Finding The Nearest Hospital With The Secure Sharing of PHR

Shakthi.S,[1], Mrs. R. K . Kapila Vani [2], Mrs. Rupa Kesavan[3]
[1]Dept of Computer Science and Engineering
[2, 3]Assistant professor
[1, 2] Prince Shri Venkateshwara Padmavathy Engineering College, Chennai, India .

Abstract- *The broad acknowledgement of cloud based administration in the me the medical services area has brought out financially scalable and helpful trade of Personal Health Records(PHR) among the elements of e-Health Frameworks. Putting the Secret Well Being data to cloud servers is helpless to disclosure or robbery and requires the involvement of philosophies that guarantee the protection of the PHR's.The SeSPHR is an emerging framework of health information exchange, which is often stored at central storage.But there are still various emerging problems as PHR could be discovered to unauthorized people. To control the efficient access of patient centric PHR report, can encrypt the stored data in the cloud based storage efficiency in key administration,flexile access and efficient user control. We propose a methodology for control of data access to PHRs,we provide AES encryption approach to encrypt each PHR file.We focus on multiple data owners and specifically specified access to various sorts of clients on various parts of the PHRs. Extensive analysis and experimental results are provided on the proposed scheme. The users can authenticate with the user id and password and can able to register with the web application. The patients can search the nearest hospital using theuserscurrent location or manually searching the location. The main idea is to book the reliable services through the user account.*

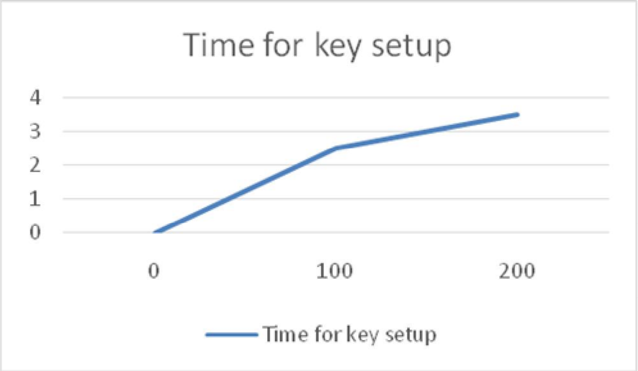
I. INTRODUCTION

YHIS,personal Health Records(PHR) has raised as a standard of health report management. A PHR model allows a user to create, manage, and control health data at one cloud storage through the technology of web, which has thus made storing retrieval, and sharing of the information more efficient in the cloud management.

Each user is allowed to take the full control of medical records and can share health informationwith variety of users, including medical report providers, family members and friends.

But while it is easier to have PHR services can slow down its acceptance in the storage. The main reason to worry about is whether the patients or users could control the sharing of health Record(PHR) specificallywhen they are sorted on external services where user may not fully assurance. On the other side due to suspect health information PHR, the external cloud storage are often at risk of various attacks which may lead to vulnerability of PHR.To ensure userconfidential control on their own PHR's, it is fundamentally to have data access control model that works with cloud.

The PHR information can be encrypted with the AES Encryption to store the personal information securely in the cloud.



A basic idea would be to encrypt the data before storing on cloud. The PHR owner should be able to decide how to encrypt files on the storage and to allow or not which users to recogize access to each file. A PHR informatin must only be accessible to the some of the users while it remains confidential to the other users. Next would be that the patient shall always have the access right to not only to acesss the PHR, but also be able to access authorization when they feel it is necessary. However, the patient-centric privacy is often in danger with the amount of scalability in a PHR system.The certified and confined users may either need to retrieve the PHR for own use or authoritative use. Different from the single data owner type which is often considered in most of the PHR system, there are numerous users who may encrypt according to their own possible ways, by using sets of keys. Here a concern would be, allowing each user acquire keys from very owner whose PHR wants to be read would limit the access since patients are not always online.So an another way would be to employ a central authority to do all the key management for all PHR owners, but this again require much attention on storage.

The users can authenticate with the user id and password and can able to register with the web application. The patients can search the nearest hospital using the users current location or manually searching the location. The main idea is to book the reliable services through the user account. The services are provided with the registered hospital. The providers are the persons who can able to login with web application and can register the hospitals, branches and doctors.

II. PROBLEM DEFINITION

To study a PHR system where there are numerous PHR owners and PHR users. The owners can be users who have full access control over their own PHR data where they can construct maintain and delete it. There is a server which belongs to the PHR service provider which stores all the owners' PHRs. The users may come from the various places and various category.

A. Authentication of unauthorized action

The method is an important requirement for efficient PHR access is to enable sharing. This means that the patient should have all the control over their personal health record. The Admin can determine which users shall have access to their PHR record. User controlled access, retrieval and revocation is the two main security objectiveUser controlled write access control in PHR system states the prevention of unauthorized users to access the records and modifying it.

B.Access control

Access control should be used in a manner that different users are authorized to read different sets of documents. Whenever a user keys no longer applicable, the user need not be able to access further PHR files using the same keys.

C. Managing PHR

The PHR should allow users from both the personal andpublic. Considering the groups of end users from the public domain may be immense in size and uncertain, the system should be scalable, and efficient in managing the complexity in the communication, computation and storage information. Also, the owners struggle in governing users and keys should be reduced to enjoyusability.

PHR PARTITIONING

The PHR is logically partitioned into the following four partitions

- ✓ Personal Information
- ✓ Medical information
- ✓ Insurance related information
- ✓ Prescription information

However,it is essential that the above said partition is not inflexible and correct. It is at the discretion of the user to partition the PHR intosmall or more number of partitions.The PHRs can be easily partitioned and can be represented in formals. For example , a PHR owner may place more than one partition into the same level of access control. Any partition user might not be granted a full access on the health records and not be granted a full access on the health records and some of the PHR partitions may be restricted to the user Pharmacist may be given access to related information prescription and insurance whereas the personal and medical information may be restricted for a pharmacist.

III. SYSTEM ARCHITECTURE

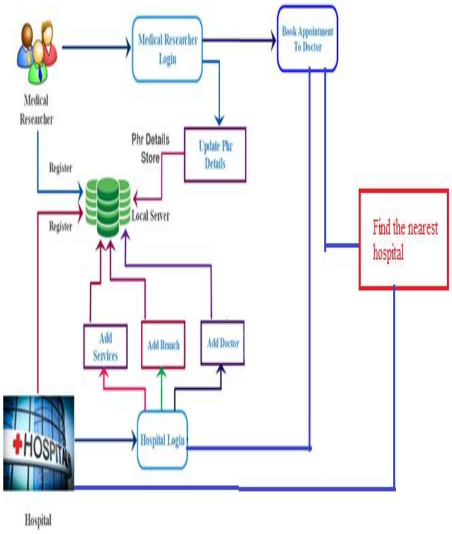


Fig 2.1 System Architecture

The cloud computing also integrates various important entities of healthcare domains, such as patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service provider. Generally, the PHRs contain information, such as graphic information like medical history including the diagnosis, allergies, past surgeries, and treatments,laboratory reports, data about health insurance claims, and private notes of the patients about certain important observed health conditions.

IV. DESIGN

There are 6 modules in the proposed system, they are namely,

1. 1.Find the nearest hospital
2. Admin Modules
3. Provider Module.
4. Doctor Counsel.
5. User Module
6. Database Report Upload

V. MODULES DESCRIPTION

Hospital Finder

Technological examinations and advancements which have shown a rapid growth concerned with the each and every field of science, the rapid development that has occurred in web based application has become a very significant factor in achieving our daily tasks. The user can able to find the nearest hospital by searching in the web application by their location.

The user can able to search the nearest hospital usingthemanual location or by automatically searching the location. The user can able to register and login and they can able to book services through the web application in which hospital they want to book services and can provide with reliable services.

The location of the user can be taken and can be able to search the nearest hospital with the user location.The user can able to Register with details like name,id,address,phone number.

The hospital can able to register and login through the providers. The providers can able register and login through the providers login in the web application and can able to add the hospitals,doctors and add also add branches and the doctors can add the services provided by the hospital. They can provide various type of services like scanning doctor counselling, blood test.

The providers can able to add the specific hospital details and doctor details to the web application.

Admin Module

The user can be authenticated with the web application and can be able to provide the reliable services through the provider side.

The admin can able to view the details of the doctors and can be able to manage the details of the users, doctors and patients. The admin is the only authorized person who can able to view the services.

Provider Module

When every provider has unique list of hospital and providers And can comes under the application and can able to book the services through comes under the particular provider.

When an User booked his Provider along with Hospitality Functions and the Doctor Specialist in an application.Oncean User come back for further Process They made an counselling to Particular Doctor.

The unique id has been to the providers, users, hospitals, branches and it is useful the admin to identify the hospitals using the unique id provided to each hospitals.

The unique id is used for identification of the each and every hospital.The user can provide with the unique id for an can able to verify with that.

Doctor Counsel.

When the PHR information is stored in the central storage, they will try to find out the secret well being of the individual as much as possible. The third party can access the storage beyond their accessibility.

The user counselling provides the counselling with the doctor with the symptoms.The doctor can ale to give their suggestions to the user according to the symptoms. The user can encrypt the details of the symptoms and suggestion of doctor if they want.

User Module

The implemented methodology to limit the view of the user personal information by others. The user can able to login and register with the application and provide the reliable services with the application. The user can able to search the nearby hospitals with the user location or manually entering the location.

The algorithm provides the necessary rules to identify the user at the entry level is that a validate user or not.

Database Report Upload

aadmin can able to view users report, Users personal Records and User Counselling Records. A user had made encrypted their information it will visualization in cipher text format and age display in the K-Anatomy Format.

Algorithm

For Encrypting the details of the Personal Health Records AES algorithm is used to encrypt the details of the PHR details and store the centralized information in the cloud server. For Privacy the PHR information can be encrypted to cloud server. For the use of the doctor the PHR information are encrypted to the cloud Server

VI. CONCLUSION

The proposed methodology to securely share and stores the information in the central storage and transmission of the PHRs to the authorized users in the cloud and to find the nearest hospital using the web application. The methodology preserves the confidentiality of the PHRs and enforces a confined access to the patients.The implemented mechanism provides the access to specified portions of the user records. In addition to privacy preserving, the details can be used to book services the concerned hospital by searching the nearest hospital.The performance evaluation was done on the on the basis of hospital selection, PHR encryption. The experimental results exhibit the liability SeSPHR methodology to securely share the PHRs in the cloud based environment storage.

VII. FUTURE ENHACEMENT

The project can be used by nearby orphanages,homes efficientlyThe Encryption can be more standardized in the more efficient way.The PHR details can be used in a more efficient ways for enhancing their features.

REFERENCE

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, *Wireless Sensor Network Technologies for the Information Explosion Era, Stud. Comput. Intell.* Springer-Verlag, 2010, vol. 278.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2006.

[3] A. A. Abbasi and M. Younis, “A survey on clustering algorithms forwireless sensor networks,” *Comput. Commun.*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, “AnApplication-Specific Protocol Architecture for Wireless MicrosensorNetworks,” *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, “An Analytical Modelfor Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 13, pp.1290–1302, 2002.

[6] S. Yi, J. Heo, Y. Cho *et al.*, “PEACH: Power-efficient and adaptiveclustering hierarchy protocol for wireless sensor networks,” *Comput.Commun.*, vol. 30, no. 14-15, pp. 2842–2852, 2007.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, “Design and Implementation Issues of Clustering in Wireless Sensor Networks,” *Int. J. Comput.Applications*, vol. 47, no. 11, pp. 23–28, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a*et al.*, “SecLEACH-On the security of clustered sensor networks,” *Signal Process.*, vol. 87, pp. 2882–2895, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, “Security and performance analysis of a secure clustering protocol for sensor networks,” in *Proc.IEEE NCA*, 2007, pp. 145–152.

[10] K. Zhang, C. Wang, and C. Wang, “A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management,”

[11] M. Blanton, M. M. J. Atallah, K. B. K. Frikken, and Q. Malluhi, “Secure and Efficient Outsourcing of Sequence Comparisons,” Comput. Secur. 2012, pp. 505–522, 2012.

[12] M. Franklin, M. Gondree, and P. Mohassel, “Communication-efficient private protocols for longest common subsequence,” in Topics in Cryptology--CT-RSA 2009, Springer, 2009, pp. 265– 278.

[13] M. Gondree and P. Mohassel, “Longest common subsequence as private search,” in Proceedings of the 8th ACM workshop on Privacy in the electronic society, 2009, pp. 81–90.

[14] D. Szajda, M. Pohl, J. Owen, B. Lawson, and V. Richmond, “Toward a practical data privacy scheme for a distributed implementation of the SmithWaterman genome sequence comparison algorithm,” in Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS 06), 2006.

[15] M. Blanton and M. Aliasgari, “Secure outsourcing of DNA searching via finite automata,” in Data and Applications Security and Privacy XXIV, Springer, 2010, pp. 49–64.

[16] J. R. Troncoso-Pastoriza, S. Katzenbeisser, and M. Celik, “Privacy preserving error resilient dna searching through oblivious automata,” in Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp. 519–528.

[17] K. B. Frikken, “Practical private DNA string searching and matching through efficient oblivious automata evaluation,” in Data and Applications Security XXIII, Springer, 2009, pp. 81–94.

[18] K. Kozl and C. Listy, “Biochemical nomenclature and related documents,” Chem. List., vol. 72, pp. 288–305, 1978.

[19] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in Proceedings of the 17th international conference on Theory and application of cryptographic techniques (EUROCRYPT’99) , 1999, pp. 223–238.

[20] D. Chaum, “Blind signatures for untraceable payments,” in Advances in cryptology, 1983, pp. 199– 203.