isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 6, Issue: 3,Special Issue: 2 ,May,2021 ,ISSN_NO: 2321-3337

Secure And Efficient Sharing Of Health Records Using Random Key Generation Technique

Mrs. Lavina Balraj, M.E., Professor of Computer Science Department,
Ms. A. Durga, Student of Computer Science Department,
Ms. R. Bavya, Student of Computer Science Department,
Ms. M. Sasikala, Student of Computer Science Department,
St. Joseph College of Engineering, Sriperumbudur, Chennai.

Abstract

Sharing digital medical records on public cloud storage via devices facilitates patients (doctors) to get (offer) medical treatment of high quality and efficiency. However, challenges such as data privacy protection, flexible data sharing, efficient authority delegation, computation efficiency optimization, are remaining toward achieving practical fine-grained access control in the Electronic Medical Record (EMR) system. Nevertheless, storing the confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the EMR. Therefore, a methodology called secure sharing of the EMR (SeSEMR) in the cloud has been implemented. The SeSEMR scheme ensures patient-centric control on the EMR and preserves the confidentiality of the EMR. The patients store the encrypted EMR on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. In our proposed RC4 algorithm is used to encrypt data and random key generator is used for every request.

Key Terms: RC4-Rivest cipher 4, API – Application Programming Interface, SAS– Storage aggregation Server.

1. Introduction

Cloud computing has emerged as an important computing paradigm to offer pervasive and on-demand availability of various resources in the form of hardware, software, infrastructure, and storage. Consequently, the cloud computing paradigm facilitates organizations by relieving them from

the protracted job of infrastructure development and has encouraged them to trust on the third-party Information Technology (IT) services. Additionally, the cloud computing model has demonstrated significant potential to increase coordination among several healthcare stakeholders and also to ensure continuous availability of health information, and scalability. Furthermore, 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 providers.

2. Literature Survey

A. Solanas et al. [1] discussed about health environments. In modern healthcare environments, healthcare providers are more willing to shift their electronic medical record systems to clouds. Instead of building and maintaining dedicated data centres, this paradigm enables to achieve lower operational cost and better interoperability with other healthcare providers. The adoption of cloud computing in healthcare systems may also raise many security challenges associated with authentication, identity management, access control, trust management and so on. This paper ensures that privacy concerns or accommodated for processing access requests to patient health care information.

Greenberg et al. [2] provided research about health organizations and electronic equipment's. 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 centre.

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.

Shifting data to the cloud environment relieves the health care organization of the tedious task of infrastructure management and also minimizes development and maintenance cost.

Pagliuca et al. [3] provided substantial research in the field of Personal Health Record. Personal Health Record (PHR) has been developed as a promising solution that allows patient–doctors interactions in a very effective way. Cloud technology has been seen as the prominent candidate to store the sensitive medical record in PHR.

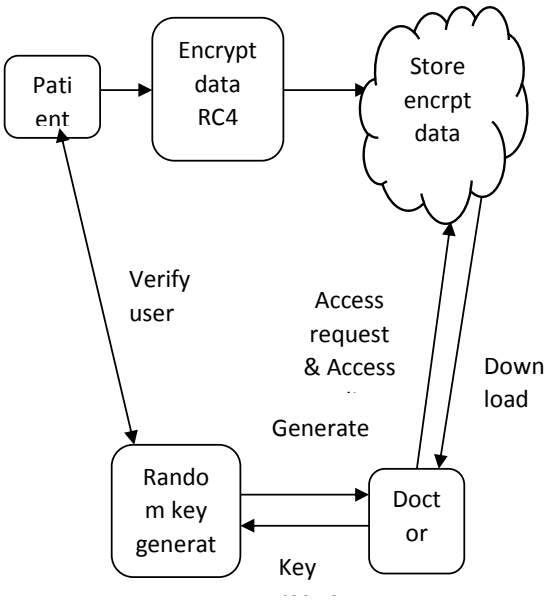
The security protection provided is yet inadequate without impacting the practicality of the system.

The general framework enables patients to securely store and share their PHR in the cloud server and furthermore the treating doctors can refer the patients' medical record to specialists for research purposes, whenever they are required, while ensuring that the patients' information remains private.

3. System Design

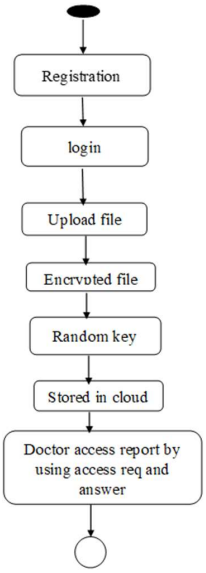
In the proposed system we are going to see about the 4 important concepts such as EMR, cryptography, Cloud storage, Micro aggregation. In our project to encrypt the data using RC4 encryption.

The access request and access permission send and receive between doctor and patient. One important technique is used that is random key changing technique. The purpose of this technique is random key will be generated after every attempt. This is the main concept in our program.

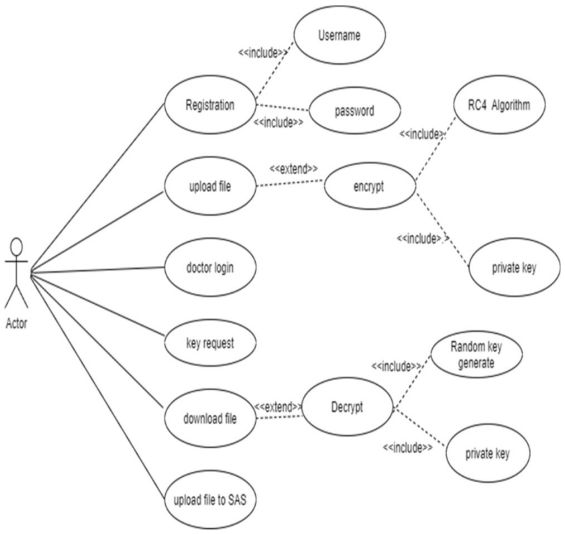


Initially patient login their details in patient login portal. Then enter their

details. Send these details to patient storage. To compress the data micro aggregation is used.



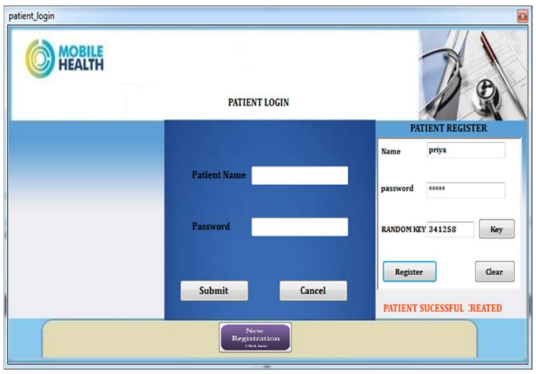
Finally encrypted data send to SAS. Doctor can see the data in server side. Doctor enter the doctor details in login portal.



Doctor send the request and get the permission from the patient. By entering the random key, they can see his patient original details. Upload the prescription. Finally close the portal.

4. Implementation

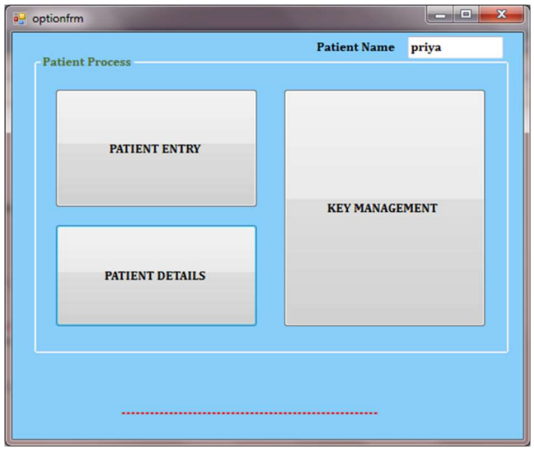
The system is composed of two major components, namely the server and client. First the patient/user needs to login the account. If he doesn't have account he has to register. During registration the random key is set in order to enhance more security. Once username and password match with the database then particular patient can login to next form.



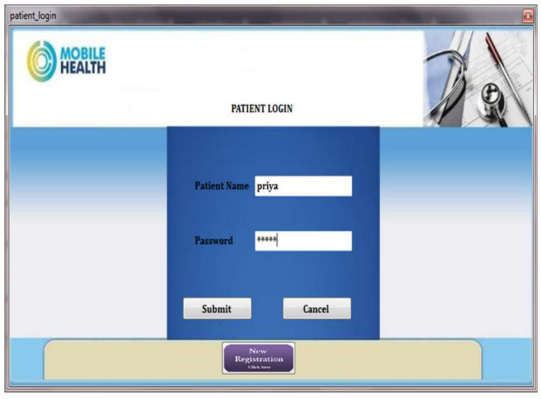
The patient will enter the details of his/her in the storage area. Using the file key, the patient will encrypt the data and send to the cloud. The required file will be transferred to the doctor. RC4 algorithm is

Volume: 6, Issue: 3,Special Issue: 2 ,May,2021 ,ISSN_NO: 2321-3337

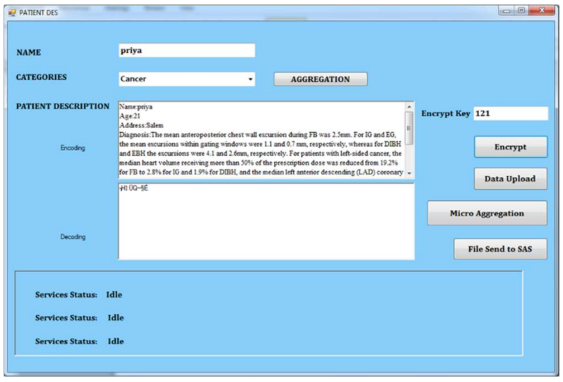
used. The doctor can download particular report of patient by satisfying attributes of owner of report.



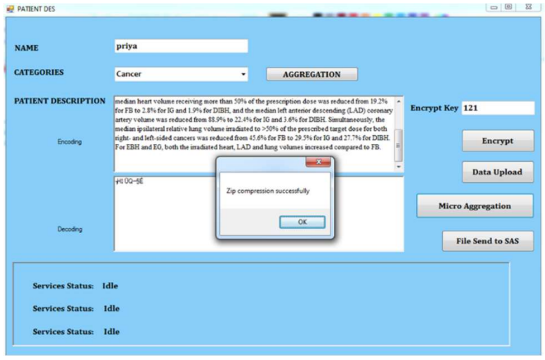
The patient will give the file to the doctor using the file key of decrypted data. So that the data will be fully secured and no one can able to access the file without the authentication key and the file key.



After the patient sent the file, the doctor will receive the file. The doctor must open the file by sending the key request to the patient. After the patient viewed it, he/she can update the random key and the patient will send the original key to the doctor. With the authentication key and file key the doctor will process the file. Here the data received from the client are accessed by the doctor by login to his account.



The process is further proceeded by requesting a random key to the patient. When the patient receives the message, he sends the key to the doctor. The doctor accesses his required patient's details on successful matching. Upload the prescription.



5. Conclusion and Future Enhancement

We proposed a methodology to securely store and transmission of the EMRs to the authorized entities in the cloud. The methodology preserves the confidentiality of the EMRs and enforces a patient-centric access control to different portions of the EMRs based on the access provided by the patients. We implemented a fine-grained access control method in such a way that even the valid system users cannot access those portions of the EMR for which they are not authorized. The EMR owners store the encrypted data on the cloud and only the authorized users possessing valid re-encryption keys issued by a semi-trusted proxy are able to decrypt the EMRs. The role of the semi-trusted proxy is to generate and store the public/private key pairs for the users in the system.

6. References

[1] A. Solanas and A. Martínez-Balles "V-MDAV: Variable group size multivariate microaggregation," pp. 917–925.

[2] Greenberg, 1987, Rank Swapping for Masking Ordinal Microdata Tech report. U.S. Bureau of the Census, unpublished.

[3] "Brand Microdata protection through noise addition, 2002," Lecture Notes in Computer Sci., vol. 2316, pp. 97–116.

[4] Pagliuca and G. Seri, 1998, "Some Results of Individual Ranking Method on the System of Enterprise Accounts Annual Survey", Esprit SDC Project, Deliverable MI3/D2.

[5] G. J. Matthews and O. Harel, 2011, "Data confidentiality: A review of methods for statistical disclosure limitation and methods for assessing privacy," Statist. Surveys, vol. 5, pp. 1–29.