HEALTH INFORMATION SWAP OVER BASED - OBJECTIVE STRUCTURE ASSISTED BY CLOUD

B.Gayathri[1]   S.Lalitha[2]   D.Kaleeshwaran[3]
[1]UG Student, Department of Computer science , [2]UG Student ,Department of Computer Science , Assistant professor [3],Dept of Computer Science and Engineering.

INTRODUCTION

Cloud computing is emerging as a new computing paradigm in the healthcare sector besides other business domains. Large numbers of health organizations have started shifting the electronic health information to the cloud environment. Introducing the cloud services in the health sector not only facilitates the exchange of electronic medical records among the hospitals and clinics, but also enables the cloud to act as a medical record storage center. Moreover, shifting to the cloud environment relieves the healthcare organizations of the tedious tasks of infrastructure management and also minimizes development and maintenance costs. Nonetheless, storing the patient health data in the third party servers also entails serious threats to data privacy. Because of probable disclosure of medical records stored and exchanged in the cloud, the patients' privacy concerns should essentially be considered when designing the security and privacy mechanisms.

Various approaches have been used to preserve the privacy of the health information in the cloud environment. This survey aims to encompass the state-of-the-art privacy-preserving approaches employed in the e-Health clouds. Moreover, the privacy-preserving approaches are classified into cryptographic and non cryptographic approaches and taxonomy of the approaches is also presented. Furthermore, the strength and weaknesses of the presented approaches are reported and some open issues are highlighted.

Abstract:

Electronic Health Record (EHR) is longitudinal collection of electronic health information for and about persons, where health information is defined as information pertaining to the health of an individual or healthcare provided to an individual and it can support of efficient processes for health care delivery. In existing system the Clinical Document Architecture developed is a core document standard to ensure such interoperability and propagation of this document format is critical for interoperability. Unfortunately, hospitals are reluctant to adopt interoperable HIS due to its deployment cost except for in a handful countries. With the world's population increasing and everyone living longer, models of treatment delivery are rapidly changing, and the datasets keeps increasing. New technologies have also made healthcare data not only much bigger but also much more difficult to handle and process. A problem arises even when more hospitals start using the CDA document format because the data scattered in different documents are hard to manage. To maintain the large number of patient's medical records, clearest opportunities exist to reduce the costs through the use of Cloud. The specific information is extracted from the data rich environment and produces the information about history of the disease and how it can be cured. It is done by using the decision support system implementation for health care with the use of software that aids in the process of decision-making in order to ensure the correct diagnosis of any illness. This system consists of a data collection layer with a unified standard, a data management layer for distributed storage and parallel computing, and a data-oriented service layer. The medical diagnosis of an illness can be done in many ways; from the patient's description, physical examination and/or laboratory tests.

MODULES

- Hospital admin
- Apply the attribute based encryption for PHR
- Doctor maintain for PHR
- Secret key generation
- Deployment in cloud environment.

MODULE DESCRIPTION

Hospital admin: The hospital admin to create the account for patient and the account consists of following information details like

- Patient name
- Email id
- Age
- Blood group
- Another person access details
- Disease information

Online Appointment Management System allows getting online appointment instead of physical visit. With the help of online appointment management system patient, staff and doctor can check the status of appointment easily. This appointment management system allows to get an appointment for registered patients and also send updates to the customer through SMS or email.

Hospital Management System developed by Solution Dots Systems is an achievement that could change the administration and management of the hospital. It keeps it easy for the patient to get services and for the doctors to perform their duties in a better way. The Modules of Hospital Management System developed by Solution Dots Systems shows their own efficiency and effectiveness. With the help of this system, it will be easy to manage and upgrade the hospital system according to the demand and requirement.

Apply the attribute based encryption for PHR:

Personal health information could be exposed to those third party servers and to unauthorized parties so we want to secure the PHR .in this part we are using attribute based encryption to protect the PHR information.

Attribute-based Encryption Scheme

According to these schemes, a summary of the criteria, that ideal attribute-based encryption schemes, are listed as follows,

Data confidentiality

Before uploading data to the cloud, the data was encrypted by the data owner. Therefore, unauthorized parties including the cloud cannot know the information about the encrypted data.

Fine-grained access control

In the same group, the system granted the different access right to individual user. Users are on the same group, but each user can be granted the different access right to access data. Even for users in the same group, their access rights are not the same.

Scalability

When the authorized users increase, the system can work efficiently. So the number of authorized users cannot affect the performance of the system

User accountability

If the authorized user is dishonest, he would share his attribute private key with the other unauthorized user. It causes the problem that the illegal key would share among unauthorized users.

User revocation

If the user quits the system, the scheme can revoke his access right from the system directly. The revocable user cannot access any stored data, because his access right was revoked.

Collusion resistant

Users cannot combine their attributes to decipher the Encrypted data. Since each attribute is related to the polynomial or the random number, different users cannot collude each other.

Doctor maintain for PHR:

Doctor to view the patient PHR information and give the prescription for the corresponding patient and this details only access the authorized patient and his gave the privileges friends or relatives.

The personal health record (PHR) is proposed as an innovative solution to the problems of fragmented communication and lack of interoperability among diverse electronic medical record (EMR) systems. It provides a single source (the patient's PHR) for authentication and remote access of the health information data from all EMR systems. A voluntary survey was offered to selected patients, caregivers, and health providers of the Willmar, MN, PHR project to determine if a PHR was useful to these stakeholders, and if so, what aspects of a PHR would be most helpful in caring for patients

Secret key generation:

The patient wants to know about the status of the PHR first search the record and the corresponding secret key will be automatically mail to the authorized patient mail id .after enter that secret key to access the PHR file information.

Deploy cloud environment:

Finally we are deploying this application in cloud environment. Why we are deploying cloud environments means to reduce the bottle neck problem and any ware any time we can access our information and real time insert, delete, and update our record to the cloud environment.

Architecture:
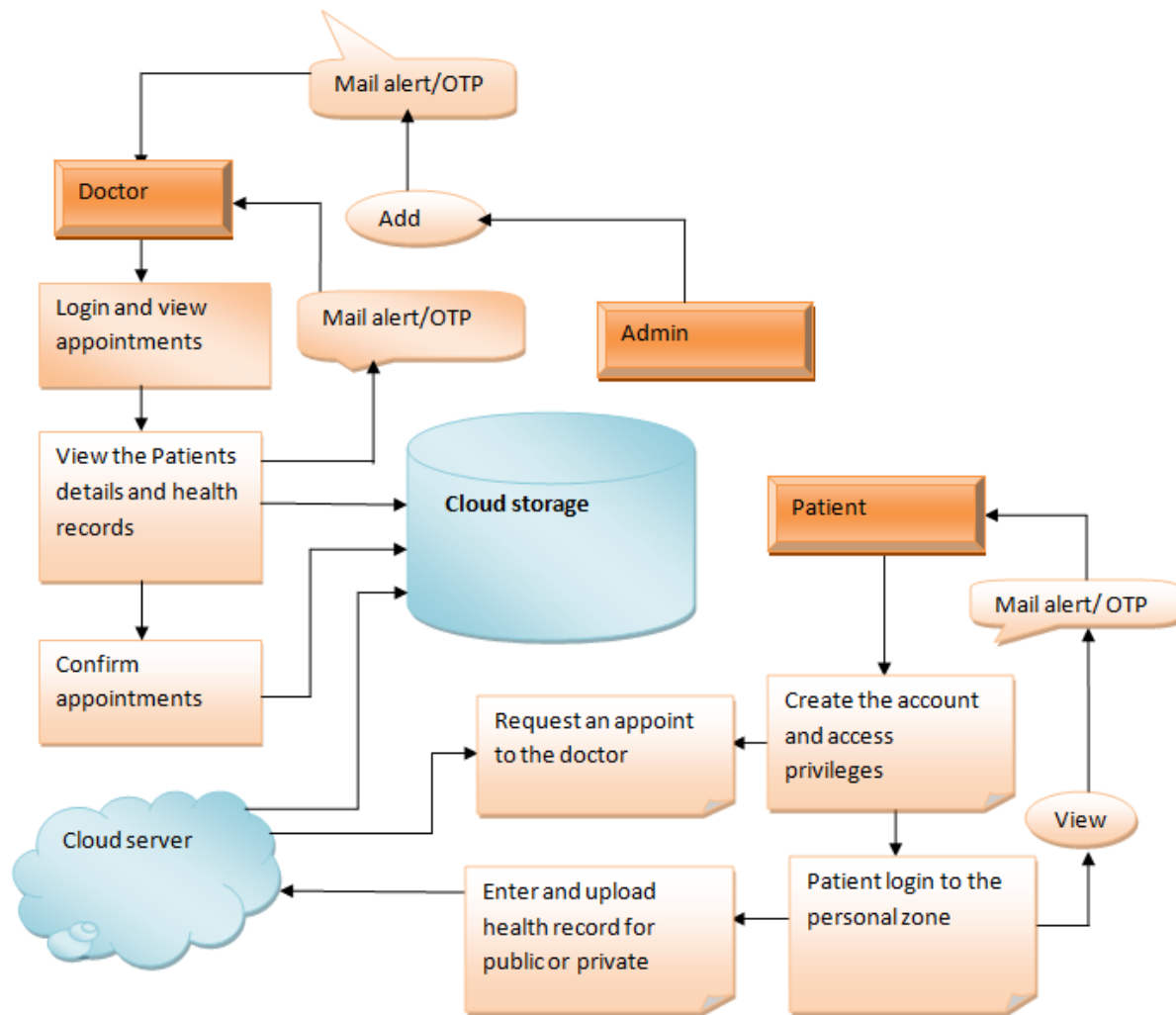
CONCLUSION

We have proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient.

REFERENCE:

1) M. Chen, Y. Hao, Y. Li, D. Wu, and D. Huang, "Demo: LIVES: Learning through interactive video and emotion-aware system," in Proc. ACM Mobihoc, Hangzhou, China, Jun. 22–25, 2015.

2) M. Chen, Y. Hao, Y. Li, C. Lai, and D. Wu, "On the computation offloading at ad hoc cloudlet: Architecture and service models," IEEE Commun. Mag., vol. 53, no. 3, pp. 1–7, Jun. 2015.

3) M. Chen, "NDNC-BAN: Supporting rich media healthcare services via named data networking in cloud-assisted wireless body area networks," Inf. Sci., vol. 284, pp. 142–156, Nov. 2014.

4) J. Wan, D. Zhang, S. Zhao, L. T. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions," IEEE Commun. Mag., vol. 52, no. 8, pp. 106–113, Aug. 2014.

5) J. Wan et al., "Cloud-enabled wireless body area networks for pervasive healthcare," IEEE Netw., vol. 27, no. 5, pp. 56–61, Sep./Oct. 2013.