Enhanced Data Security in Cloud-based E-Health Care System

Asha Bhadra S Kumar[1]
[1]Student, Dept. Of Computer Science & Engineering, Mangalam College of Engineering, India,

Aswathy N[2]
[2]Student, Dept. Of Computer Science & Engineering, Mangalam College of Engineering, India,

Eizabeth K Jacob[3]
[3]Student, Dept. Of Computer Science & Engineering, Mangalam College of Engineering, India,

Arya Binu[4]
[4]Student, Dept. Of Computer Science & Engineering, Mangalam College of Engineering, India,

Ms. Divya S B[5]
[5]Assistant Professor, Dept. Of Computer Science & Engineering, Mangalam College of Engineering, India,

***Abstract*— : Medical Health Records are getting used in healthcare services to deal with the challenges and limits of paper-based techniques, but acceptance has been limited because of the high cost of implementation and storing data. Thanks to their unfamiliarity with electronic medical systems, many hospitals have relied on paper-based approaches. The foremost common concerns are counseling, data sharing, and authority delegation. Implementation of Medical Data Management Cloud computing in healthcare is currently a well-established trend. Additionally, the proposed model includes a patient data security mechanism that gives a high level of patient data confidentiality and authentication not found in existing applications**.

Keywords— Cloud, Cryptography, Authentication, Confidentiality

I. INTRODUCTION

An electronic health record (EHR) is an e-medical version which provides the medical reports in accessible way. EHRs has the flexibility to produce information about the patient care, in an exceedingly well secured form, to multiple authorized personal. Even though EHRs are varied in context and systematic approach of the record, they're often created to own the medical and treatment history records of the patient, as well as the particular patient's medications, diagnoses, radiology images, immunization dates, allergies, and laboratory test results, among other information. The relationship between a doctor and his patient wasn't as narrow as they're today. The doctor was concentrating primarily on the disease and wasn't necessarily fascinated by the patient's personal history. Of course, when a family is always followed by the identical doctor, this finally ends up creating links and allowing the latter to spot the personality of his patient and thus memorize his various interventions, which makes it possible to avoid always asking the identical questions. Each doctor had his own way of working, and without a decent memory, his consultations had to be written down. But if the patient changes doctor, he would should start everywhere again and the practitioner can't help asking inquiries to identify the illness from which his patient is suffering, especially within the case where the patient has various illnesses consulted by different specialists. In other words doctor's observations during a consultation weren't systematically recorded and even though they were, they might not be shared. But the prodigious development of bio science has created important problems with trust, transparency and accountability between health professionals and patients. The traceability of consultations has become practically essential and this concern is now reflected within the keeping of a medical file.

In this paper, we propose such a system where the patients data is protected with high confidentiality, to beat the paper based hospital data's the system will meet a necessary important role. The System is being mainly employed by the hospital administrations. The data is being stored to the cloud, here we use AWS Cloud as our cloud storage system, since cloud will provide high storage capacity and security it's a contemporary technology. this method also provide an external Security for the Patients Medical records using Cryptography. The remainder of the paper is organized as follows: Section II describes the
background and related works, Section III presents the present system , section IV provides the proposed methods, algorithms and Architecture of the system. Finally, in Section V, we present the conclusions and future works.

II. LITERATURE SURVEY

A. Secured Electronic Health Record Management System

An electronic health record (EHR) is an e-medical version which provides the medical reports in accessible way. EHRs has the flexibility to supply information about the patient care, in a very well secured form, to multiple authorized personal. Even though EHRs are varied in context and systematic approach of the record, they're often created to own the medical and treatment history records of the patient, as well as the particular patient's medications, diagnoses, radiology images, immunization dates, allergies, and laboratory test results, among other information. The Electronic record turns into a function through which the family practice industry can transform its practices to fulfil its needs and therefore the needs of its patients. The enhanced working algorithms and access to the data make the practicing of pharmacy needs more efficient for specialized physicians and their required staff. the choice support is provided and

their automated reminders help to practicing and delivering safer and high distinguishable care to patients and to the community. The electronic record is about quality needs and efficient works. it's a good function for specialized physicians and therefore the required patients. While getting the specified benefits of electronic record systems requires the eminent change of practices, which is predicated. upon the quality improving methods, system and team based medicine, and evidence-based care. This electronic record refers to the pc software which the physicians can use to trace all various aspects of patient cares.

B. M-Health Application for Managing a Patient's Medical Record based on the Cloud: Design and Implementation

The abandonment of the paper medium, which is gradually supplanted by the pc medium, has inspired public health policies in many industrialized countries, which tend to favor the transposition of medical data on Smartphone's. In fact, nowadays, the transportable isn't any longer used just for communications and also the exchange of short messages. New uses have appeared like email, Internet browsing, music, videos, etc. The generalization of mobile phones with large touch screens has raised new interests and particularly an interest during a broader view of the medical record the work applied during this paper consists in creating a mobile application for Android, offering the user the possibility of making and managing their Electronic Medical Record computer files within the type of XML documents stored in the Google Firebase Cloud. The mobile application will aim to make sure the right management of the patient's medical file in order that he can consult and manage his various medical documents. This application will make it easier for the user to access their file and monitor their state of health via a mobile terminal.

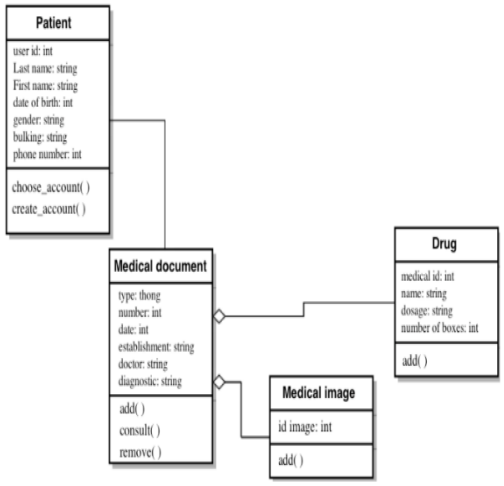

Figure 1 :UML Diagram

C. A Patient Data Management System for Medical Services and Training

When a physician visits a patient, he's within the middle of other medical personnel like nurses and resident students. After consulting the patient observation sheet and inspecting the patient's current health status, the physician makes observations that are noted by a nurse or a resident student, who then writes the notes into the patient's observation sheets after the visit. Thanks to the person taking notes, certain information is usually ignored or distorted. This document is used internally in hospitals, and thus the structure of the document varies looking forward to the patient's condition and thus the specialization accustomed treat the patient. The structure of the observation sheet is modified to produce better information for the physician to trace the patient's healing progress. Storing patient data in an electronic format encompasses variety of advantages, but it also raises certain issues about data security and privacy. Multiple professionals examined the privacy of patient clinical observation sheets specifically, additionally as Electronic Medical Records (EMR) normally, and presented their findings in multiple articles within the literature

D. Improving the information security of personal e-health records to protect a patient's health Information

PEHRs (personal electronic health records) are a set of online technologies that connect individuals to their medical information and enable them to control their own health.as well as healthcare PEHRs allow for the collecting of health data. Information in a single location in order to establish an efficient system Pathway of communication between patients and healthcare providers, as long as essential data can be provided. Furthermore, PEHRs aid in the reduction of medical errors and the improvement of patient care. Health conditions are being monitored. As a result, patients can More effectively monitor and enhance their health status. The health information of a patient is deemed confidential.as well as private. The term "privacy" refers to a person's ability to keep his or her personal information private. Keep personal information private while expressing oneself selectively with this information As a result, if PEHRs are to be taken seriously, a role in the delivery of a fully integrated and successful Information security controls must be in place in healthcare. That way, the patient's privacy will be protected. A person has the ability to manage and control their personal health information (PHI) through the use of programs that are commercially available and span from mobile to desktop devices to Web- or Cloud-based services, resulting in the creation of additional For the patients, accessibility and convenience are important.

E. Design of e-Healthcare Management System Based on Cloud and Service Oriented Architecture

People's demands for medical computers are growing in various areas of healthcare. Extension of communication and information technology system, as well as dispensing massive amounts of medical information. It is crucial to have information systems. Some private hospitals and clinics use a computer-based data system to keep track of their patients, but there is no formal mechanism in place for exchanging information. The e-healthcare management system in Iraq has been proposed in this paper as a model for improving medicinal services. Health information is largely stored by digitalized record system and it falls into two groups: client-server or cloud based. A medical practitioner's data stored in cloud-based system on external servers and will be accessed

through the online needing merely a computer having an online connection. Data is stored in-house by client-server systems, needing a server, software and hardware be installed within the office of the physician. Electronic health card which is kept in patient is complete and accurate. All the medical information are often accessed by the doctor through patient's identity causing the treatment best. The proposed system shows an e-Healthcare management system in Iraq, where the patient details are required to store in a central database. It is based on two main technology Service Oriented Architecture (SOA) and cloud services. SOA is a architecture not a technology which most IT giants use to handle their enterprise more effectively and in more agile way. In simple terms, it is a middleware solution which makes two system to communicate with each other. This system keeps or maintain separate records for each patient reports such as X-rays, Lab test in cloud database. In addition to that, health insurance of the respective patient is also included. For each patient there is a health card which has the details of the patients and it is stored in cloud.

III. EXISITING MODEL

Privacy is an key concept. Privacy is an increasingly imperative concern when considering information system that collect personal and sensitive user data. There may be cyber threats to the data record. Most organizations provide e-services to identify and manage the personal information of patient.

Data breaches can lead to malicious activities and can damage both personal and organizational front. To secure the data record developed a conceptual framework with three distinct and sequential phases. The first phase is defined as the planning to identify the key limitations of contemporary frameworks so these can be minimized to ensure privacy in each layer of data processing. The second phase incorporates the key components of data privacy to satisfy the efficiency and effectiveness of the proposed framework. Finally, the third phase is the implementation of the selected requirements of the assessment phase to prevent privacy incursion events in PRMS. After all the phases, the complete framework is anticipated to deliver a sophisticated resistance in contradiction to the continuous data breaches in the patients' information domain.

This framework is built with an accumulation of privacy by choice fundamental principles, privacy design strategies, standards, and privacy impact assessment that deliver an in depth privacy preserving environment in PRMS. The healthcare systems which employed the prevailing frameworks are behind to supply an entirely privacy-protected system, as desirable data privacy mechanisms don't seem to be properly consumed by the prevailing frameworks. a scientific activity is dispensed within the this framework through three identified phases of system design named the look phase, assessment phase, and implementation phase. the aim of the this framework is to include the mandatory data privacy mechanisms in a specific place while analyzing, managing, and keeping personal information, thus the healthcare system can ensure maximum privacy to the non-public data. Besides, the identified limitations that are acknowledged in our work are going

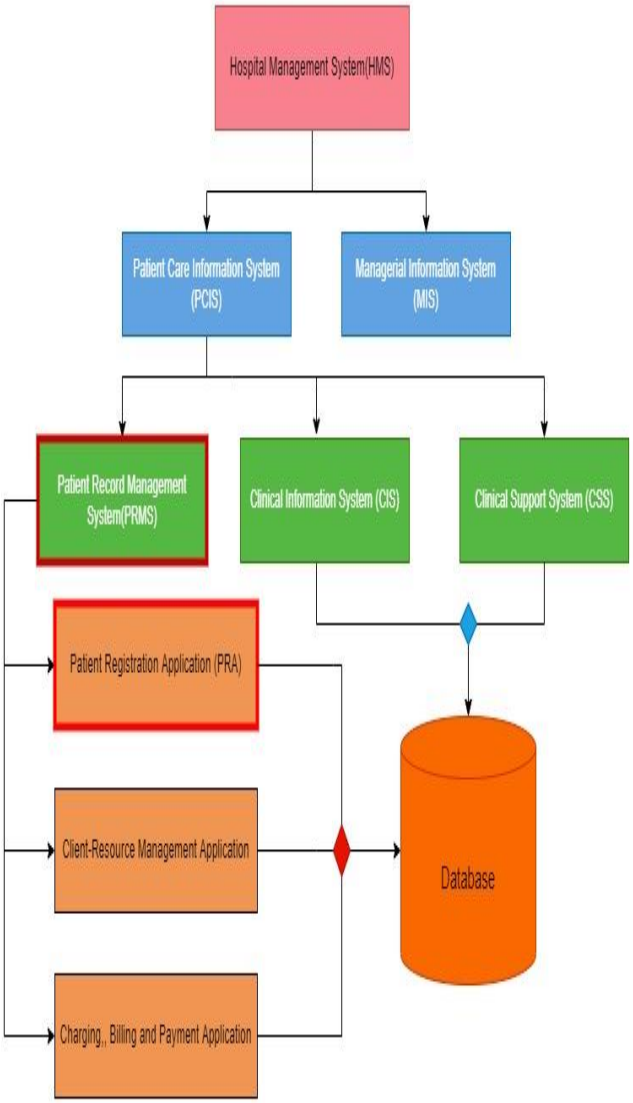

Figure 2: Relations of Patient Record Management System (PRMS)

to be eliminated. The anticipated framework will ensure a complicated healthcare system incorporating privacy contexts compatible with the .NET Core framework. Implementing each of the proposed requirements will facilitate overcoming the gaps with complete privacy protection to realize the specified outcome. The resulting framework will guarantee the integrity and confidentiality of PRMS while delivering high-level integration and allocation of non-public data to decrease data breaches globally.

PCIS involves patients' personal and medical information, which are collected, managed, and released by this technique. PCIS mainly consists of three sub-systems:

1) PATIENT RECORD MANAGEMENT SYSTEM
PRMS could be a sub-system of PCIS and consists of applications that enable care providers to stay track of individual or groups of patients in an exceedingly fast, responsive, flexible, and friendly manner with efficient use of accessible resources.

2) CLINICAL data system (CIS)
CIS facilitates patient care directly like activities for care Providers primarily doctors, nurses and medical professionals.

3) CLINICAL network (CSS)
CSS provides services to perform tests and supply supplies based on the tests. Care providers request these facilities through the CSS

IV. METHODOLOGY

A. Proposed System

The system propose an online app where the patient's data is stored within the application. Patient's personal details, Bi- stander details, Insurance, Previous anamnesis history all are collected and data is stored to AWS Cloud and supply external security using Cryptography. The patient's data is in Encrypted format for the person, a collection of hospitals are added to the system which are being using this method. when a patient is spoken other hospital this hospital send details to the well-liked hospital in encrypted format the receiving hospital decrypt the information.

B. Algorithm

The user sign in with the basic details and make themselves an account. The communication between the users is done by this application. The practice of encrypting crucial data when sending data from one computer to another or keeping data on a computer is known as cryptography. Fernet is a block cipher mechanism that ensures the encrypted message cannot be altered or read without the key. The keys are encoded using URL safe encoding. Fernet also employs 128-bit AES in CBC mode with PKCS7 padding, with HMAC authentication based on SHA256. Python supplies a cryptography package that aids in the encryption and decryption of data. Using the encrypt and decrypt methods, the fernet module of the cryptography package offers built functions for generating the key, converting plaintext to ciphertext, and decrypting ciphertext back to plaintext.

Methods used:

generate_key(): A fresh fernet key is generated using this procedure. The key must be kept secure because it is required to decipher the ciphertext. The user will be unable to decrypt the communication if the key is lost.

encrypt(data): A "Fernet token," or ciphertext, is the result of this encryption. When it was generated in plaintext, the encrypted token also included the current timestamp. If the data isn't in bytes, the encrypt procedure will fail.

decrypt(token, ttl= None): The Fernet token given as a parameter is decrypted by this procedure. The original plaintext is returned if the decryption is successful; otherwise, an exception is thrown. token (bytes), the Fernet token (ciphertext) is passed for decryption. The 'ttl' denotes the time about how long a token is valid.

The following command is used to install the cryptography package: `pip install cryptography`

'from cryptography.fernet import Fernet' is used to import Fernet module from cryptography package

E.System Architecture

The system can be used by the Hospital Administration by providing them with login/sign-in credentials. The Sign-in log() function is used for this. Separate areas for conducting various tasks can be found on the Home Page. If the patient's injury is reported as a police case, the hospital can send out an email alert to a nearby police station.

The details of the referred patients are also displayed on the home page; for example, if a patient is referred from Hospital A to Hospital B for medical treatment, Hospital B can examine the patient's history records. The CSV file is compared to the mentioned patient's CSVid. If a matching id is identified, the details are displayed in a row. When a doctor consults with a patient, the patient's data is updated that is stored in the cloud. Images are saved in a folder and data is added to a CSV file of each patient. The functions encrypt() and decrypt() are used to encrypt and decode data.

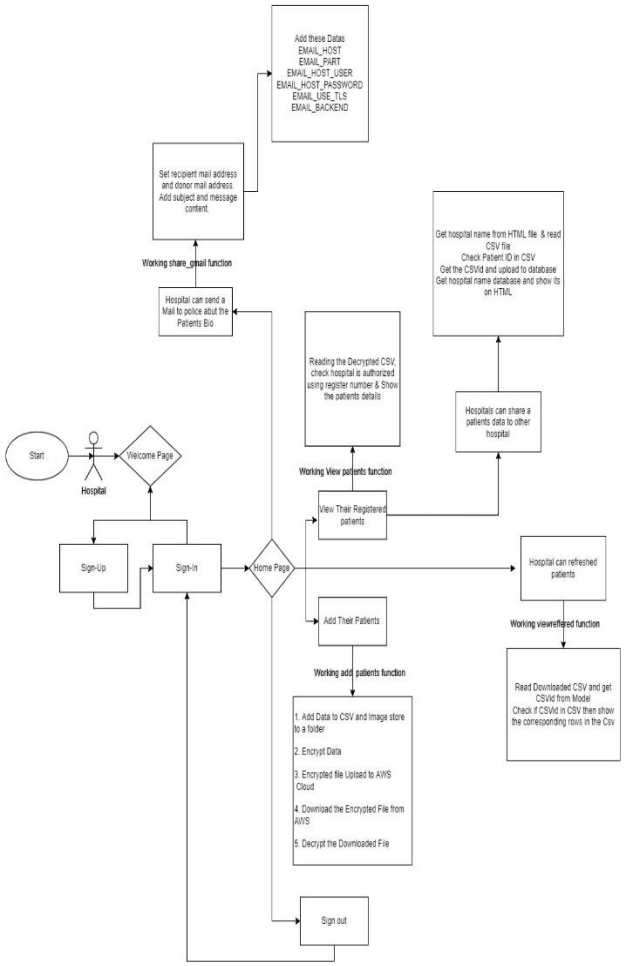

Figure 3: System Architecture

V. FUTURE SCOPE

The E – Health care system is presently growing very fastly during this epoch, high security and confidentiality we providing for the patients personal data is that the main reason for this sudden change. This project will be improved to an open software form with the specifications like data storing to the cloud & provide an external security of Block chain Security. Currently this feature display as an internet app that's we upgrade to an open software, which is to be mainly using for the hospital administrations and also identifies the threats and vulnerabilities in health care.

VI. CONCLUSION

The paper presents a system that was conceived to scale back the overload of physicians within the hospital and to help them within the process of recording the observations within the patient clinical observation sheet.

The cloud architecture offers a web-enabled framework that integrates with the activities of doctors, prescribers, and laboratory personnel. Using the e-Health Cloud, the administration engages with businesses and professionals to develop the entire healthcare system. Health-care security should aim to enhance the quality of healthcare while cutting costs.

Our model aims at protecting health care from unauthorize users' attacks. The research looks at sophisticated multifact or
authenticaticated health records that are secure in the cloud. The new security system is more secure than prior system security.

ACKNOWLEDGEMENT

The authors wish to thank Principal Dr.Vinodh P Vijayan, Dr.Ranju S Kartha, H.O.D, Computer Science Department,for the proper guidance, valuable support, and helpful comments during the proofreading.

REFERENCES

[1] A Conceptual Framework to Ensure Privacy in Patient Record Management System, December, 2021IEEEAccessPP(99):11,DOI:10.1109/ACCESS.2021.3134873Available:https://ieeexplore.ieee.org/document/9646903
[2] Development of a Mobile Application for Patient's Medical Record and History Available: https://ieeexplore.ieee.org/document/9454227
[3] Secured Electronic Health Record Management System Available: https://ieeexplore.ieee.org/document/8724010
[4] M-Health Application for Managing a Patient's Medical Record based on the Cloud: Design and Implementation,DOI:10.1109/IHSH51661.2021.9378744,Available: https://ieeexplore.ieee.org/document/9378744
[5] Improving the information security of personal electronic health records to protect a patient's health information, Date Added to IEEE Xplore: 08 May 2017, Date of Conference: 8-10 March 2017,DOI: 10.1109/ICTAS.2017.7920658, Available: https://ieeexplore.ieee.org/document/7920658
[6] Medical Records Management Using Cloud Technology,DOI:10.1109/ICESC51422.2021.9532675Available:https://ieeexplore.ieee.org/document/9532675
[7] Improving The Efficiency of E-Healthcare System Based on Cloud, Available: https://ieeexplore.ieee.org/document/8701387
[8] Securing Personal Health Records using Advanced Multi-Factor Authentication in Cloud Computing, Available :https://www.ijrte.org/wpcontent/uploads/papers/v8i6/F9724038620.pdf
[9] Ensuring Privacy and Security in E- Health Records, Available at: https://ieeexplore.ieee.org/document/8440164
[10] Enhanced e-Health Framework for Security and Privacy in Healthcare System, Available at: https://ieeexplore.ieee.org/document/7470795
[11] A Patient Data Management System for Medical Services and Training,Available at: https://ieeexplore.ieee.org/document/8424792
[12] An Electronic Medical Record Management System based on Smart Contracts, Available at: https://ieeexplore.ieee.org/document/9049592
[13] Design of e-Healthcare Management System Based on Cloud and Service Oriented Architecture, Available at: https://ieeexplore.ieee.org/document/7391393