International Journal For Technological Research In Engineering
Volume 7, Issue 12, August-2020 *ISSN (Online): 2347 - 4718*

SECURITY SYSTEM FOR MEDICAL RECORDS.

Dr. Anusuya M A[1], Greeshma M[2], Harshitha M L[3], Noor Ul Huda[4]
JSS Science and Technology University (Formerly known as SJCE) S J C E Campus, Manasa Gangotri
Mysuru, Karnataka 570006, India

Abstract: The usage of cloud storage in medical field has been playing a very important role. Patients medical records are stored in the cloud hence the name Electronic health records (EHR).There are various challenges associated with this kind storage. In order to solve some of the issues like confidentiality we have used AES algorithm, for key storage we have used Shamir's algorithm and simple mail transfer protocol for access key.
Keywords: privacy, cloud, Electronic health record (EHR), confidentiality, and access key.

I. INTRODUCTION

Maintaining patient's medical data in paper becomes a tedious task with time and it is a lot of mess when it comes to storage and retrieval. For easy storage and access of patient's medical records cloud based storage is appropriate one. Electronic health records eliminate the use of paper and stores the entire patient medical history digitally and these digitized records can be accessed by all authorized users to provide proper clinical support to the patients at any time and from anywhere. Electronic health records automate and ease much of patient treatment process but these records comes with lot of baggage of security. As patient medical data or EHR's are stored in third party system, privacy is of primary concern. We cannot let EHR's to be tampered as this might dirty the medical information in the patient record and can affect the patient health directly and we also cannot let the patient medical data to be accessed unauthorized by the intruders. So here we are proposing simple security model using cryptographic algorithms in order to authenticate the EHR's and maintain the patient's integrity and confidentiality

II. BACKGROUND AND MOTIVATION

Electronic health records (EHR) allows to keep entire patient information such as patients identity, medical reports and medical history and this entire content can be accessed by authorized users to provide quality treatment to the patients without causing any sort of errors and thereby improving patients safety and patient clinical outcomes. This is the major motivation for transforming paper based medical records to digitized medical records.

III. LITERATURE SURVEY

Increase in the importance of security and privacy of the medical records has led to the creation of several methods to fight against the threat to the information in the system. Many works concentrate on firewalls, cryptography and antivirus software.

U.S. Department of health and Human Services [1] has recognized few best practices to protect the privacy of the patient's medical records and all the confidential information stored inside a network. This organization used packet filtering firewall system in order to filter the internal data and to prevent external data from entering the organization's secured network. This is similar to restrict access to specific IP addresses. This is a static method which should be implemented in the core. This can be expensive, and change based on the size and scope of an organization.

Liu V et al.[2] proposed another version of above mentioned system[1]. This class of firewalls is status inspection firewalls. Inspection firewalls are dynamic in nature and initiate a correlation between the incoming electronic data and past filtered electronic data [2]. This is almost identical to the packet filtering firewalls with respect to the core functionalities. Due to the dynamic nature of the inspection firewall and the compounded correlation of connections of IP addresses, the complexity of inspection firewall increases and becomes expensive, which is not the finest choice for all organizations.

SOAPware Electronic Medical Records is a product by the DOCS, Incorporation. The scope of this software system is restricted to a clinic. The tool is able to connect different units of an organization such as billing system, labs and clinical data. Since the scope of this system is small, excessive usage freezes up the system quite often which may lead to the loss of data. This tool enables users to view all appropriate data on one screen thus reducing the amount of time spent in searching a record.

OnmiMD Physician Empowered Company has come up with a product called OmniMD Electronic Medical Record. This is an internet based EMR application reachable by users both within and outside of the EMR system. This tool automates and simplifies the patient record document, storage and retrieval process. But this software fails to protect the sensitive information and support the users in time.

Jannetti MC [3] and Vockley M[4] in their work have proven that the digital signatures are the solution to prevent breaches of PHI. This shows that the use of cryptography ensures the security of sensitive data in electronic health record systems.

Specifically, encryption has enhanced security of EHRs during the exchange of health information. Lemke J. [5] and Chen YY et al.[6] in their work have shown that another form of cryptography can be used to secure the records. This method uses usernames and passwords as a firewall to the system. This can eventually prevent security breaches by including personal privacy concerning passwords and users are required to change personal passwords frequently [5, 6].Few rules are designed regarding the creation of passwords to avoid the probability that a hacker could postulate the password. This method of cryptography is also a useful security technique for providers in setting up role-based access controls. Role-based access control (RBAC)

assigns permissions to users based on their role within an organization. This method restricts information to users based on the role assigned to them by the system administrator. Internal breaches and threats can be avoided by this technique [6].
Regardless of all the efforts and measures taken by different organizations all around the world, the survey shows over 40 million patient records were breached last year affecting around 21 million records.

IV. WORKING METHOD OF APPLICATION

System requirements
This application needs a system with an i3 processor of 2.4 GHz+ Speed and 8GB RAM with 100GB hard disk.ASP.NET frame work is used to build the application and ADO.NET technology is used communicate between the webserver and database. C# coding language is used with Microsoft visual studio to build the application. And SQLyog is used as a database in backend.

System structure and functional modules
The functional module of the application is shown in Figure 1. The system functions mainly include four parts: Admin, doctor, patient, and Receptionist.

1. Admin function module
The admin function module contains four parts: department information management, hospital information management, medical records management and authorization management. Admin can add departments and modify department information in the system. Admin can also add hospital accounts and receptionists for the added
hospitals. Admin can upload and manage the data (medical trial records). Admin has power to accept or reject the access request made by other doctors for authorized electronic medical records in the system.

2. Receptionist function module
Thee receptionist function module contains two parts: Doctor Account management and patient account management. Receptionist is also responsible for collecting patient's clinical and general information such as past medical history, allergies and social history.

3. Doctor function module
The doctor function module contains two parts: Patient management and medical records management. In Patient management doctor can enter patients ID and view all data in a single window. Patient's data includes past medical history and general data. Doctor is also responsible for updating the patient's record with treatment after proper medical diagnosis. Doctors have option to view and request medical records uploaded by the admin.

4. Patient function module
The patient function module has only one option to enter their patient ID and get all the details for their reference.

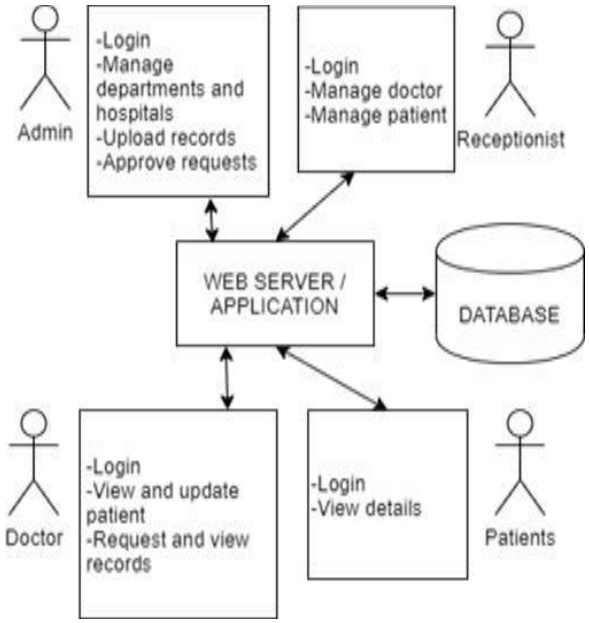

Figure. 1. Structure of the EMR system.

System Design and Implementation:
The objective of the application is to provide security to the sensitive data present in health care. The application uses cryptographic algorithms (Figure 2) and Role-based access control methods to protect the privacy of patients. It also ensures that the confidentiality and integrity of the medical records are shielded from unauthorized access.

Based on the functional modules of the system, a corresponding database is established in the backend for perfect functioning of the system. This database includes few tables with related attributes.

Sensitive information such as medical trial data uploaded by the admin and patient's treatment information updated by the doctors is encrypted using Advanced Encryption Standard(AES) Rijndael algorithm(Figure 2). This is a symmetric encryption algorithm which is faster in both hardware and software. AES is more secure and crypto-analysts agree that Rijndael will prove secure for all its real-world applications and the process may be strengthened through the addition of more rounds of transformation. AES supports various lengths of keys for different level of security. This key is randomly generated through code.
In order to increase the security and to avoid the threat to key we are using Shamir's secret sharing algorithm. In this algorithm the secret key is divided into parts where each part is unique and stores them in the database. Encrypted data can also be altered or modified using several techniques such as SQL injection, which makes the decryption process difficult and the result data may not be same as the original data. To maintain the integrity of the sensitive data we are converting the encrypted data into QRcode image, which cannot be modified under any circumstances and stored in the database.

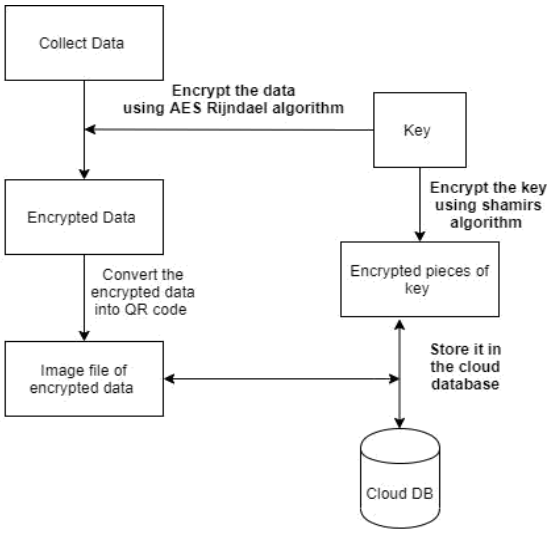

Figure 2. Encryption

Encrypted data can be accessed or viewed by the intended personnel once they get the approval from the system administrator(Figure 3). So, when a doctor or any actor who has an authorized access to the record requests for the data, that request is logged in the database and notified to the administrator.

Later a verification key is generated and sent to the respective doctor's mail address, and then the doctor will be asked to enter the verification code in order to view the record. The code is validated against the verification key and if it is a match then the encrypted data is extracted from the QRcode image or else the access is denied.

Once the encrypted data is extracted from the QRcode image, the original key is reconstructed by taking a defined minimum number of parts from the encrypted key through Shamir's algorithm. This key is used to decrypt the cipher text using AES decryption algorithm.

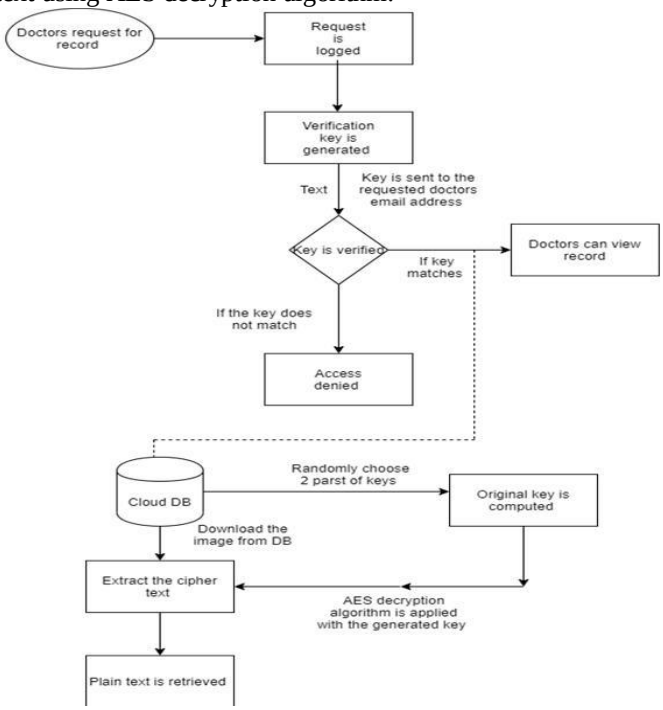

Figure 3. Decryption

V. TESTING AND RESULT

Managing user access control is an extremely difficult and continuous work. Keeping track of the users that should not have access to data and provide access to new users is a delicate task but is essential to guarantee confidentiality of patient's data. This paper proposes a solution to the difficulty that is managing user access control to a complex universe of user data and guarantee confidentiality while using cloud computing services to store medical records.

In terms of availability, patient's records is accessible from any computer with access to the Internet. There are confidentiality levels within the records. Some records can be publicly accessed while other should only be accessed by a restricted number of users. If confidential records end up in the hands of a person not privy to the information, the consequences can be overwhelming. Breach of medical records could lead to identity theft, which can destroy a person's finances, credit and reputation. Victims could seek litigation against the healthcare practice in which the breach occurred. If the breach affected multiple patients, the practice is headed down a long road of legal tribulations.

Step	Description	Input	Expected Result	Actual Result	Status
1	Open application	N/A	Application Home page should be displayed	Application home page is displayed	Pass
2	Log in as a Admin	User id:1111 password:5858	Admin login successful message must be displayed	Admin login successful message is displayed	pass
3	Authentication Verify	N/A	Admin must be able to verify login	Login verification successfully done	Pass
4	Manage Hospital & Department	Add Hospital & Departments	Admin must be able to Add hospital & department details	Admin is able to Add hospital & department details	Pass
5	Manage Data	Add data based on department	Admin must be able to manage data	Admin successfully Add data with Authorized access or General Access	Pass
6	Manage Doctors based on departments		Receptionist must be able to add doctors	Receptionist is able to add doctors	Pass

7	Map Doctor to Hospital		Receptionist must be able to map doctors	Receptionist is able to map doctors	Pass
8	Manage data request by doctor for authorized data		Admin must provide/Enable access rights to doctors to access data	Admin provides /enable access rights to doctors .	Pass

Test case:1

Test Case 2:

Step	Description	Input	Expected Result	Actual Result	Status
1	Open application	N/A	Application Home page should be displayed	Application Home page is displayed	Pass
2	Receptionist login	id:1414 password:12121	Receptionist login successful message must be displayed	Receptionist login successful message is displayed	Pass
3	Manage Patient	Add patient	Receptionist must be able to add patients	Receptionist is able to add patients	Pass

Comparison of timecomplexity between AES and DES algorithm

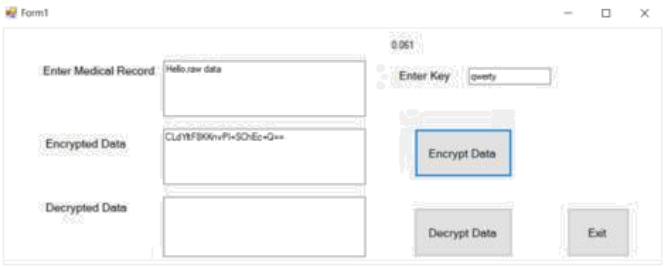

Figure 4:AES time complexity

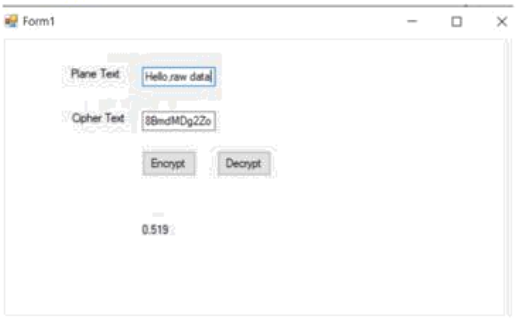

Figure 5: DES time complexity

VI. CONCLUSION AND FUTURE WORK

The project has described a new way in providing authentication and confidentiality while the information is delivering from the data center to doctor/patient using the Web Application,AES Rijndael Algorithms & Shamir's concept. It is scalable approach i.e., any number of doctor/patient can be added in the application.

The system can able to verify a user as an authenticated doctor/patient or not. The main goal achieved here is security and confidentiality of information.

REFERENCES

[1] U.S. Department of Health and Human Services. Cyber security: 10 best practices for the small healthcare environment.
[2] Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States. J. Am. Med. Assoc.
[3] Jannetti MC. Safeguarding patient information in electronic health records. AORN J. 2014;
[4] Vockley M. Safe and secure? Healthcare in the Cyberworld. J Biomed.Instrum. Technol. 2012
[5] Lemke J. Storage and security of personal health information.
[6] Chen YY, Lu JC, Jan JK. A secure EHR system based on hybrid clouds. J. Med. Syst. 2012.
[7] https://ijcsmc.com/docs/papers
[8] https://www.gsd.inesc-id.pt/~mpc/pubs/securing-electronic-health.pdf
[9] https://www.ironmountain.com/resources/general-articles/e/electronic-health-records-security-and-privacy-concerns

