iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3067

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Secure Management of Health Care Data using Cloud Computing

Dr. A. Radhakrishnan[1], Ajilin Femi. T[2], Theepshika. L[3]
[1]*Assistant Professor,* [2,3]*UG Student, Department Of Information Technology, University College of Engineering, Konam, Nagercoil-629004 (Anna University Constituent College)*

Abstract: ***Electronic health record of patients are kept and managed by medical institutions in their databases. A patient who wants to receive treatment in different institutions needs to ask his already treated doctor to release his medical records. This process is time consuming and complex. To overcome these problems, we are proposing a solution that a government organization to maintain the medical records of the patients in the public cloud. The recognized medical institution, who got approval by the government, stores the medical records of the patients in the cloud. The medical records which are entered are encrypted using Advanced Encryption Standard (AES-256) algorithm. If a patient wants to receive treatment in different institution, that medical institution can get access to the records directly from the cloud. This will reduce the time delay for further treatment.***

Keywords: Public cloud, AES Encryption, Fingerprint, Adhar number.

I. INTRODUCTION

Medical Institutions gather and store medical records of a patient with the goal of providing the best care. The medical history of patients is essential to guarantee that the right diagnosis is achieved. The medical information is highly sensitive and must be kept private .At the same time, the medical records should be accessible to any other medical institution to ensure that the patient can be attended anywhere. Since the medical institutions stores medical record in databases, it cannot be accessed by any other medical institutions. Patient's medical records should be available to other medical institutions. Using cloud computing, storing and managing the medical records can be a solution. Using cloud computing, each medical institution stores the medical records of a patient in public cloud. Public cloud services are capable of scaling and provide availability since they can be accessed through the Internet. Before storing the medical record in cloud, it is encrypted by using Advanced Encryption Standard cryptographic technique. This paper proposes a novel approach for storing EHRs in public clouds. It focuses in ensuring data confidentiality and integrity.

II. LITERATURE SURVEY

Yong Xiang et al[4] have proposed two Secure and Efficient Dynamic Searchable Symmetric Encryption (SEDSSE) schemes over medical cloud data. Firstly, they improve the secure k-Nearest Neighbour (KNN) and Attribute-Based Encryption (ABE) techniques to propose a dynamic searchable symmetric encryption scheme, which can achieve two important security features, i.e., forward privacy and backward privacy which are very challenging in the area of dynamic searchable symmetric encryption. Then, they proposed an enhanced scheme to solve the key sharing problem which widely exists in the KNN based searchable encryption scheme. In this paper they address two new issues: the collusion between the cloud server and search users as well as different secret key distribution among search users.

In order to improve the efficiency of encryption, Dong Zheng et al [5] introduce the online/offline encryption technology in the encryption phase. Before the message is found, a large amount of work that is needed at the encryption stage will be done. Then, once the message is known, the cipher text can be generated quickly. To protect the privacy of users and improve the efficiency of encryption, they proposed a secure medical data sharing system, where sensors and mobile terminals can encrypt sensitive data of users, then send it cloud servers. And users who can satisfy access control structure can access data in this system.

Hadeal Abdulaziz Al Hamid et al [4] mainly focused on how to secure healthcare private data in the cloud using a fog computing facility. For this, a tri-party one round authenticated key agreement protocol has been proposed based on the bilinear pairing cryptography that can generate a session key among the participants and communicate among them securely. Finally, the private healthcare data are accessed and stored securely by implementing a technique.

To overcome the barriers in the effective medical data exchange process, Yilong Yang et al [6] present a novel hybrid cloud called MedShare, dealing with interoperability issues among disconnected but autonomously functioning healthcare providers. Their

architecture and its implementation is based upon : 1) custom data extractors to extract legacy medical data from the three hemodialysis under consideration 2) negotiated and converted to a common data model in each of the private cloud of a provider 3) indexed patient information using the HashMap technique into the public cloud that operates on private clouds, called a hybrid cloud and 4) a set of services and tools installed as a coherent environment to exchange information smoothly. MedShare allows the healthcare providers and administrators to maintain control of their patient data, which is always the primary concern in building a trustworthy environment for exchanging patient information. Medshare effectively addresses primary security and privacy concerns surrounding the deployment of data exchange process by including patient consent and a two-way authorization process.

Yong Xiang et al [4] they have proposed a system which provides complete privacy and anonymity to the users of health care applications from adversaries and the authentication server. In this authentication scheme, they have utilized rotating group signature scheme based on Elliptic curve cryptography (ECC) to provide anonymity to the patients. To add an extra layer of protection, they have used the Onion Router (TOR) to provide privacy at the network layer. Their scheme is evaluated by theoretical analysis which demonstrates that it resists various attacks and provides several attractive security features.

III. METHODOLOGY

This section introduces the proposed design of the cloud based electronic medical record system.

A. Architecture of the System

The architecture of the cloud based medical record system is shown in the figure 1.

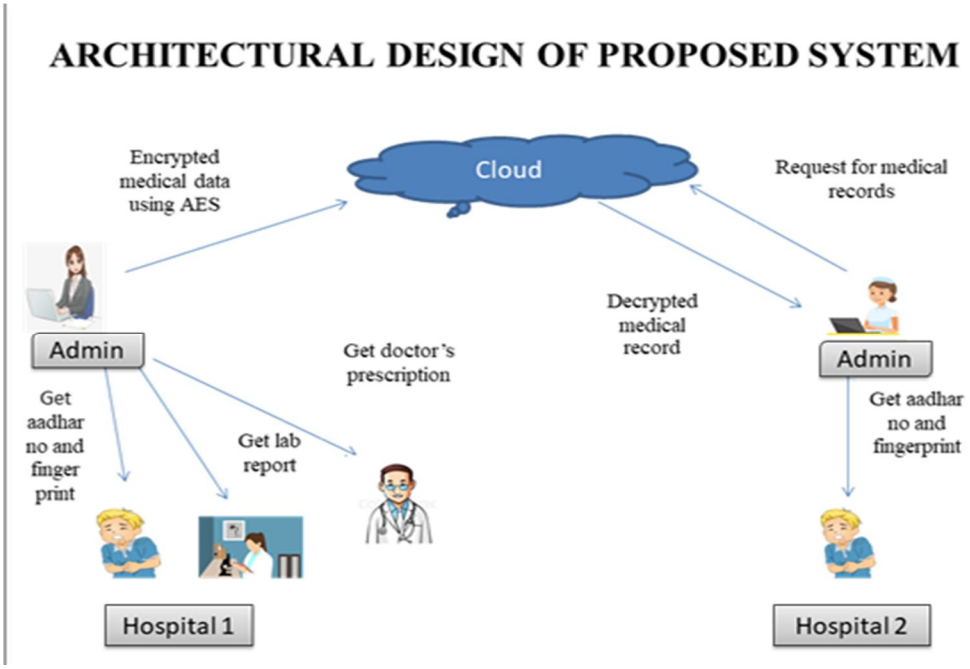


Figure 1

In the proposed system architecture, the government organization maintains the medical records of the patients in the public cloud. Only the recognized medical institutions who got approval by the government can access the cloud. Firstly, when a patient getting treatment in an medical institution, that institution collects all the personal details of that patient including the aadhar number and fingerprint. After treating the patient and taking all the scans, the medical institution login to the cloud using their credentials and enter the patient's aadhar number and fingerprint for authentication purpose and stores the medical records that includes doctor's prescription, lab reports etc in the public cloud. When a patient wishes to receive treatment in another medical institution, he/she can provide his/her aadhar number and fingerprint to that institution. That medical institution can directly access the medical records of that patient from the cloud using the aadhar number and fingerprint.

Our proposed system will also be useful in emergency situations. When a patient is in unconscious state and admitted in a medical institution, they do not know the medical history of that patient and the treatment is delayed. In such situations, our system will be useful. The medical institution can simply get the fingerprint of that patient and get access to his medical records. This will reduce the time delay for further treatment.

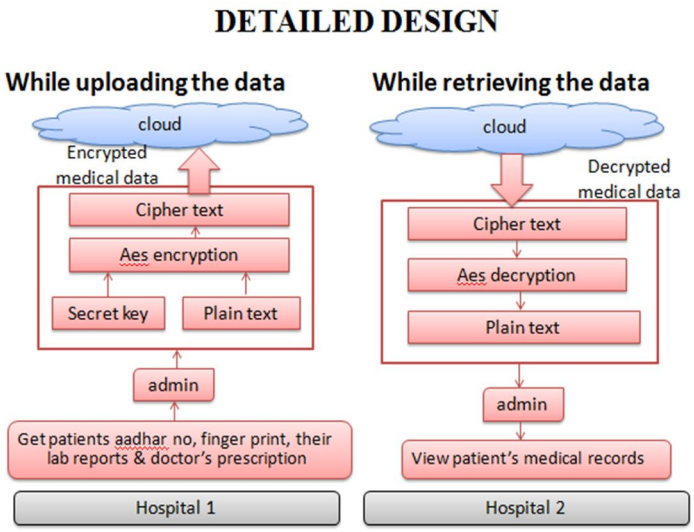


Figure 2

B. Algorithm

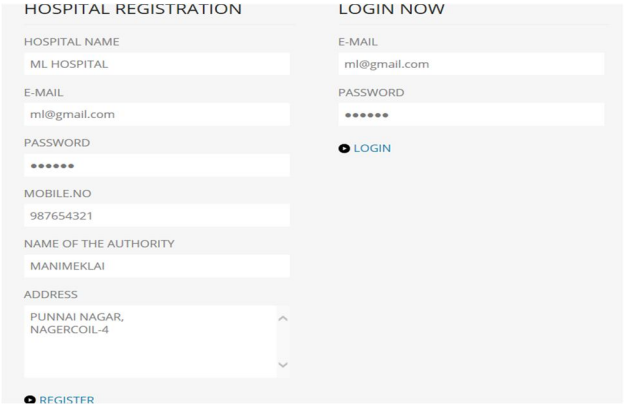
The medical records are confidential and should be stored in secure manner. Before storing the medical records in the cloud, it must be encrypted by using Advanced Encryption Standard(AES) algorithm.

In our proposed system we use AES 256 algorithm. AES is a symmetric encryption algorithm that takes input of 128 bit.

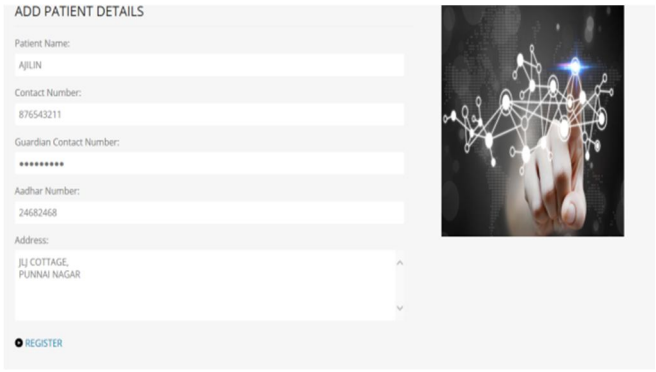
AES allows for three different key lengths: 128,192 or 256 bit. Encryption consists of 10 rounds of processing for 128- bit keys, 12 rounds for 192- bit keys and 14 rounds for 256- bit keys.

IV. OUTPUT

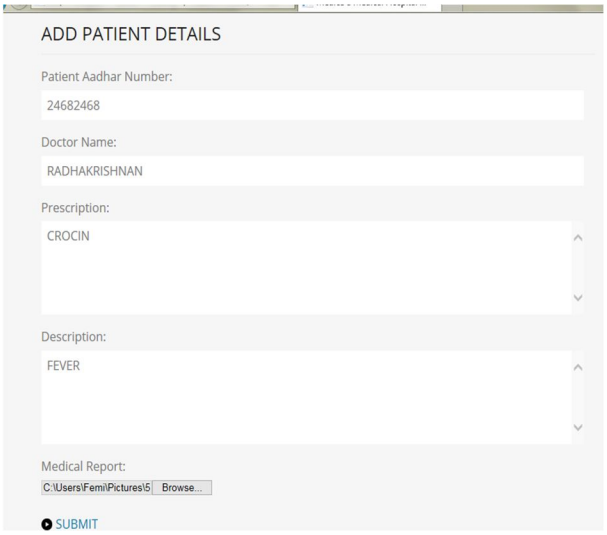
A. Hospital Registration And Login



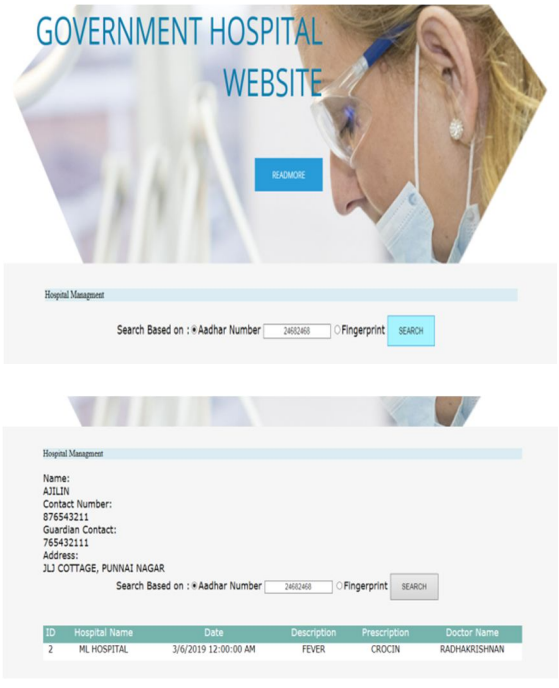
B. Patient Registration



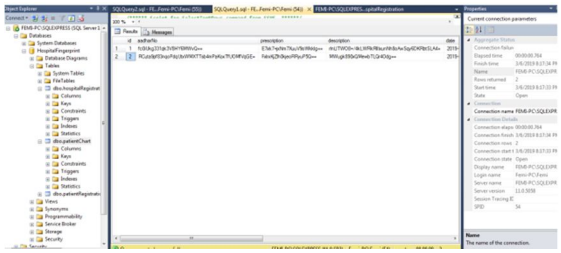
C. Adding Patient Medical Records



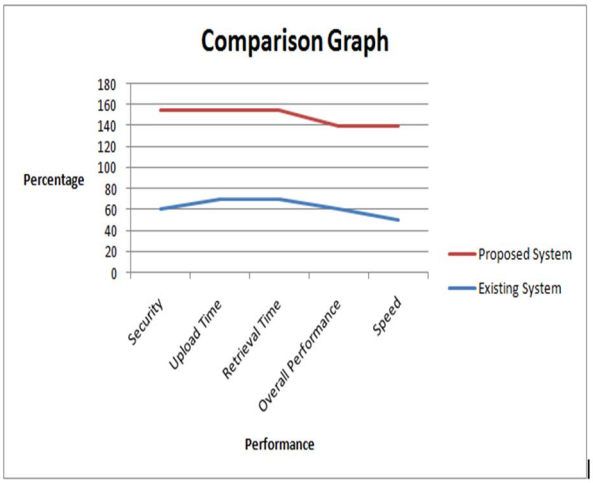
D. Retrieving Patient Medical Records



E. Encrypted Medical Record



F. Performance Graph

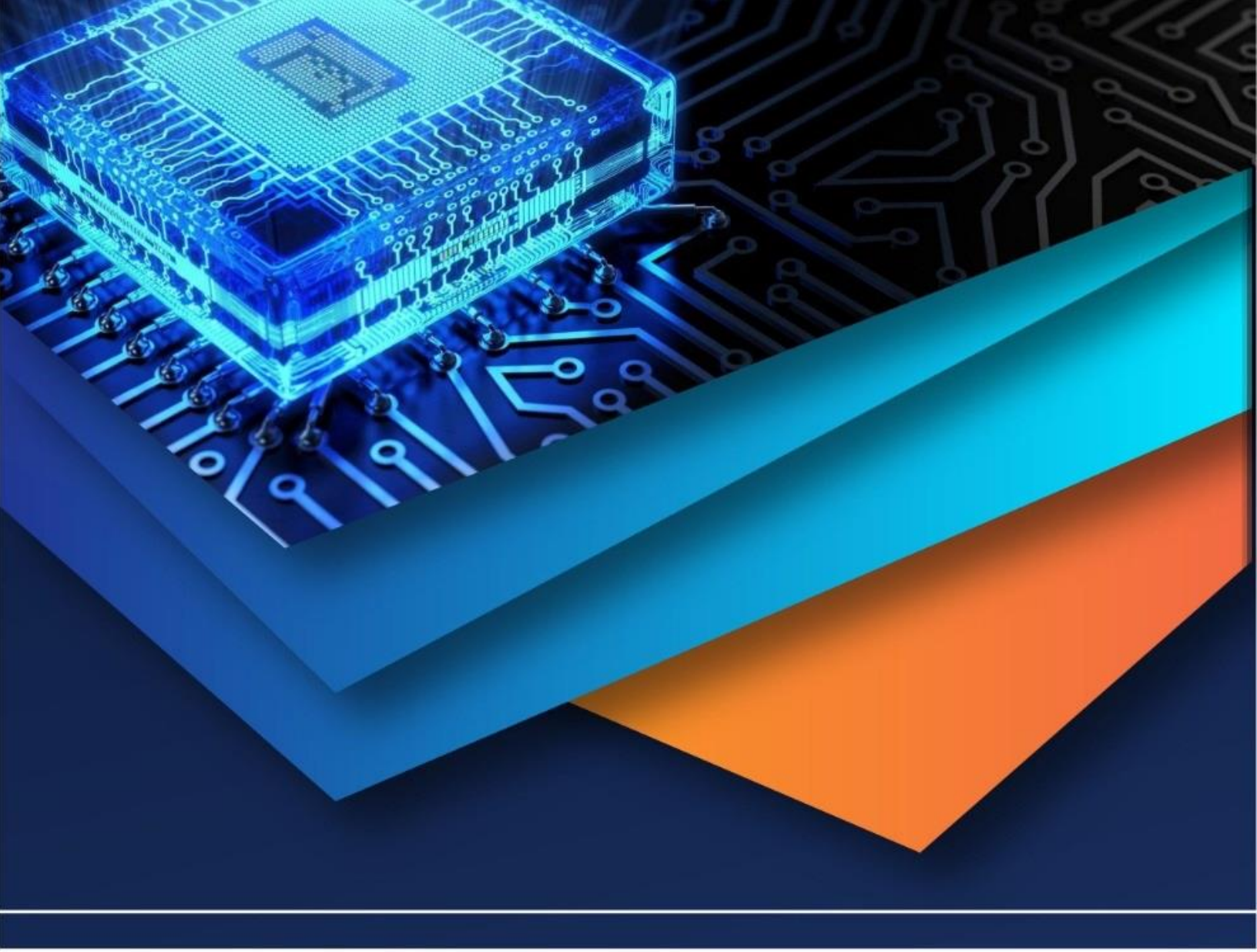


V. CONCLUSION

In this work, a cloud based electronic health records system has been designed and implemented. Cloud computing is an emerging technology and it offers many advantages like low cost, data backup recovery etc. The solution proposed in this paper solves the problem of denial of medical records among the medical institutions. And our system is also useful in emergency situations.

REFERENCES

[1] Dong Zheng, et al, “Efficient and Privacy Preserving Medical Data Sharing in IOT with Limited Computing Power”, IEEE Access, 2018
[2] Yong Xiang, et al, “Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data”, IEEE, 2017
[3] QiXia, et al, “MedShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain”, IEEE Access, 2017
[4] Esposito, et al, “Blockchain: A Panacea for Healthcare Cloud based Data Security and Privacy”, IEEE, 2018
[5] Ruizhang, et al, “Searchable Encryption for Healthcare Cloud’, IEEE, 2017
[6] Wenting Shen, el al “Enabling Identity Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage”, IEEE, 2018
[7] Hadeal Abdulaziz, el al, “A Security model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud using a Fog Computing Facility with Pairing based Cryptography”, IEEE, 2017
[8] Hanlin zhang, el al, ”Cloud Storage for Electronic Health Records based on Secret Sharing with Verifiable Reconstruction outsourcing”, IEEE Access, 2018
[9] Yilong Yang, el al, “MedShare: A Novel Hybrid Cloud for Medical Resource Sharing among Autonomous Healthcare providers”, IEEE, 2018
[10] Yong Xiang, “Anonymous Authentication Scheme for Smart Cloud based Healthcare Applications”, IEEE, 2018



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY