Secure Medical Records System Using Cryptography

Rahul Sanas[1], Mukesh Sen[2], Suraj More[3], Ashok Kanthe[4]

[1] *Department of Computer Engineering, Pillai HOC College of Engineering and Technology, Rasayani, India*

Abstract- To achieve confidentiality, authentication, integrity of medical data, and support fine-grained access control. The medical data related to the patient is often vulnerable. The cyber-attacks are done on medical data. Hence, it is today's need to secure medical data. In this paper, the secure hospital system is proposed. We used MD5 algorithm for users, doctors, and admin login system, for all sensitive data that store in the database is encrypted by transparent database encryption, and when a user/patient try to access the pdf file i.e. contain information about prescription, bill payment, etc. it needs password before open the pdf. Each data is encrypted by AES Encryption to secure medical health records. AES encryption has a public key and hash value with a data file which is needed to be encrypted when data is encrypted it will form a unintelligible form so no other third party can read or access that file.

Indexed Terms- Cryptography, Symmetric Encryption, and Cloud Storage.

I. INTRODUCTION

The privacy of patients and the security of their information is the most imperative barrier to entry when considering the adoption of electronic health records in the healthcare industry. Considering current legal regulations, this review seeks to analyze and discuss prominent security techniques for healthcare organizations seeking to adopt a secure electronic health records system. Despite the many technological advances in health care over the past few decades, the typical patient record of today is remarkably similar to the patient record of 50 years ago. This failure of patient records to evolve is now creating additional stress. Cryptography techniques are more popular now a day's for data security. But the use of a single algorithm is not effective for high-level security to data in cloud computing. The Cryptography technique translates original data into an unreadable format. This technique uses keys for translating data so that only an authorized person can access the data. To encrypt large hospital data is through symmetric encryption, but that isn't very secure. A Primary Patient record is used by health care professionals while providing patient care services to review patient data or document their observations, actions, or instructions. The purpose of this project was to develop software for Medical records. Because records serve as the central repository for planning patient care and documenting communication among patient and health care provider and professionals contributing to the patients care.

In this paper, we proposed different algorithms with different purposes to provide security, integrity, and privacy to the patient's health records that are stored in database or cloud storage. At the start of the system MD5 Algorithm/Encryption technique is used to encrypt the data related to login details of a user, doctor, and admin. MD5 Algorithm was developed with the main motive of security as it takes an input of any size and produces an output if a 128-bit hash value and to store one way hash of a password. MD5 Algorithms are useful because it is easier to compare and store these smaller hashes than to store a large text of variable length. The MD5 algorithm is a widely used algorithm for one way hashes that are used to verify without necessarily giving the original value.

The huge amount of data is available for patient's health records and it will store and manage in a database called MariaDB. phpMyAdmin is a free web application that provides a convenient GUI for working with the databases like MariaDB database management system. It is the most popular MySQL administration tool that is used by millions of users worldwide. Over the storage concept security of this, all data is the main thing to do, so it will be secure with the TDE (Transparent Data Encryption) technique. Transparent Data Encryption (TDE) enables you to encrypt sensitive data that you store in tables and tablespaces. After the data is encrypted, this data is transparently decrypted for authorized users or applications when they access this data. TDE helps protect data stored on media (also called data at rest) if the storage media or data file is stolen. To prevent unauthorized decryption, TDE stores the encryption keys in a security module external to the database, called a Keystore. Too many chances of lack of data so the local database will be joined to the cloud storage because the cloud storage will be more beneficial for managing and accessing the data. Cloud Computing is a type of computing that is based on shared computing resources. It does not have any standalone servers or other devices to manage applications or process requests. In the case of Cloud storage, the data is stored on different remote servers and the user can access it from anywhere through the internet. It is maintained, operated and managed by a cloud storage service provider on storage servers.

To secure health records that contain information about patients, doctors, medicines, bill payments or a data transfer/receive from the cloud, etc. each data is encrypted by AES Encryption. This data is encrypted with a public key and hash value so it will form a non-readable form so an unauthorized person can not read and without key data is not accessible. AES requires the use of keys during the encryption and decryption processes, The keys used in AES encryption are the same keys used in AES decryption. AES uses different types of keys such as 128 bits, 192 bits, 256 bits. The higher bits are used dit provides more security. 128 bits provide lower security than other higher bits.

When it comes to a pdf file that is provided to the patient after treatment containing information about the patient (like illness, prescription, bill payments) it is only accessible to individual person or patient who logged in by its own user ID and Password, it can only download its own pdf file and its also accessible to the doctor the patient belongs to. If someone other patient or doctor trying to access a pdf of another patient it will not be download.

We used SSL Certificate On a Cloud. SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on cloud servers, it activates the padlock and the https protocol and allows secure connections from a cloud server to a browser. SSL certificates are used to create an encrypted channel between the client and the server. Transmission of such data as credit card details, account login information, any other sensitive information has to be encrypted to prevent attcacks.

II. LITERATURE SURVEY

In the paper [1], Authors presented that the use of a single algorithm was not efficient to provide security, so a new security mechanism using symmetric-key cryptography algorithm and steganography was introduced. A new method hybrid cryptography has been applied using AES and RSA. In this technique the symmetric key used for message encryption is also encrypted, which ensures better security.

In This paper [2], presents some recommendations for healthcare and also proposes a security framework for health records on the cloud. This framework can be an efficient tool for small-to-medium healthcare for a better vendor selection process. This framework will reduce the cost and increase quality.

In This paper [3], in this smart generation requires smart access to the clinical information on requirement basis, E-health systems are better options to maintain the medical connectivity globally, so they can be accessed from any place. This paper helps to shows how to ensuring privacy and security of E-health Records and also managing patients' data, authorization, authentication and encryption and decryption of data. Only one key is required for storage encryption and decryption. Securing network communication between server and client is the main perspective. For security reasons, appropriate communication protocols are required. These protocols have many disadvantages that can attract the attacker to intercept the communication between client and server. Drawbacks of the communication protocol include weakness against the known network attacks. It manages the Medical records and health records individually.

In the paper [4], In this paper to secure data from theft, they have introduced an idea of using the MD5 algorithm at the server to encrypt the original data before the transition and secure the personal information. Here, the MD5 algorithm is used for encrypting the personal data of the userWe use this technique in our framework to secure or encrypt the data of the user, doctor, and admin login information such as (User ID and Password).

III. PROPOSED METHODOLOGY

The proposed framework is based on the AES Encryption technique and TDE to secure the medical data. The architecture of the proposed work is depicted in the figure 1 below. First, the MD5 algorithm is used to encrypt the data related to the login details of a user, doctor, and admin. Encrypted Login details are also stored in a database in an encrypted form. In the given framework the AES and TDE Algorithms are used to encrypt the patient's records. Transparent Data Encryption used to encrypt the database and TDE uses the AES algorithm to do that. Now the database is encrypted so it will provide more security to the login information that comes from the MD5. Then the encrypted data are stored in the cloud so that it can be easily accessible from different hosts of that hospital. The different hosts of the hospital are considered for implementing the proposed system. There are three different hosts of the hospital Patient, Doctor, and Admin. Each user will have the login id and password by creating a new account to the database of the hospital. But an Admin is not a regular person like patients or doctors, admin login is very limited. The authorize admin login details are given only to one or two-person to maintain the framework. In the cloud storage, the Secure Sockets Layer Certificate is used to make an encrypted form of the channel to send and receive any information or file securely between the client and server.

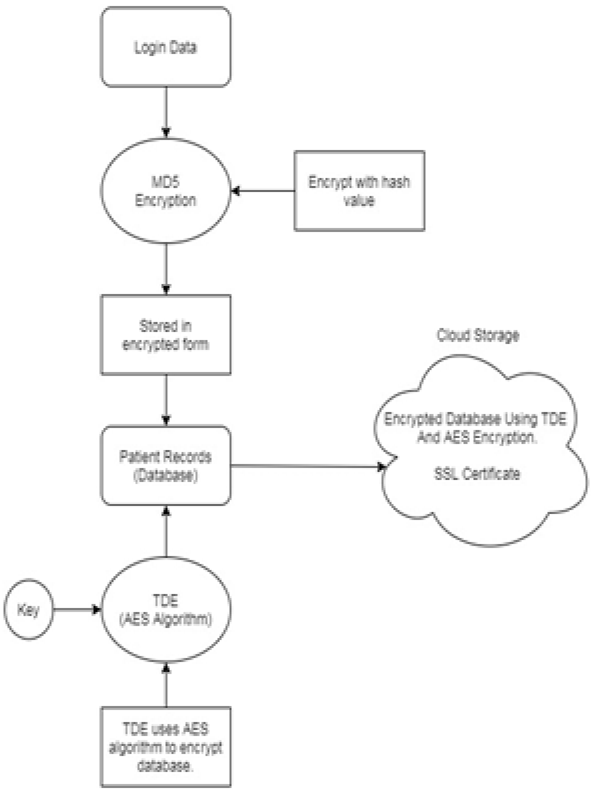

Figure 1 Proposed System Architecture

The patient host is responsible to make entry of new patients by taking complete details of patients like Patient name, address, mobile number, appointment date and time, department to visit, choosing of doctors, etc ., patient's entry can be done by the patient itself or by doctors or also by admin. The doctor's host can view booked appointments by the patients and approved them for a checkup. Each doctor can only view an appointment that the patient registered to them. The admin host is the main aspect of this framework. Each information about the department of the hospital like OPD, Radiology, Pharmacy etc., doctors of the hospital, and also the new patient's bookings, adding available medicine details, etc., is given or entered by the admin. Admin is only responsible to maintain this all information that is going to show on the website to patients and doctors and to itself.

IV. RESULTS AND DISCUSSIONS

The time required for encryption and decryption of a files with a different sizes are depend on speed of cloud server. High speed cloud storage is proposed in this framework. The data in files are encrypted using AES Algorithm and Database is encrypt by using TDE.

CONCLUSION

The system which hospital managements are using currently is extremely liable to data breach and is not available handy all the time. There's always the likelihood that data are often stolen, modified, or tampered. The information is maintained in an exceedingly record file or book manually and also the book is kept with the hospital staff. It's a awfully tedious job to look the mandatory records from the book and to take care of the book for a protracted time. Sometimes booking appointments by calling at the reception of the hospital take a long process and cannot process in the right way. The process is also very time consuming and hence there is a need for a system that maintains data properly and also keeps it secure and easy to use. Therefore patient logins to take an appointment by the patient itself with their selected doctor, doctor logins to approve appointments, admin host to maintain all hospital information, to add or remove doctors and patients, to add medicines that are available in a hospital, etc., and a system to store all these records efficiently so that they can be easily accessible is proposed in this paper.

REFERENCES

[1] Abdelali El Bouchti ,Samir Bahsani ,Tarik Nahhal - Encryption as a Service for Data Healthcare Cloud Security

[2] M. Plachkinova, A. Alluhaidan, S. Chatterjee,

Int'l Conf. Health Informatics and Medical

Systems, HIMS'15, pp. 152-158 (2015)

[3] Records – Jayneel Vora, Prit Italiya, Sudeep Tanwar, Sudhanshu Tyagi. - Ensuring Privacy and Security in Health, (2018)

[4] N.Jayapandian, R.Menagadevi, S.Abinaya, O.Sri Sampoorani. - To Enhance Consumer Privacy and Security For Online Shopping Using MD5 Algorithm, (2017)'