrieve the data whenever it is required. Since it is a cloud storage there are large number of data can be stored and accessed

B. Security design

As this paper deals with the semi-trusted security because the data of the patient is shared over the in the cloud where there will be the access of the third party so this phase of storing the data is not fully trusted and it is semi trusted system. This storage of data in the cloud will provide the maximum security over the data so that the data is not shown to the third party. The security becomes the major issue in storing the data in the cloud so that the third party access over the personal data is less. The access of the data should be restricted only to the patient

C. Requirements

The patient will only have the access over the data so that the patient will restrict the use ability of the data to whom the patient wish to share the personal data. For instance the patient want to restrict to share the data the patient can hide the data which ever the patient does not wish to share to other doctor or family members, on the other hand if the patient wish to share the data only to the restricted people he/she can give the accessibility to only the specific person so that the person can access the data even when the patient is not online .This type of providing the security over the data is the patient is not always online. That is the main reason that the patient wishes to secure the data with in self.

D. Right to access:

The accessibility of the data is given by the patient, if the patient wishes to give the login id and password to the doctor only then the doctor can do updates of the medical data in the patient profile. So, the right to access the data is given and authorized by the patient. This scenario of giving the right to access for the people is right to access

V. CONCLUSION

In this paper, we propose the trusted, secure, scalable method of sharing the data by using Attribute based encryption, Pseudo random code algorithm, blocking of third party user in the cloud storage. By proposing this idea we make sure that the data is secure in the semi trusted method. The patient only has the full control over the data thus the data will be fully protected even if the patient is not always online. It is not necessary that the patient should be online always.

The encryption and blocking of other user ,the data is fully protected and it is secured by the way of handling the data of the patient medical details between the patient and the doctor and also the patient family members whom the patient wish to give. Thus this becomes a solution of both secure and trust in sharing the patient details

REFERENCES

[1] Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption Ming Li,Shucheng Yu,Yao Zheng, , Kui Ren, ,and Wenjing Lou

[2] 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

[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] A. Lewko and B.Waters, “Decentralizing attribute-based encryption,”Advances in Cryptology–EUROCRYPT, pp. 568–588, 2011.

[5] S. M¨ uller, S. Katzenbeisser, and C. Eckert, “Distributed attribute based encryption,” Information Security and Cryptology–ICISC 2008, pp. 20–36, 2009

[6] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,” Journal of Computer Security, vol. 18, no. 5, pp. 799–837, 2010.

[7] Narayan, M. Gagn´e, and R. Safavi-Naini, “Privacy preserving ehr system using attribute-based infrastructure,” ser. CCSW ’10, 2010, pp. 47–52.