Integrated Electronic Health Records (EHR) Platform: Enhancing Patient-Centric Healthcare Management

Mr Madar Bandu[1], K. Sai Sandeep Reddy[2], P. Meghana Reddy[3], Siddharth T[4], V. Rishikesh[5]

[1,2,3,4,5]Department of Computer Science and Engineering, Anurag University Hyderabad Telangana.

Abstract: In contemporary healthcare systems, digitizing medical records has become imperative to streamline and enhance patient care. This research paper explores the development and implementation of a website that integrates patients' medical records, aiming to provide a comprehensive and patient-centric approach to healthcare management. The platform seeks to facilitate seamless information exchange among healthcare providers, improve treatment decision-making, and empower patients in managing their health.

1. Introduction

1.1 Background

The developed application focuses on making electronic health records easier to store, and access, and the integration of the data is not compromised. It addresses a significant challenge that patients and hospitals commonly face when it comes to patient records. [1] The problems may include the inability to store or access the records, and the security and privacy of data. [2] These problems arise when the records are stored only on paper or different hospitals have different systems to store the records. [6] The application aims to provide both patients and hospitals with a common platform where everyone can access the records when needed and everything is stored accordingly. Additionally, it also aims to make the treatment, medication, and tests faster by saving the data and providing a clear summarization so that there is no further need to undergo tests that have already been done and recorded. [3] The application also stores previously undergone treatments and medications and their reactions so there is a record that contains any allergies that should be kept in mind. By integrating these functions, the applications aim to make the treatment, medication, storing, and accessing the records faster and in an efficient manner. Additionally, the awareness of the patient about their medical history is also given the same level of importance through this application.

2. Literature Review

2.1 The Role of EHR in Healthcare

There has been immense research done on the existing models of EHR and many methods are used to implement them. The impact of this research has proven to be of great value as these models have improved the pre-existing models. [1] Using the PDFM or privacy-free data fusion and mining has been proven to be beneficial when it comes to providing a health-service platform that is time-efficient and a privacy-preserving platform. However, when it comes to fusing different privacy protection solutions and integrating different keywords of the same data, it does not perform well. [2] When we use the hybrid ontology method, it certainly eliminates heterogeneity in data which makes storing different records easier. The problem arises when the patient needs to either search or share the data, using hybrid ontology has proven to be inefficient. [3] The use of blockchain has become prominent in many industries but it has its limitations due to the lack of exploration or the interoperability and correction of any mistake. Using blockchain has proven to have high implementation costs and the inability to focus on managing multiple databases at once. There is, however, very high security and more privacy when blockchain is used.

2.2 Challenges in Current EHR Systems

The EHR systems have been evolving rapidly with new technology emerging, yet there is a difficulty in storing, accessing, and sharing all the records from one platform. There are issues when it comes to interoperability through the app when approaches like blockchain are used to store the data. Data security becomes inefficient when the data is not encrypted or any unsafe databases are used to store the data. The patient engagement becomes less efficient when the patient is required to do a lot of work when it comes to maintaining the records. The storing, handling, and management is not a good experience for the patient.

3. Methodology

3.1 System Architecture

Frontend Development: The frontend is the user-facing part of the application. We are using React to build interactive and user-friendly interfaces for healthcare providers to input and access patient data.

Backend Development: The backend is responsible for processing requests, managing data, and executing business logic. We are using Python, along with the framework Flask for the backend.

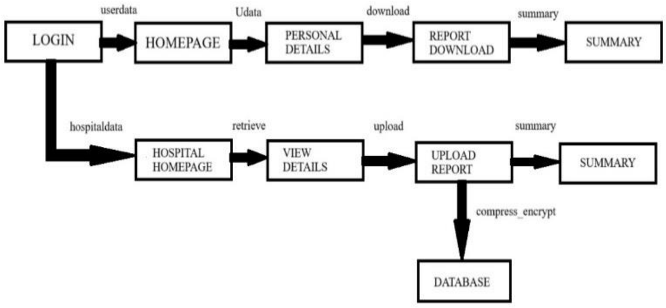
Database Management: Patient records, medical histories, and other healthcare data are stored in databases. We are using SQLite3 a file-based database system.

APIs (Application Programming Interfaces): APIs enable communication between different components of the System. RESTful APIs are being used to facilitate data exchange between the frontend and backend. For our application to run efficiently, we created our APIs using Flask REST APIs.

The HospitalData and UserData APIs are used for the hospital login and user login respectively. The Register Api is for the signing up of new users. The Udata is the API responsible for the patient easily filling up the general form. The Upload API aims to make the uploading of the records easy. The Retrieve and RetrieveP are the APIs that are responsible for fetching the records from the database. The download and downloadp APIs are used to make the downloading of the files efficient. Summary and Summaryid are the two APIs that retrieve the summary of the patient record from the database and display it.

Security Mechanisms: Robust authentication (verifying user identity) and authorization (determining user access levels) are crucial for protecting patient data. We are employing Flask Security too for security.

Data Security and Compliance: Encryption techniques like AES, 3DES are used in the current system to secure the medical reports of the patients in the database.



3.2 Data Security and Privacy Measures

Encryption:

AES and 3DES: These are robust symmetric encryption algorithms. Use them to encrypt medical records both during transmission and when stored in the database. AES is widely adopted for its strength and efficiency, while 3DES, although less common today, may still be used in certain legacy systems.

Key Management:

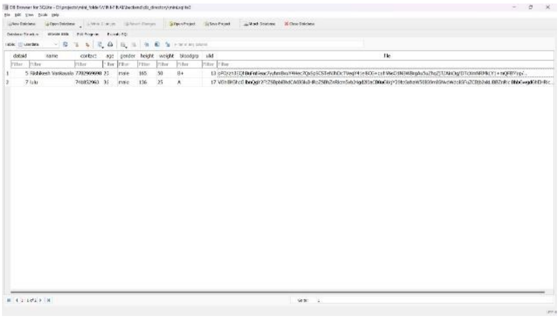
Safeguard encryption keys, as they are crucial for decrypting data. Utilize secure key storage mechanisms and consider hardware security modules (HSMs) to protect keys from unauthorized access.

3.3 Algorithms Used

AES: The Advanced Encryption Standard (AES) is a widely adopted symmetric key algorithm that operates on fixed-size blocks of 128 bits. It supports key sizes of 128, 192, and 256 bits, with the number of rounds varying accordingly (10 rounds for 128-bit keys, 12 for 192, and 14 for 256). Employing a Substitution-Permutation Network (SPN) structure, AES incorporates key expansion to generate unique round keys and utilizes operations such as byte substitution, shift rows, mix columns, and add round key in each round. The algorithm employs principles of diffusion and confusion for enhanced security, ensuring that changes in one bit of the plaintext have a widespread impact on the ciphertext, and the relationship between the key and ciphertext is intricate. As of my last knowledge update in January 2022, AES is considered highly secure and is extensively used for encrypting data in various applications, including securing internet communications and protecting sensitive information. It is important to stay informed about the latest developments in cryptographic standards to ensure the continued effectiveness of security measures.

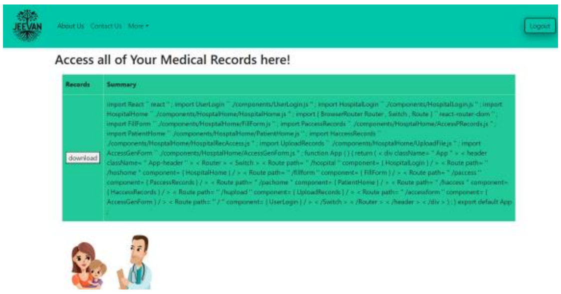
3DES: 3DES also known as Triple Data Encryption Algorithm (TDEA), is a symmetric key block cipher designed to enhance the security of the original Data Encryption Standard (DES). In 3DES, the DES algorithm is applied three times consecutively in a process known as Encrypt, Decrypt, Encrypt (EDE). It operates on fixed-size blocks of 64 bits and offers three keying options: 2TDEA (Double DES), which employs two different keys for encryption, decryption, and encryption; and 3TDEA (Triple DES), which utilizes three different keys for the three passes. The key size options include 56, 112, or 168 bits, achieved by using three 56-bit DES keys. While 3DES has been widely used for its increased security over the original DES, its usage has diminished with the advent of more modern and efficient symmetric key algorithms, such as AES. Despite its enhanced security, 3DES is relatively slow compared to contemporary encryption algorithms, prompting consideration of newer options for applications requiring robust security measures. It's essential to stay informed about evolving cryptographic standards and make informed choices based on the latest advancements in encryption technology.

3.4 Sample Data



	dataid	name	contact	age	gender	height	weight	bloodgrp	uid	file
1	5	Rishikesh Vankayala	7702969698	23	male	165	50	B+	13	[illegible]
2	7	lulu	7416852963	35	male	136	25	A	17	[illegible]

The above figure displays how the encryption algorithms play a role and encrypt the data, safeguarding it from any intruders. The decompressed and decrypted data can only be accessed by the authorized users.

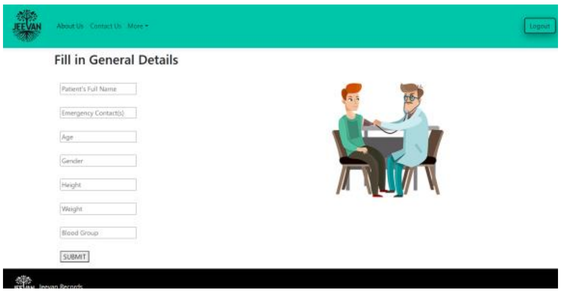


Access all of Your Medical Records here!

Records	Summary
download	import React " react " ; import UserLogin " ./components/UserLogin.js " ; import HospitalLogin " ./components/HospitalLogin.js " ; import HospitalHome " ./components/HosptalHome/HospitalHome.js " ; import { BrowserRouter Router , Switch , Route } " react-router-dom " ; import FillForm " ./components/HosptalHome/FillForm.js " ; import PaccessRecords " ./components/HosptalHome/AccessPRecords.js " ; import PatientHome " ./components/HosptalHome/PatientHome.js " ; import HaccessRecords " ./components/HosptalHome/HospitalRecAccess.js " ; import UploadRecords " ./components/HosptalHome/UploadFile.js " ; import AccessGenForm " ./components/HosptalHome/AccessGenForm.js " ; function App ( ) { return (< div className= " App " > < header className= " App-header " > < Router > < Switch > < Route path= " /hospital " component= { HospitalLogin } / > < Route path= " /hoshome " component= { HospitalHome } / > < Route path= " /fillform " component= { FillForm } / > < Route path= " /paccess " component= { PaccessRecords } / > < Route path= " /pachome " component= { PatientHome } / > < Route path= " /haccess " component= { HaccessRecords } / > < Route path= " /hupload " component= { UploadRecords } / > < Route path= " /accessform " component= { AccessGenForm } / > < Route path= " / " component= { UserLogin } / > < /Switch > < /Router > < /header > < /div >) ; } export default App

The above figure displays how the decryption works and only authorized users will be able to access and download the decrypted file as well as the summary of the decrypted file will be displayed next to it.

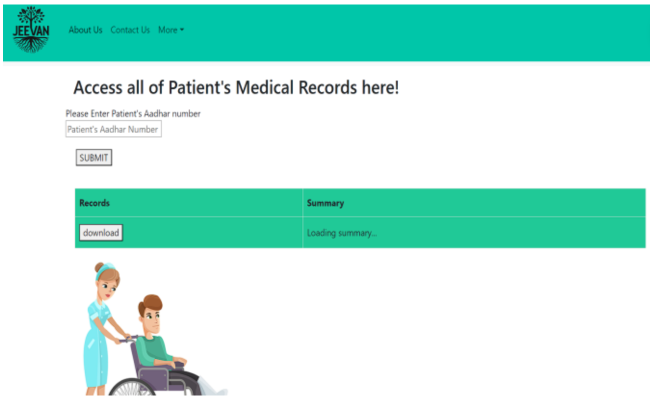
4. Results and Evaluation



Fill in General Details

Patient's Full Name
Emergency Contact(s)
Age
Gender
Height
Weight
Blood Group
SUBMIT

Fillform.js- This file contains the UI definition of the page where the patient will have to fill in their general details as they login for the first time. The general details consist of the patient's full name, Emergency contacts, Age, Gender, Height, Weight, and blood group. These details can be accessed by the hospital in cases of emergency and the treatment can be done faster.



Access all of Patient's Medical Records here!

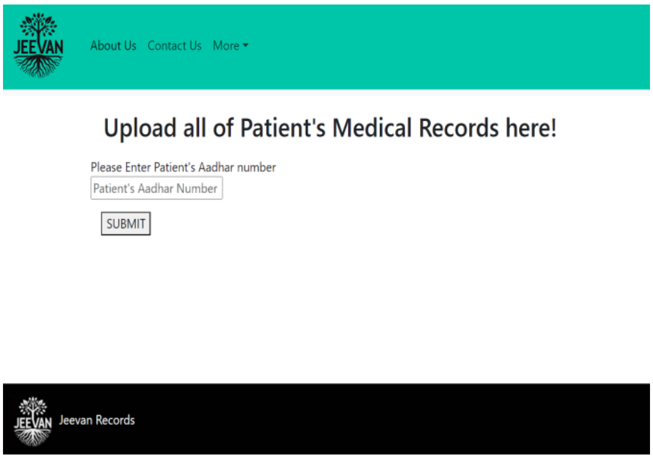
Please Enter Patient's Aadhar number

Patient's Aadhar Number

SUBMIT

Records	Summary
download	Loading summary..

AccessRecords.js - This page contains access to the patient records. Once the hospital gives the Aadhar number of the patient whose records they want to access, the records are available to view, and download, and the summary of it is also available. This helps the hospital to view the patient history of medical records. All the data is encrypted so that no other parties can access it but it is decrypted to the hospital when they need to access it.



Upload all of Patient's Medical Records here!

Please Enter Patient's Aadhar number

Patient's Aadhar Number

SUBMIT

UploadFiles.js - This page contains access to the patient records by their Aadhar number. They can add the medical records of the patient who is diagnosed in their hospital. This gets stored in the SQLite database to be accessed by both the hospital and the patient**.**

5. Conclusion

In concluding the implementation of strategies for ensuring patient medical records' confidentiality and integrity, key achievements include deploying robust encryption algorithms (AES, 3DES) at database and transit levels, enhancing overall security. The project aligns with healthcare data protection regulations (HIPAA, GDPR), conducting regular risk assessments. Thorough data classification, strict access controls, and a robust key management system ensure data security. Effective incident response, real-time monitoring, and user training address security incidents and human-related risks. Regular security audits and communication with stakeholders maintain resilience against evolving cybersecurity challenges. The successful implementation establishes trust in medical records' secure management, emphasizing ongoing vigilance in the evolving healthcare landscape.

6. References

- [1] Quingguo Zhang, Bizhen Lian, Ping Cao, Yong Sang, Wanli Huang, and Liang Qi, "Multi-Source Medical Data Integration and Mining for Healthcare Services", *IEEE Access, vol.8, pp.165010-165017, 2020.*
- [2] "Computer-based patient record data integration method based on ontology" by Cai Xiufen, Xu Yabin in 2011 at IEEE International Symposium on IT in Medicine and Education.
- [3] Hao Jin, Yan Luo, Peilong Li and Jomol Mathew, "A Review of Secure and Privacy-

Preserving Medical Data Sharing”, *IEEE Access, vol.7, pp.61656-61669, 2019.*

- [4] S. Din and A. Paul, ‘‘Smart health monitoring and management system: Toward autonomous wearable sensing for Internet of Things using big data analytics,’’ Future Gener. Comput. Syst., vol. 111, p. 939, Feb. 2020.
- [5] N. C. Benda, T. C. Veinot, C. J. Sieck, and J. S. Ancker, ‘‘Broadband Internet access is a social determinant of health!,’’ Amer. J. Public Health, vol. 110, no. 8, pp. 1123–1125, Aug. 2020.
- [6] E. Sillence, J. M. Blythe, P. Briggs, and M. Moss, ‘‘A revised model of trust in Internet-based health information and advice: Cross-sectional questionnaire study,’’ J. Med. Internet Res., vol. 21, no. 11, Nov. 2019, Art. no. e11125.
- [7] K. Szulc and M. Duplaga, ‘‘The impact of Internet use on mental wellbeing and health behaviors among persons with disability,’’ Eur. J. Public Health, vol. 29, no. 4, pp. 185–425, Nov. 2019.
- [8] T. Peng, Y. Lin, X. Yao, and W. Zhang, ‘‘An efficient ranked multi-keyword search for multiple data owners over encrypted cloud data,’’ IEEE Access, vol. 6, pp. 21924–21933, 2018.
- [9] H. Dai, Y. Ji, G. Yang, H. Huang, and X. Yi, ‘‘A privacy-preserving multi-keyword ranked search over encrypted data in hybrid clouds,’’ IEEE Access, vol. 8, pp. 4895–4907, 2020