International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

SECURITY MODEL FOR PRESERVING THE MEDICAL BIGDATA IN HEALTH CARE CLOUD

Ms. R. Sudha Abirami[1], Ms. T. Priyadharshini[2]

[1]Assistant Professor, Thassim Beevi Abdul Kader College for Women, Kilakarai, Ramanathapuram District, Tamil Nadu, India.
[2]III Year MCA, Thassim Beevi Abdul Kader College for Women, Kilakarai Ramanathapuram District, Tamil Nadu, India.

ABSTRACT:- *First identify the design problems on privacy preservation and then provide solutions. To ease the understanding, start with the basic scheme so that can identify the possible privacy breaches. Then provide an improved scheme by addressing the identified privacy problems. The resulting improved scheme allows the mHealth service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. To reduce clients decryption complexity, incorporate the recently proposed outsourcing decryption technique into the underlying multi-dimensional range queries system to shift clients computational complexity to the cloud without revealing any information on either clients query input or the decrypted decision to the cloud. To relieve the computational complexity on the company's side, which is proportional to the number of clients, proposed a further improvement, leading to our final scheme. It is based on a new variant of key private proxy re-encryption scheme, in which the company only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy, further reducing the computational and communication burden on clients and the cloud.*

Key words: privacy preservation, security, electronic medical record.

I. INTRODUCTION:

Currently, electronic medical records (EMRs) are very prominent in healthcare networks. They enables users to share their health data in a flexible and convenient way. For example, to find one's diagnostic report, a patient or his/her doctor needs only to retrieve the information from a database rather than having to search through numerous physical documents. Health data is very sensitive, and it is a major challenge to securely store and access EMRs in modern EMR systems. As most EMRs are outsourced to the cloud, they are easily exposed to potential threats and vulnerable to leakage, loss, and theft[1]. To prevent EMRs from unauthorized access, a standard solution is to perform an encryption before uploading them to the cloud.

Specifically, an EMR owner encrypts an EMR using a symmetric key, and only authorized medical staffs are authorized to access and decrypt it. However, data sharing becomes inflexible in this case. Two potential issues are the complicated key management and repetitive encryption [2] as patients usually do not know who is allowed to access their EMRs, they encrypt many pieces with distinct session keys and distribute the keys to different medical staff members.

The approach to accessing users' data needs to be flexible enough to address changes in users' roles[3]. Several schemes adopting attribute-based encryption (ABE) have been presented for fine-grained access control[4][5]. Users with attributes satisfying the access policy can decapsulate the EMR data. In addition, some advanced mechanisms, consisting of a multi-authority model in an outsourcing system[6] and a view-based access control [7] that allows patients to specify a list of authorized/unauthorized users, have recently been proposed. Role-based access control schemes (RBACs) [8] also allow fine-grained access control. They define a role-based policy for a hierarchical organization with identity-based broadcast encryption (HIBBE).While the above proposals achieve data confidentiality in the EMR system; privacy preservation for patients is still an unresolved issue. For example, an EMR of the patient "Lucy" is uploaded to the cloud, and no attacker can read the encrypted EMR. If the doctor is an expert in the hepatitis disease, an attacker can infer that Lucy may carry hepatitis B without decrypting her EMR. This means that an attacker can obtain her disease-related information by linking Lucy to her doctor, even without seeing the detailed EMR. This means that adversaries possess the capacity that no matter if the EMRs are encrypted or not, adversaries can deduce the EMR owners' diseases based on some experience, such as the acquired identity-related information. Therefore, if there is an anonymous scheme that obfuscates the identity of the patient during an examination, adversaries can only determine that "someone" carries hepatitis B without knowing who it is. Thus, the patient's privacy is preserved.

II. SECURITY REQUIREMENTS

In practice, all entities are likely to attack an EMR system. A dishonest party may try to obtain useful information from encrypted data that it is not authorized to access or to divert instructions from the system regarding benefits (e.g., with false information in medical disputes). Multiple dishonest parties may collude to achieve this goal. In the context of these attacks, the EMR system is expected to meet the following security requirements[9].

- **Data Confidentiality.** Personal data needs to be encrypted before being uploaded and securely stored on the cloud until an entitled recipient downloads and decrypts it. Specifically, only the users whose roles satisfy the associated access policy have the privilege to access the data, with all other unauthorized entities not able to obtain any useful information from the encrypted data, even if they collude with each other.

- **Identity Anonymity**. Identity-related information needs to be hidden, as individual privacy is vulnerable to loss, theft, and illegal transactions. When a user's identity is hidden in an EMR system, it decreases the possibility of an adversary guessing that user's identity such that hardly any third party can obtain useful patient information.

III. Proposed Work:

This is implemented with 5 Modules. These are:

- S-CSP
- Registration & Login for Doctor
- Key Generation
- Patient Personal and Health Info Registration
- View & Update the Status of Patient Health Record

1) S-CSP

This is an entity that provides a data storage service in public cloud. The S-CSP provides the data outsourcing service and stores data on behalf of the patients. To reduce the storage cost, the S-CSP eliminates the storage of data. In this project, S-CSP is always online and has abundant storage capacity and computation power.

2) Registration & Login for Doctor

In which doctors can enroll their data in cloud by giving their personal information, medical practice certificate number. After they registered, they have to wait for some time until his registration is accepted by administrator or higher officials like administrator of cloud or dean of doctors committee. After their registration is accepted by administrator, they can log into the cloud by giving their user id and password. After that they have to give a secret key which is generated and sent by administrator.

3) Key Generation

Here, Administrator have to be approved/rejected the doctor's application based on their certificate and practice term. Whenever a doctor is logged into the cloud, a unique and secret key is generated based on KP-ABE technique for him by administrator.

4) Patient Personal and Health Info Registration

All the personal and health information are registered by a doctor who is taking care of the patient initially. After the registration process, one time unique id is generated for that patient. This id is informed by doctor to the patient either by in person or through mail id or mobile number. Regarding health information, doctor has to give blood pressure, blood test report, scan report, ECG report and lot if they have any other information about patient's health.

5) View & Update the Status of Patient Health Record

Once patients' information is registered in the cloud, the particular patients can go to the any doctor in the world for the treatment. First, patient has to give his patient id to the doctor who is going to take the treatment for him at present. After that his previous health information, treatment, doctor name, previously taken medicine are accessed from the cloud and shown on doctor's screen. Now, the doctor has to add the medicine details which is prescribed by him and he must add the scan reports, EEG, ECG reports and other test reports, surgery details if they are put into service. Patient also can view his personal and health information by giving his patient id and finger print.

IV. CONCLUSIONS:

To Design a Security Model For Preserving the Medical Bigdata in Health care Cloud which can effectively protect the privacy of clients and the intellectual property of Health service providers. Since patient's all the health information are maintained in the cloud, they don't need to maintain their records individually in home and PHR couldn't loss. To protect the clients' privacy, apply the KP-ABE technique. So health records can be only accessed by authorized doctors.

Finally, to enable resource constrained small companies to participate in Health business, our design helps them to shift the computational burden to the cloud by

applying newly developed key private proxy re-encryption technique. It has been shown to achieve the design objective.

VI. REFERENCES:

[1] M. J. Atallah, M. Blanton, and K. B. Frikken, "Dynamic and efficient key management for access hierarchies," ACM Trans. Inf. Syst. Secur., vol. 12, no. 3, 2009.

[2] J. Huang, M. Sharaf, and C. T. Huang, "A hierarchical framework for secure and scalable ehr sharing and access control in multi-cloud," in ICPPW 2012. IEEE, 2012, pp. 279–287.

[3] M. C. Mont, P. Bramhall, and K. Harrison, "A flexible role-based secure messaging service: Exploting ibe technology for privacy in health care," IEEE Computer Society, vol. 432, 2003.

[4] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in SPSM 2011. ACM, 2011, pp. 75–86.

[5] S. Narayan and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," in CCSW'10. ACM, 2010, pp. 47–52.

[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp.131–143, 2013.

[7] M. Sicuranza, A. Esposito, and M. Ciampi, "A view-based acces control model for EHR systems," in IDC 2014. Springer, 2014, pp. 443–452.

[8] W. Liu, X. Liu, J. Liu, Q. Wu, J. Zhan, and Y. Li, "Auiting and revocation enabled role-based access contrl over outsourced private ehrs," in HPCC 2015. IEEE, 2015, pp. 336–341.

[9] Xingguang Zhou, Jianwei Liu Qianhong Wu, And Zongyang Zhang", Privacy Preservation For Outsourced Medical Data With Flexible Access Control", Digital Object Identifier 10.1109/Access.2017. Volume 4, 2016.