A Major Project Report

on

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

Submitted in partial fulfilment of the requirements for the award of the degree

BACHELOR OF TECHOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

by

Siddharth Thirkateh
(20EG105146)

K. Sai Sandeep Reddy
(20EG105123)

V. Rishikesh
(20EG105159)

P. Meghana Reddy
(20EG105136)

Under The Guidance of

Mr. Madar Bandu

Assistant Professor, CSE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ANURAG UNIVERSITY

VENKATAPUR– 500088

TELANGANA.

Year 2023-2024

CERTIFICATE

This is to certify that the Report entitled "**Integrated Electronic Health Records Platform: Enhancing Patient-Centric Healthcare Management**" that is being submitted by Siddharth Thirkateh (20EG105146), K. Sai Sandeep (20EG105123), Rishikesh Vankayala (20EG105159) and P. Meghana Reddy (20EG105136) in partial fulfilment for the award of B.Tech in Computer Science and Engineering to the Anurag University is a record of bonafide work carried out by them under our guidance and supervision.

The results embodied in this Report have not been submitted to any other university or Institute for the award of any degree or diploma.

Signature of the Supervisor
Mr. Madar Bandu
Assistant Professor, CSE

Dr. G. Vishnu Murthy
Dean, Dept. of CSE

External Examiner

DECLARATION

We hereby declare that the report entitled "**Integrated Electronic Health Records Platform: Enhancing Patient-Centric Healthcare Management**" submitted for the award of Bachelor of Technology Degree is our own work and the Report has not formed the basis for the award of any degree, diploma, associate ship or fellowship of similar other titles. It has not been submitted to any other University or Institution for the award of any degree or diploma.

Place: Anurag University, Hyderabad

Siddharth Thirkateh
(20EG105146)

K. Sai Sandeep
(20EG105123)

Rishikesh Vankayala
(20EG105159)

P. Meghana Reddy
(20EG105136)

ACKNOWLEDGMENT

We would like to express our sincere thanks and deep sense of gratitude to project supervisor **Mr. Madar Bandu** for his constant encouragement and inspiring guidance without which this project could not have been completed. His critical reviews and constructive comments improved our grasp of the subject and steered to the fruitful completion of the work. His patience, guidance and encouragement made this project possible.

We would like to express our special thanks to **Dr. V. Vijaya Kumar**, Dean School of Engineering, Anurag University, for their encouragement and timely support in our B.Tech program.

We would like to acknowledge our sincere gratitude for the support extended by **Dr. G. Vishnu Murthy**, Dean, Dept. of CSE, Anurag University. We also express our deep sense of gratitude to **Dr. V V S S S Balaram**, Academic Co-Ordinator, **Dr. Pallam Ravi,** Project in-charge**, Dr. G. Prabhakar Raju,** Project Co-Ordinator and Project review committee members, whose research expertise and commitment to the highest standards continuously motivated us during the crucial stage our project work.

ABSTRACT

In modern healthcare systems, digitalizing medical records is crucial for optimizing patient care. This project investigates the creation and execution of a website designed to merge patients' medical records, with the goal of offering a holistic and patient-focused approach to healthcare management. The platform aims to streamline the exchange of information among healthcare providers, enhance treatment decision-making processes, and empower patients to take an active role in their healthcare. By centralizing healthcare data on a digital platform, this initiative aims to revolutionize traditional healthcare practices and ultimately improve patient outcomes.

LIST OF FIGURES

LIST OF TABLES

INDEX

1. INTRODUCTION

1.1 Overview

We can see how the patients' records, to this day, are scattered across many providers, facilities, or even on paper. The lengthy process of filling up a new form with each visit to a new doctor, or filling up a patient's details in the system all over again is a time-consuming and inefficient method to maintain a health record. The hospitals have to conduct the tests again and the patient's communication about the previous results of the tests is generally ignored due to lack of central proof of all the data. This can result in being time-consuming, inefficient, and expensive.

Patient Health Records (PHR) not only encourage the patients to keep track of their health records, store and manage them but also make it easier for them to share the health records whenever necessary. These PHRs make the maintenance of the records easier but, when facing an emergency, the same repeat of tests, checking of medical history, and need to fill up the general details is required. This will again prove to be a time-consuming and expensive affair. When collecting records from different organizations, the terms start to differ from organization to organization and this might cause a problem in cases of emergencies when one organization tries to interpret the different terms. This is the reason if all the records need to be in the same place, then the integration of data will play an important role. Using ontology as suggested may cause issues while displaying the data or compromise the efficiency of the application. The solution to this is by using new technology like NLP so that the model is much more efficient.

As technology advances day by day, cyber threats are increasing exponentially too, Electronic Health Records (EHR) have not been spared either. The security of health records is very important as tampering with these records can result in fatality in some cases. The patient's personal details, health records, and many other aspects of the EHR like storage and access need to be secured from intruders, and unfortunately not much action has been taken in this regard.

To solve these issues, we have developed a web-based Health Record System that can be used by both hospitals and patients to access, manage, and store medical history (e.g. allergies, medical history, past medications, test results, surgeries, ongoing treatments, and more.) We have tried to make our system efficient and cost-friendly; our model lets the hospital access the patient's medical records and even upload the records after the consultation. This helps not only in access to the patient's records in emergencies but also makes it easier for patients to maintain their records.

1.2 Objective

To solve the disadvantages in the referred model, we use modern day technologies such as react framework so the sharing and displaying of data to the particular patient becomes efficient and use *Pegasus* to easily summarize the data and eliminate the heterogeneity of data collected from all the patient records throughout. Encryption of records of the patients for providing security to the records as it is the most sensitive information.

2. LITERATURE REVIEW

2.1 Overview

The study reflects on the research on the protection of data while storing and transferring them, the records are stored in a Protected Spreadsheet Container with Data (PROSPECD) which integrates encrypted access control policies with watermarked clinical and administrative data for advanced security measures.[4]

In parallel, a research study highlights the use of blockchain technology to store the data and the patient's records. In this case, the data which is stored is safe and secure but it is immutable, so no data or records that are entered can be changed at any cost. This might not prove to be cost-efficient.[5]

The study on keeping the data safe, where the data on the client's side is masked using AES-256 and Blowfish encryption highlights the security of the data from any external threats.[6]

The primary objective of this research is to monitor and store the activities of the patient through which we will be able to come to certain conclusions as to how certain medications are working on the respective patients and how to enhance the effect of the medications on the patient.[7]

The methodology of this paper involves the security of data using the proposed multi-source IOH (Internet of Health) data fusion and mining method.[8]

The authors proposed an extensive model with intricate research on how private institutions can share data securely through the cloud and cryptography approach and to make the model even more secure, the integration of blockchain is included in the research.[9]

These literature survey reviews provide the various ways to implement the Electronic Healthcare Records and also give insights on data privacy and security. These insights help enhance the current models to make them much more efficient, faster, and cost-friendly.

2.1.1 Comparison of Existing Methods.

S.No.	Author(s)	Method	Advantages	Disadvantages
1.	Cai Xuifen and Xu Yabin	CPR data integration using hybrid ontology which eliminates heterogeneity in data.	• No heterogeneity when data is integrated. • The integration • is done smoothly.	• The data cannotbe shared when ontology is used. • No data sharing platform.
2.	Hao Jin, Yan Luo, Peilong Li and Jomol Mathew	Secure and privacy-preserving medical data sharing with blockchain-based approaches.	• High Security. • More Privacy.	• High Implementation costs. • Cannot focus on managing multiple databases.
3.	Quingguo Zhang, Bizhen Lian, Ping Cao, Yong Sang, Wanli Huang, and Liang Qi	PDFM (Privacy-free Data Fusion and Mining) used data integration and mining solution for better services.	• Provides a health-services platform. • Time-Efficient • and Privacy-preserving platform.	• Less performance in privacy protection. • It does not focus on fusing different privacy protection solutions.

3. PROPOSED METHOD

3.1 Illustration

Our project is centered around integrating existing CPR (Computer-based Patient Record) systems from various hospitals, aiming to establish a unified platform for effortless data sharing and collaboration. The objective is to create a common ground that simplifies the exchange of patient information across different healthcare institutions.

From a user standpoint, our application offers several features. Users can access their personal information, health data, and hospital-specific reports. This empowers individuals to stay informed about their medical history and make well-informed choices regarding their health. Additionally, the benefits extend to hospitals. Medical institutions can gain comprehensive insights into a patient's medical journey across different hospitals. This holistic view can significantly impact future treatments and overall patient care.

The main focus is on the encryption, compression, and summary of data which helps protect the data from any threats and the summarization of the records can be easily understood by the patient as well as the doctors. These additional features in our application will help the treatments, especially in emergency cases to be done faster and the patient records are not vulnerable to any kind of attacks that allow only the patients and the doctors to access the records.

The primary emphasis lies in the meticulous implementation of encryption, compression, and data summarization protocols, fortifying the security and accessibility of sensitive information within our application. These enhanced features are strategically designed to shield data from potential threats, ensuring that patient records remain impervious to unauthorized access and malicious attacks.

The amalgamation of robust encryption mechanisms guarantees the confidentiality of patient data, while compression techniques optimize storage efficiency without compromising data integrity. Concurrently, the implementation of effective data summarization facilitates seamless comprehension for both patients and medical professionals, thereby expediting treatment procedures, particularly in critical emergency scenarios.

With encryption and compression of data the functionality of two-factor authentication so that unauthorized users cannot login even if the password is breached or compromised. This ensures that there is no bypass to one’s account and no records or documents are accessed by unauthorized people.

By prioritizing these advanced functionalities, our application not only upholds the highest standards of data protection but also streamlines the communication and understanding of medical records. This comprehensive approach not only enhances the efficiency of medical treatments but also ensures that only authorized personnel, namely patients and doctors, have rightful access to the pertinent records, fortifying the overall security architecture of our platform.

4. DESIGN

4.1 Project Architecture

The system interface comprises separate login mechanisms tailored for hospitals and users/patients, ensuring distinct access and functionality. Illustrated through a diagram, the interface delineates a structured navigation pathway across various web pages, each seamlessly integrated with specific application programming interfaces (APIs) to perform defined tasks within the system.

Upon user authentication, facilitated by the "userdata" API, individuals gain entry into their designated dashboard, where they can access pertinent information and functionalities. Subsequent navigation to the personal details page is enabled by the "Udata" API, offering users a platform to manage and update their personal information. The "download" API facilitates the retrieval of reports, empowering users to access and review their medical documentation conveniently. Moreover, the "summary" API provides succinct summaries of reports, aiding users in comprehending and interpreting complex medical information effectively, particularly in urgent situations.

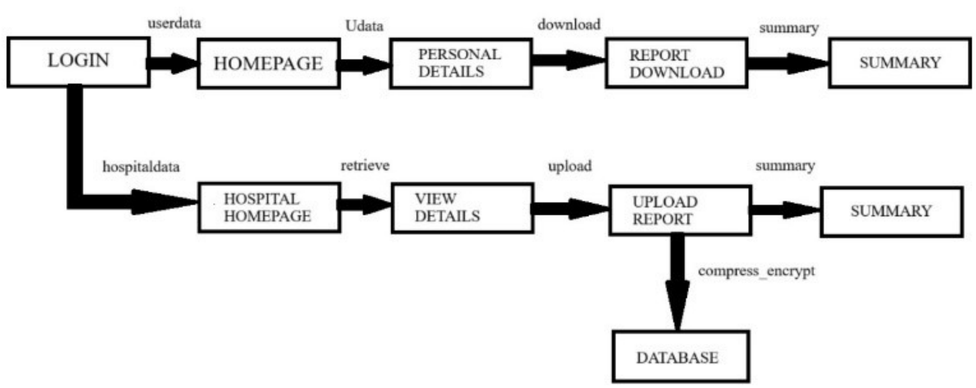


Fig 4.1.1 Working of APIs

Conversely, hospital login procedures leverage the "hospitaldata" API for authentication, granting authorized personnel access to patient details and administrative functions. Upon login, hospitals utilize the "retrieve" API to access patient information, enabling healthcare providers to view relevant medical records and histories as necessary. Subsequent utilization of the "upload" API allows hospitals to securely submit reports and medical data into the system, ensuring seamless integration and accessibility for authorized users. Furthermore, the "compress_encrypt" API facilitates the secure storage of uploaded reports within the database, employing encryption techniques to safeguard sensitive patient information.

In scenarios necessitating rapid assessment and action, such as emergencies, the "summary" API plays a pivotal role by generating concise summaries of reports, enabling healthcare professionals to swiftly grasp critical information and make informed decisions. Overall, the systematic integration of distinct APIs within the interface ensures efficient and secure management of medical data, optimizing the user experience for both patients and healthcare providers.

4.2 UML Diagrams

UML, short for Unified Modeling Language, is a standardized modeling language consisting of an integrated set of diagrams, developed to help system and software developers for specifying, visualizing, constructing, and documenting the artifacts of software systems, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing object-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects. Using the UML helps project teams communicate, explore potential designs, and validate the architectural design of the software.

4.3 Use case Diagram

A Use Case Diagram is a vital tool in system design, it provides a visual representation of how users interact with a system. It serves as a blueprint for understanding the functional requirements of a system from a user’s perspective, aiding in the communication between stakeholders and guiding the development process.

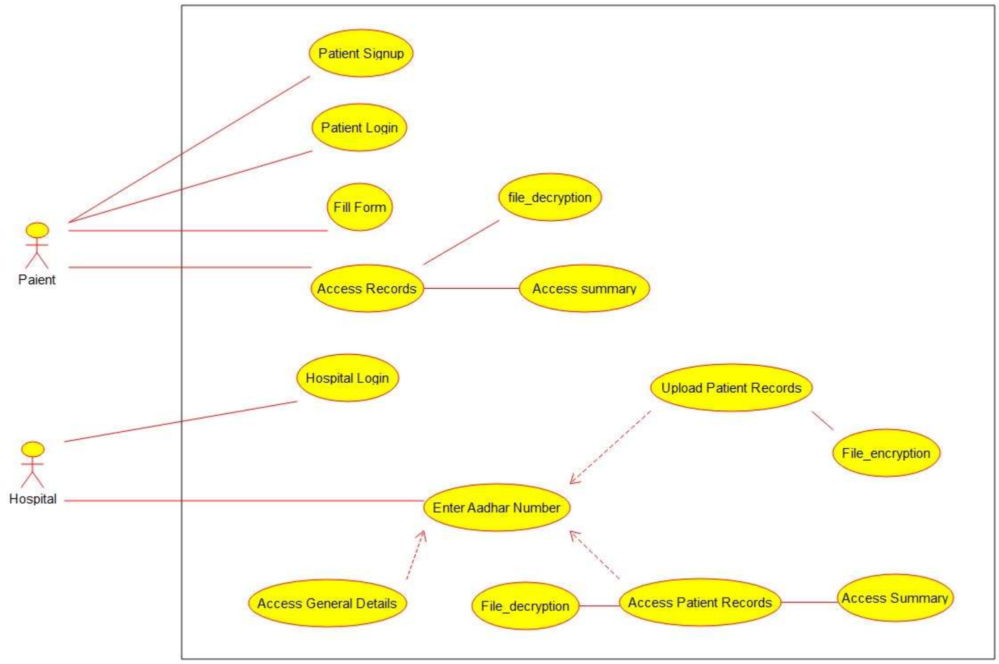


Fig 4.3.1 Use case Diagram

4.4 Class Diagram

Class diagrams are a type of UML (Unified Modeling Language) diagram used in software engineering to visually represent the structure and relationships of classes in a system. UML is a standardized modeling language that helps in designing and documenting software systems. They are an integral part of the software development process, helping in both the design and documentation phases.

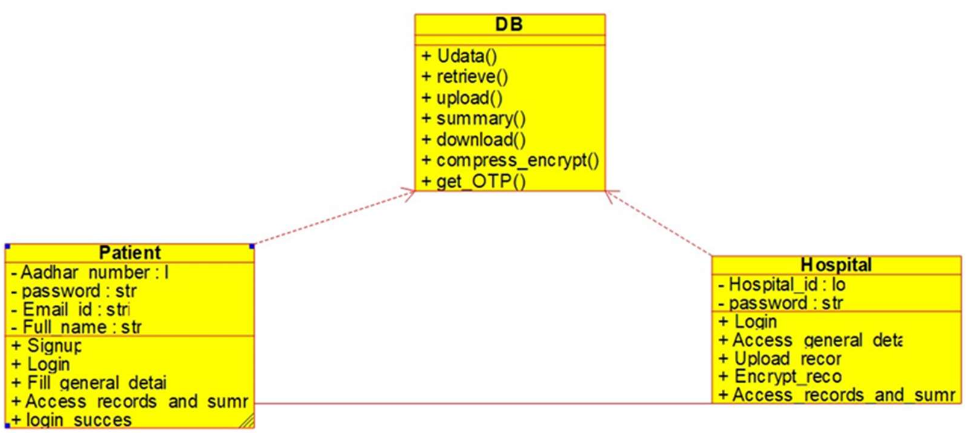


Fig 4.4.1 Class Diagram

4.5 Sequence Diagram

A Sequence diagram shows process interactions arranged in a time sequence. The diagram depicts the processes and objects involved and the sequence of messages exchanged as needed to carry out the functionality. Sequence diagrams are sometimes called event diagrams or event scenarios.

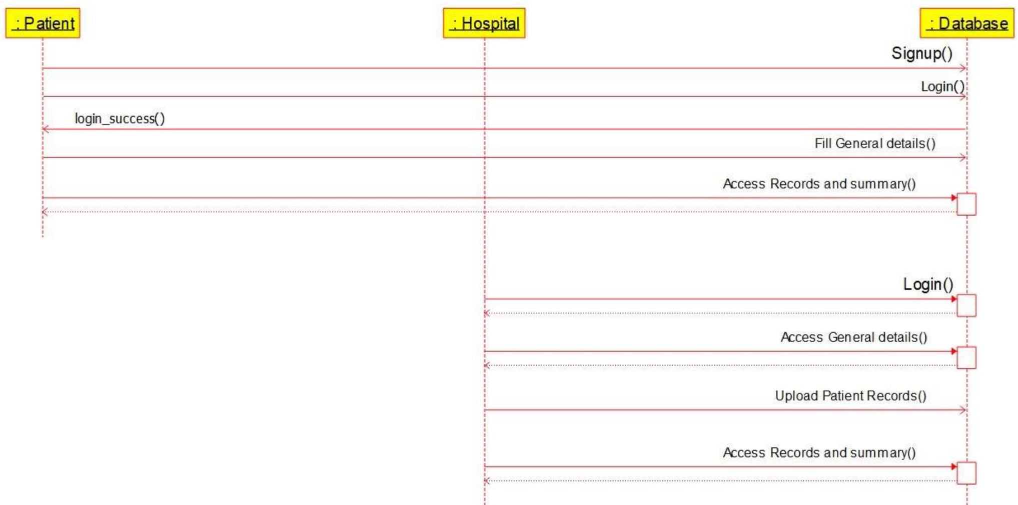


Fig 4.5.1 Sequence Diagram

4.6 Activity Diagram

Activity Diagrams are used to illustrate the flow of control in a system and refer to the steps involved in the execution of a use case. It is a type of behavioral diagram and we can depict both sequential processing and concurrent processing of activities using an activity diagram i.e., an activity diagram focuses on the condition of flow and the sequence in which it happens.

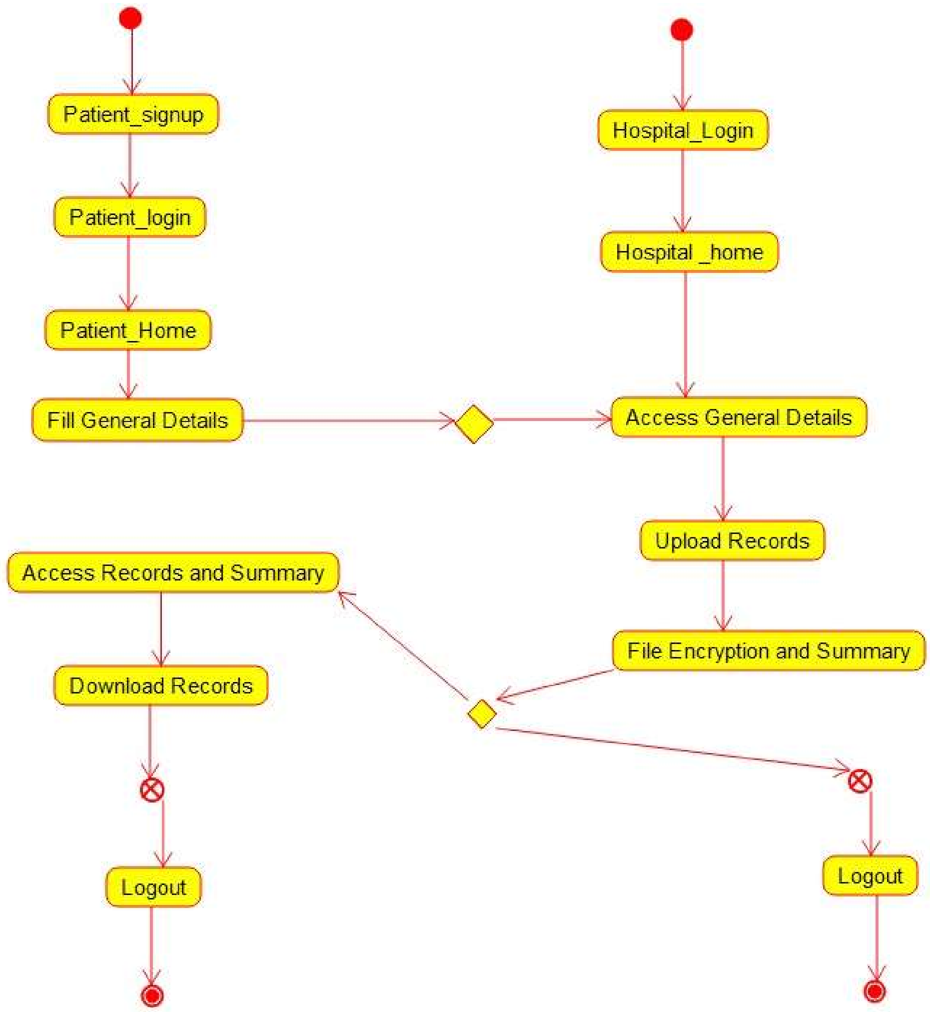


Fig 4.6.1 Activity Diagram

4.7 Deployment Diagram

A Deployment Diagram in software engineering is a type of structural UML diagram that shows the physical deployment of software components on hardware nodes. It illustrates the mapping of software components onto the physical resources of a system, such as servers, processors, storage devices, and network infrastructure.

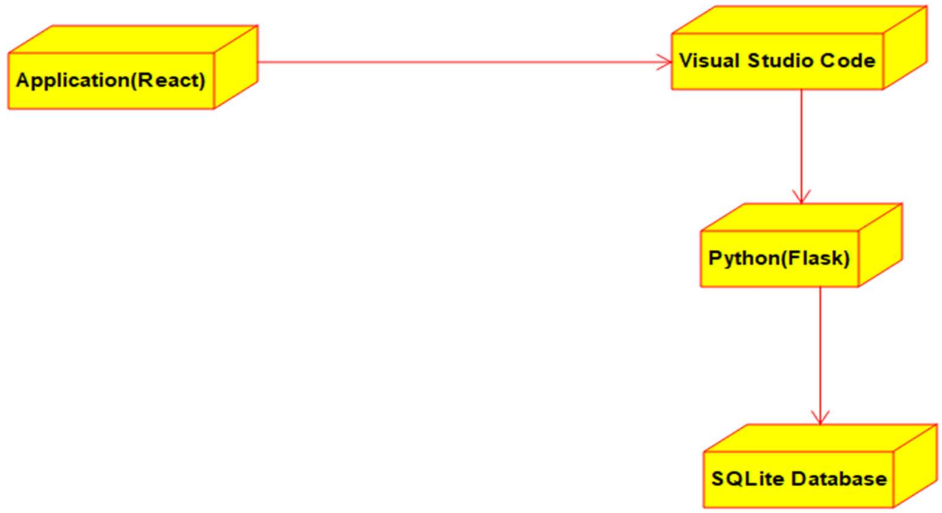


Fig 4.7.1 Deployment Diagram

5. IMPLEMENTATION

5.1 Tools Used

1. React App

A React app is a web application created using the React JavaScript library. Reactis component-based, declarative, and optimizes performance with a virtual DOM. React components are typically written in JavaScript and JSX. It's often used for single-page applications (SPAs) and is part of a large ecosystem with extensive community support. React is a popular choice for building modern, interactive web applications.

2. Flask

Flask is a lightweight web framework for Python, known for its simplicity and flexibility. It allows developers to build web applications quickly with minimal boilerplate code. Flask is extensible, supporting various extensions and libraries. It's often considered a "microframework" because of its minimalistic approach. Flask is popular for both web applications and RESTful API development.

3. SQLite Database

SQLite is a lightweight, serverless, and self-contained relational database management system (RDBMS). It is often embedded within applications and operates as a local database without the need for a separate server or external configuration. SQLite stores data in a single, portable file, making it easy to manage and transport. It is widely used in mobile apps, desktop applications, and embedded systems for its simplicity, speed, and small footprint. While it may not offer some advanced features of larger RDBMS like MySQL or PostgreSQL, SQLite is an excellent choice for projects that require a compact, local database.

5.2 Components

5.2.1. Security

Data privacy and security plays a pivotal role in Electronic Healthcare Record systems since cyber-attacks have been increasing every day. Manipulation, theft, or any threat to medical records o hospital data can prove dangerous. AES and 3DES are the two encryption algorithms used in our model which have proven to be secure and efficient. Decryption is just as essential as encryption so that the receiver has all the right data. With decryption, comes Key management, where the secret key needs to be hidden so that the data is secure throughout both encryption and decryption.

Key Management: Ensuring the protection of encryption keys, as they are vital for decrypting sensitive data. Employing secure methods for storing keys and exploring the use of Hardware Security Modules (HSMs) to prevent unauthorized access to keys.

AES: The Advanced Encryption Standard (AES) is like the guardian angel of our digital world, ensuring the safety of our sensitive information. Picture it as a master lock that operates on blocks of data, each chunk being 128 bits in size. What's impressive about AES is its adaptability, offering different key sizes of 128, 192, and 256 bits, depending on the level of security needed.

AES follows a nifty structure called the Substitution-Permutation Network (SPN). It's like a puzzle-solving algorithm that expands the original key into a unique set of round keys. Each round involves a series of transformations—think of them as secret moves—like swapping bytes, shifting rows, mixing columns, and adding special round keys swapping bytes, shifting rows, mixing columns, and adding special round keys.

But here's where AES truly shines: its commitment to security. It's designed to be like a maze where every twist and turn makes it impossible for anyone without the key to navigate through. Even the tiniest change in the starting point—the plaintext—leads to a completely different path—the ciphertext. This complexity makes AES a formidable fortress against cyber threats.

AES remains the go-to choose for encryption, ensuring our online conversations stay private and our personal data stays safe. So, just like we upgrade our home security systems, it's crucial to stay informed about the latest in encryption technology to keep our digital lives secure. But here's where AES truly shines: its commitment to security. It's designed to be like a maze where every twist and turn makes it impossible for anyone without the key to navigate through. Even the tiniest change in the starting point—the plaintext—leads to a completely different path—the ciphertext. This complexity makes AES a formidable fortress against cyber threats.

5.2.2. Summarization

The summary of the patient records when either the hospital or the patient accesses the records is displayed which is an upgrade in our model. This summary was intended especially for emergencies when the procedures are needed to be performed immediately. These summaries display the essential details from the records (e.g. allergies, medications, medical history, surgeries, and more) so that the consulting doctors will not have to check the whole records before operating in emergencies. These even save money as the test results are also displayed in the summary and there is no need to repeat the tests. This feature saves time, money and can be very helpful in emergencies.

A. Working:

We used the innovative methodology for text summarization by integrating the cutting-edge Pegasus model into our application. Our methodology is meticulously crafted to give both the patients and the doctors a concise summary of the records whenever they want to access them.

Workflow:

- *Hospital Input Acquisition:* The summarization starts only when the hospital or the consulting doctor uploads the patient records through the application.

- *Preprocessing for Summarization:* The acquired reports undergo preprocessing steps tailored to facilitate effective summarization by the Pegasus model. This preprocessing step serves as a directive to the Pegasus model, indicating the intention to generate a summary of the input content.

- *Tokenization for Model Input:* Subsequently, the preprocessed patient report is subjected to tokenization using the Pegasus tokenizer. This process involves breaking down the textual input into discrete tokens, which are numerical representations of the constituent words and subwords within the text. This tokenized format enables seamless integration with the Pegasus model for summarization.

- *Leveraging Pegasus for summarization:* The tokenized input text is then fed into the Pegasus model for summarization. Leveraging the advanced transformer architecture of Pegasus, the model engages in an abstractive summarization process, wherein it synthesizes the salient information and key insights from the input text to generate a coherent and concise summary.

- *Decoding and Presentation:* Following the summarization process, the generated summary undergoes decoding from its numerical token representations to human-readable text. This decoding operation translates the token IDs into their corresponding linguistic elements, effectively transforming the summary into a comprehensible format. The summarized content is then presented to users via the web application interface for their review and utilization.

- *User Interaction and Utilization:* The presented summary lets both doctors and patients grasp the essence of the reports. This can be utilized very well in cases of emergencies and the patients can be treated quicker.

Pegasus: The Pegasus model, referenced in the context above, is a state-of-the-art neural network architecture developed by Google Research for text summarization tasks. Unlike extractive summarization methods that select and assemble existing text segments, Pegasus employs an abstractive approach, meaning it generates summaries by paraphrasing and synthesizing information from the input text.

One of the notable features of Pegasus is its capability to produce coherent and concise summaries that capture the key points and main ideas of the input text. It achieves this by understanding the context and semantic relationships within the text, allowing it to generate human-like summaries.

Pegasus is based on the transformer architecture, which has demonstrated remarkable performance in various natural language processing tasks. It is pre-trained using a large corpus of text data and fine-tuned for specific summarization objectives.

Overall, Pegasus understands the context and semantic relationship between texts, which allows it to produce human-like summaries, making it the best open-source model to use for this application. It makes the summaries concise but captures the key points very well making it easy and faster for the doctors to understand the records and act accordingly.

5.3 Sample Code

5.3.1 Patient record encryption and upload

```
class Upload(Resource):
  def put(self,aadhar):
      user = User.query.filter_by(aadhar = aadhar).first()
      data = userdata.query.filter_by(ulid=user.id).first()
    try:
      file = request.files["file"]
      pdf_reader = PyPDF2.PdfReader(file)
      page = pdf_reader.pages[0]
      text = page.extract_text()
      model_name = "google/pegasus-xsum"
      tokenizer = PegasusTokenizer.from_pretrained(model_name)
      device = "cuda" if torch.cuda.is_available() else "cpu"
```

```
model=PegasusForConditionalGeneration.from_pretrained(model_name).to(de
vice)


 input_text = "summarize: " + text


tokenized_text=tokenizer.encode(input_text,return_tensors='pt',max_length=10
24, truncation=True).to(device)

summary_= model.generate(tokenized_text, min_length=50, max_length=400,
num_beams=4, length_penalty=2.0, early_stopping=True)

summary_text = tokenizer.decode(summary_[0], skip_special_tokens=True)

summary_text1 = summary_text.encode('utf-8')


 key = b'9898765434675432'

 padded_data = pad(summary_text1, AES.block_size)

 cipher = AES.new(key, AES.MODE_ECB)

 encrypted_summary = cipher.encrypt(padded_data)

 data.summary = encrypted_summary

 db.session.commit()


 if file:

    print(type(text.encode('utf-8')))

    print(text.encode('utf-8'))

    compressed_data = gzip.compress(text.encode('utf-8'))

    encodeed_text = text.encode('utf-8')

    print(type(encodeed_text))


    key = b'1234567812345678'

    padded_data = pad(encodeed_text,AES.block_size)

    cipher = AES.new(key, AES.MODE_ECB)

    encrypted_data = cipher.encrypt(padded_data)
```

```
            test = userdata.query.filter_by(ulid = user.id).first()
            print(encrypted_data)
            print(type(encrypted_data))
            test.file=encrypted_data
            db.session.commit()
            return jsonify({"message": "File uploaded successfully"})
        else:
            return jsonify({"error": "No file provided"})
    except Exception as e:
        print("Error:", str(e))
        return jsonify({"error": str(e)})
```

5.3.2 Patient General Details

```
class Udata(Resource):
    def put(self):
        args = upar.parse_args()
        name = args.get("name",None)
        contact = args.get("contact",None)
        age = args.get("age",None)
        height = args.get("height",None)
        weight = args.get("weight",None)
        gender = args.get("gender",None)
        bloodgrp = args.get("bloodgrp",None)
        user = User.query.filter_by(status = "lin").first()
```

```
if(name == "" or contact == "" or age == "" or weight == "" or height == "" or
gender == "" or bloodgrp == ""):
    return 400
else:
    newdata=userdata(name=name,contact=contact,age=age,height=height,
    gender = gender, weight = weight,bloodgrp=bloodgrp,ulid = user.id)
    db.session.add(newdata)
    db.session.commit()
    return {'message':'SUCCESS'}
```

6.EXPERIMENT RESULTS

6.1. Experiment Screen Shots

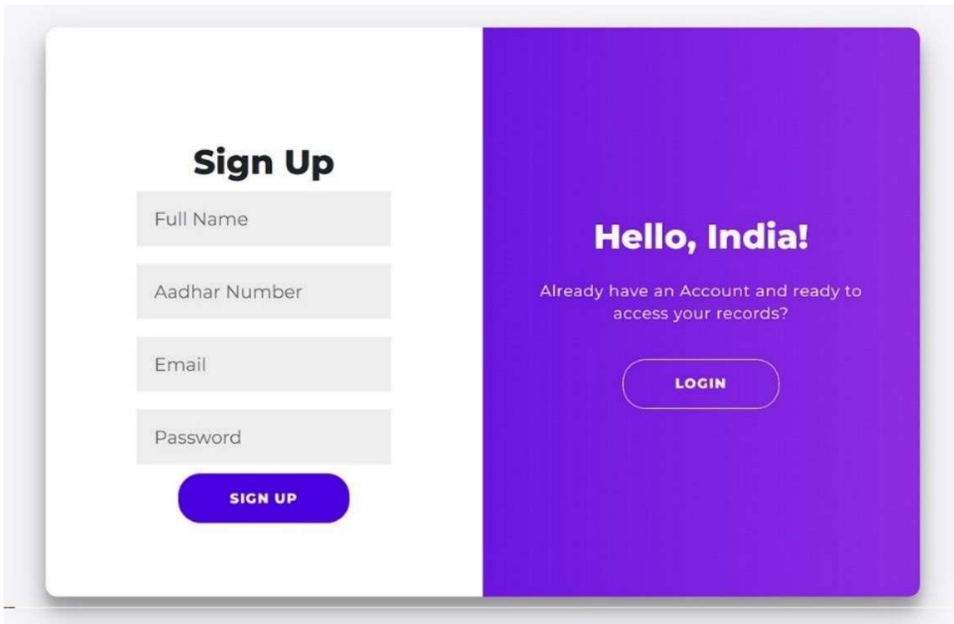


Fig 6.1.1 Patient Signup

This Figure 6.1.1 shows us the Patient Signup page where the patient can register himself or herself as a user using their Full name, Aadhar number, Email and a password.

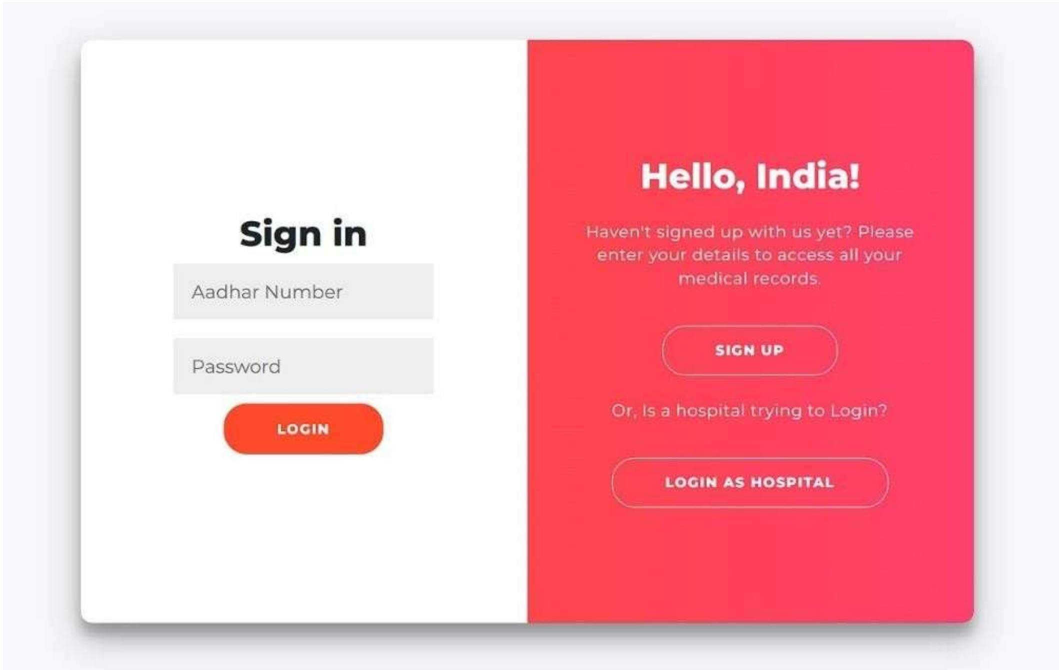


Fig 6.1.2 Patient Login

This Figure 6.1.2 is the login page for the patient where the patient enters the aadhar number and password and then gets an OTP to login.

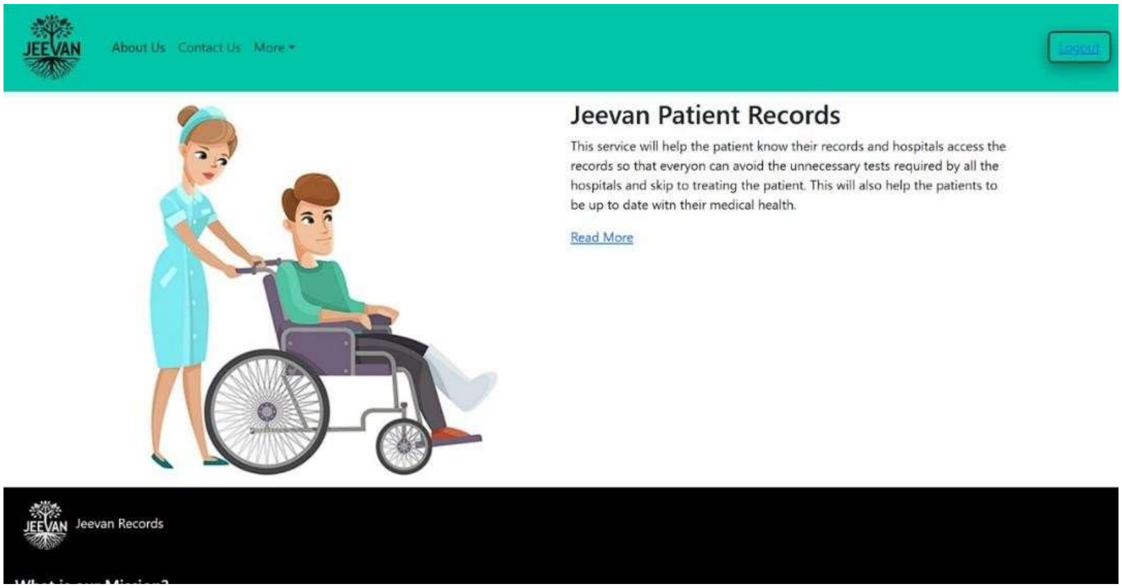


Fig 6.1.3 Patient Home

The Figure 6.1.3 shows the home page of the patient to access the other services of the portal.

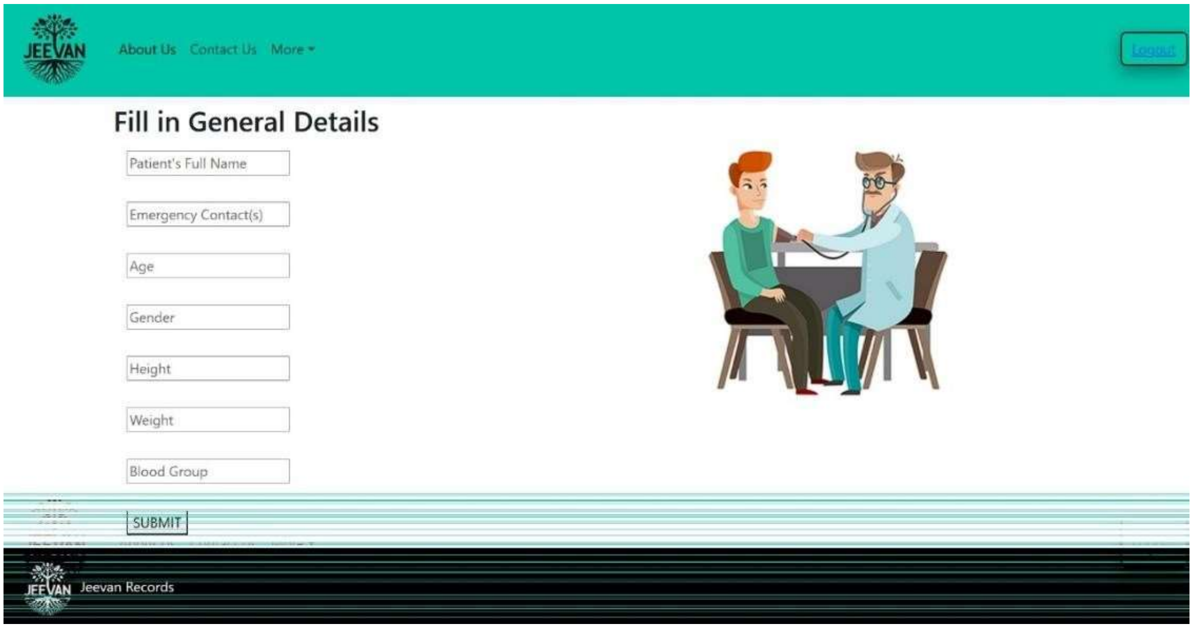


Fig 6.1.4 Patient Form Fill

This figure 6.1.4 shows the general details of the patient that are required in any scenario of the hospital services.

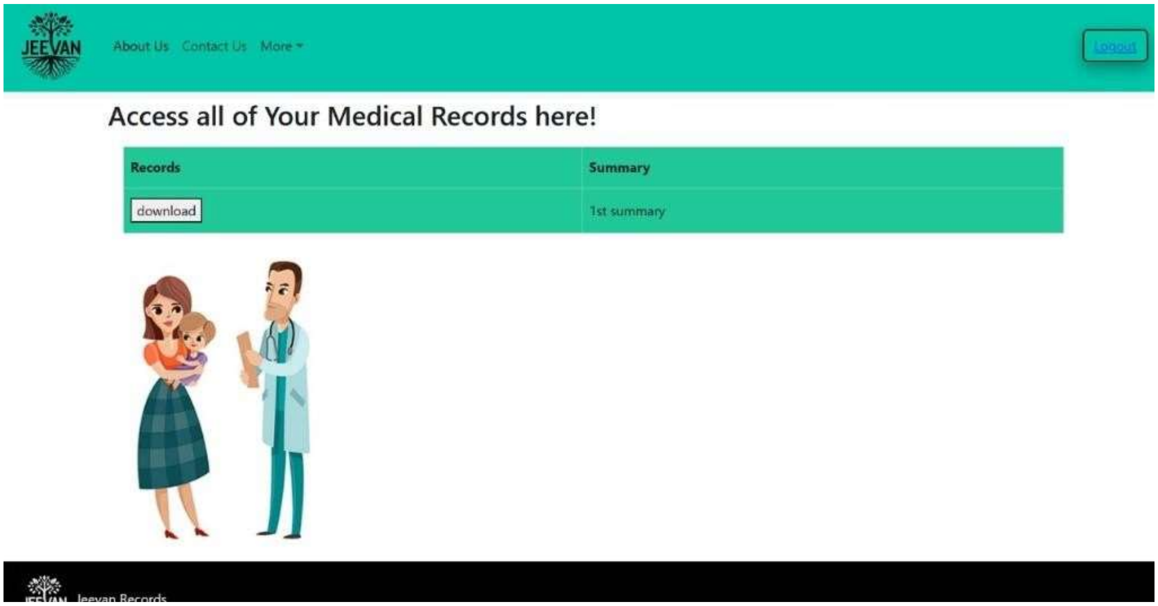


Fig 6.1.5 Access Records for patient

The above figure shows the access of the records by the patient. The medical record can be accessed and the summary is generated for the record**.** The patient can download the record.

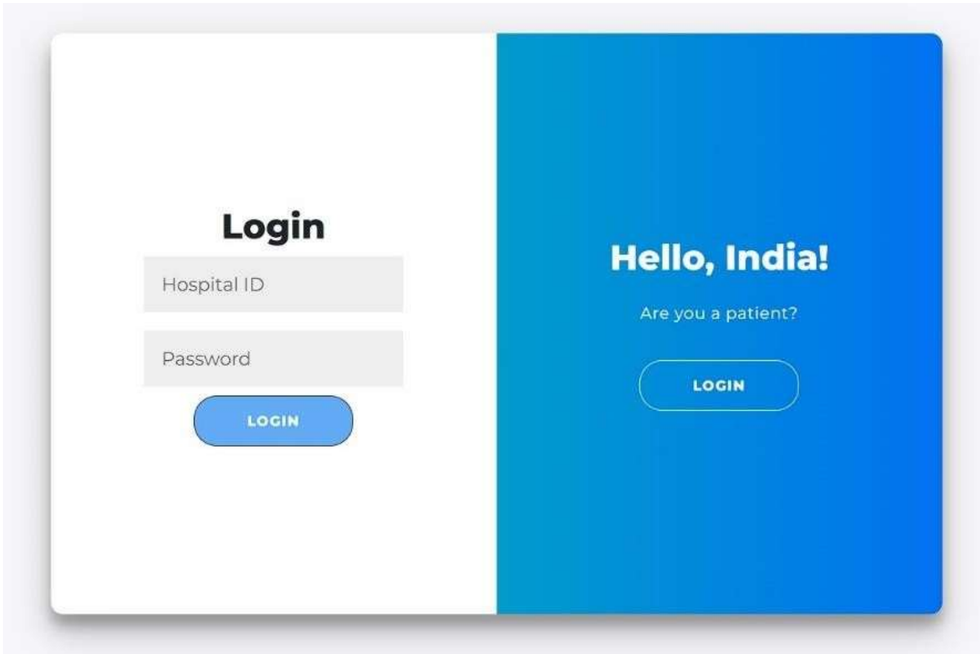


Fig 6.1.6 Hospital Login

The above figure shows the login page of hospital where the hospital id is generated by the admin.

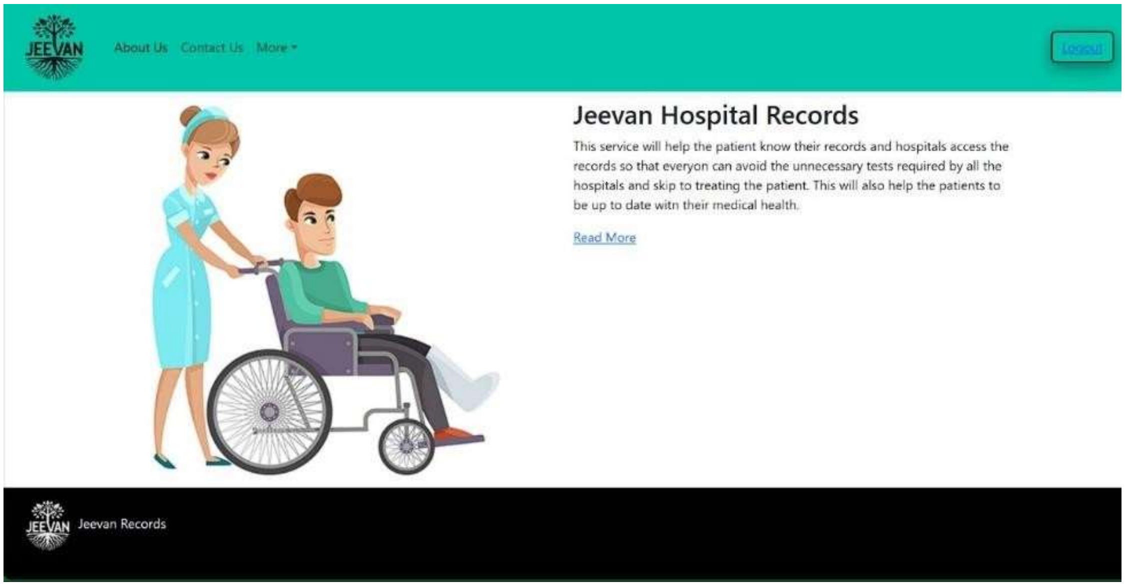


Fig 6.1.7 Hospital Home

The above figure shows the home page of hospital.

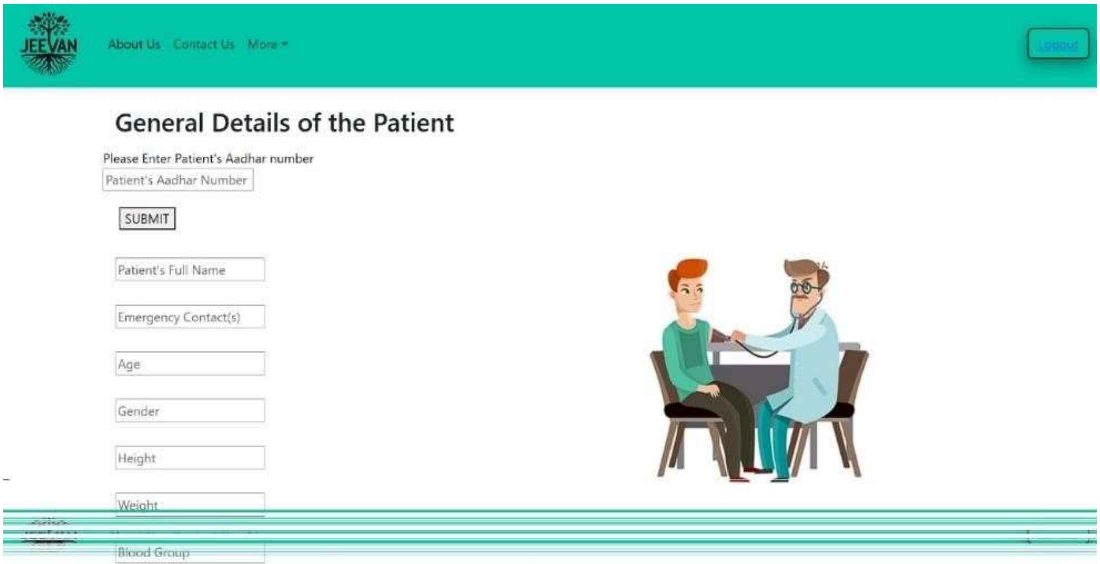


Fig 6.1.8 Access General Details of patient

The above figure shows the access of general details of the patient by entering their Aadhaar number.

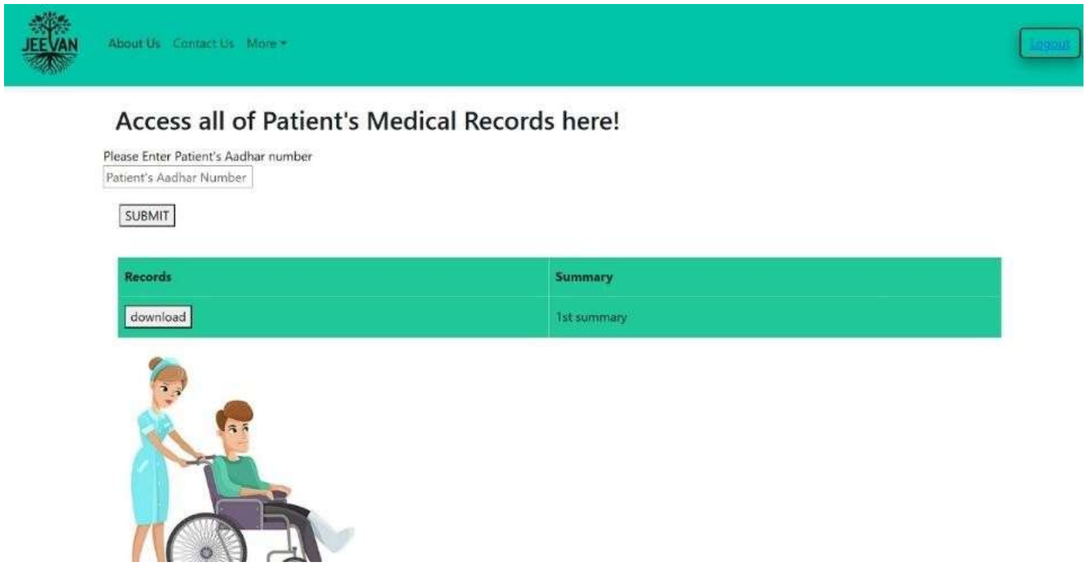


Fig 6.1.9 Access Patient Previous Records

The access of patient previous records by the hospital by entering the patient's Aadhaar number. The hospital can download the record and read the summary of the patient which helps a lot during emergency situations.

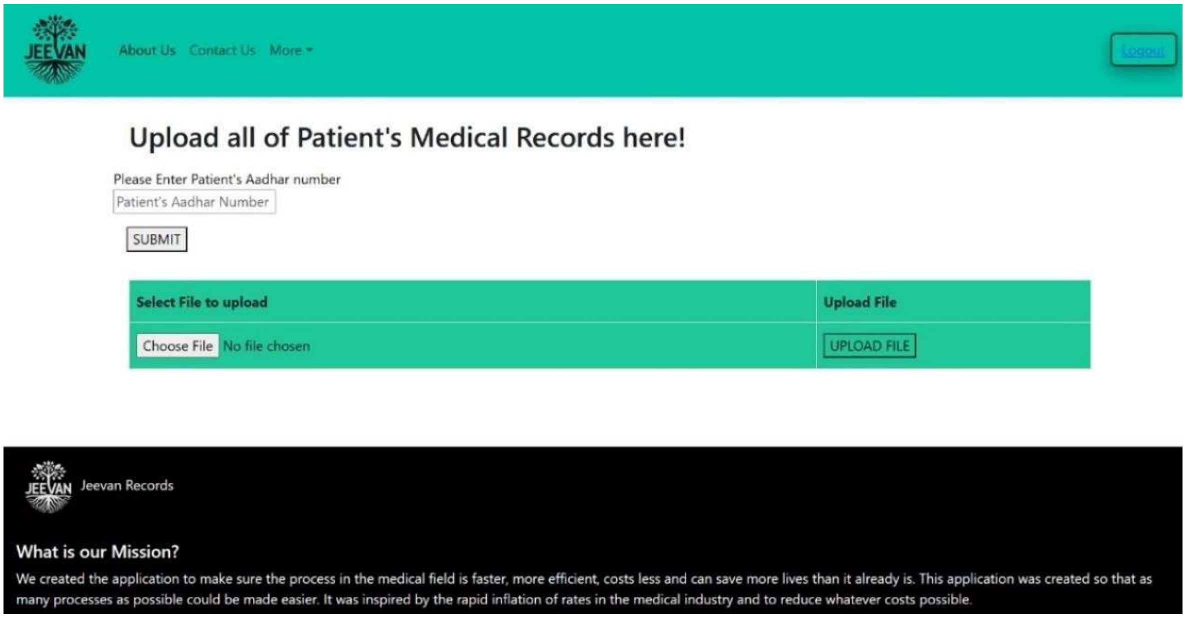


Fig 6.1.10 Upload Patient Records

The above figure shows the hospital page where the hospital uploads the records of the patient by entering the patients' Aadhaar number.

7. Discussion Of Results

7.1 Analysis

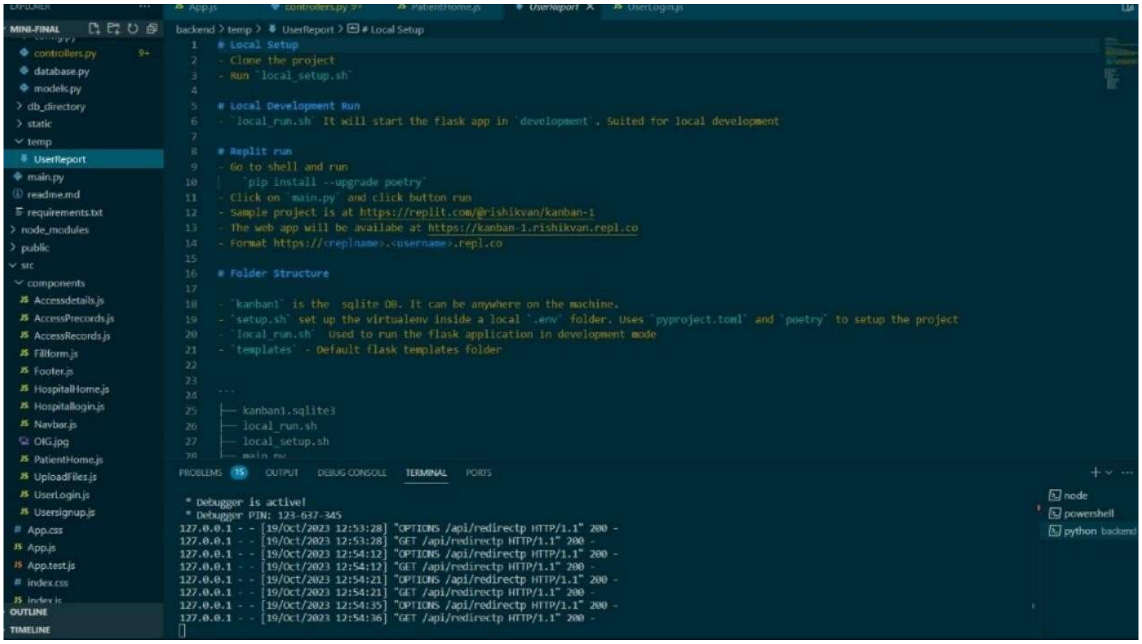


Fig 7.1.1 User Report

This is the user report that will be downloaded when the user logs into the portal and downloads the respective medical records that are uploaded by the hospital. The user report, accessible upon logging in and downloading medical records, offers a concise yet thorough glimpse into one's health journey. It begins with a brief summary, outlining crucial health details. Then, it delves into specific sections covering diagnostics, treatments, medications, and more. Each section provides clear insights, ensuring easy understanding for users of all backgrounds. From diagnostic findings to treatment histories and medication details, every aspect is organized meticulously. Specialist consultations, immunization records, and lifestyle recommendations further enrich the report, fostering informed decision-making. With clarity and accessibility at its core, the report empowers individuals to actively engage in their healthcare journey, promoting better health outcomes and greater satisfaction.

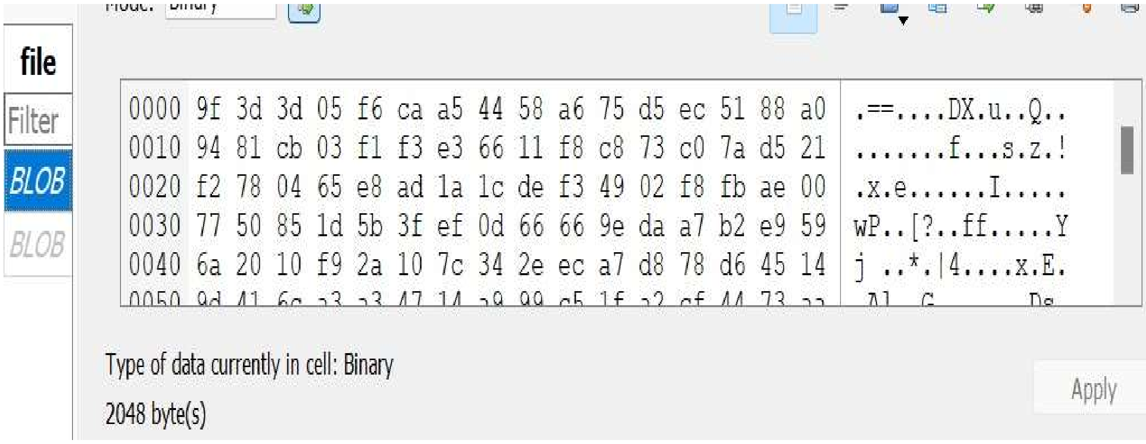
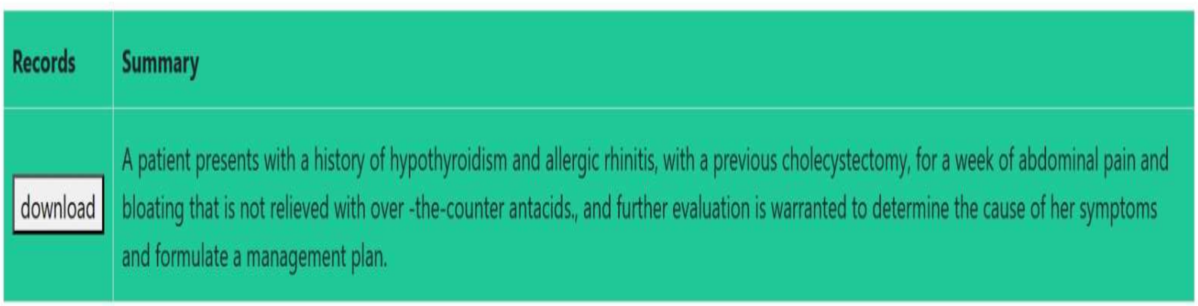


Fig 7.1.2 Encryption

This is the data that will be stored in the database. It contains the personal details of the patient that are uploaded by the patients and the reports that are uploaded by the hospitals. The data is stored by encrypting it using AES algorithm. This algorithm provides security to the data from intruders, attackers and even the administrator who cannot read the data.



Records	Summary
download	A patient presents with a history of hypothyroidism and allergic rhinitis, with a previous cholecystectomy, for a week of abdominal pain and bloating that is not relieved with over -the-counter antacids., and further evaluation is warranted to determine the cause of her symptoms and formulate a management plan.

Fig 7.1.3 Summary of the data

The patient records are summarized using Pegasus model making it easier for emergency situations. This summary helps in detecting the patient history, medications, and allergies.

8. CONCLUSION

In wrapping up the strategies we've implemented to ensure patient medical records remain confidential and intact, we've achieved some significant milestones. We've beefed up security by deploying strong encryption methods like AES and 3DES both for safeguarding data in storage and during transmission. This not only bolsters overall security but also puts us in line with important healthcare data protection regulations such as HIPAA and GDPR. We're also staying proactive by regularly assessing risks and classifying data meticulously. Strict access controls and a robust key management system are in place to keep data secure.

We've also paid close attention to addressing potential security incidents and human-related risks through effective incident response, real-time monitoring, and comprehensive user training. To stay ahead of the curve, we conduct regular security audits and keep stakeholders informed about any evolving cybersecurity challenges.

By successfully implementing these measures, we've instilled trust in the secure management of medical records. The summarization of patient records, powered by the Pegasus model, plays a vital role here. It ensures that the summaries are not just robotic but human-like, making them easily understandable for both doctors and patients. This not only saves time but also cuts costs, as doctors won't need to repeat tests already conducted in the past—the results are conveniently summarized.

In essence, our focus on encryption and data compression keeps patient information secure, while efficient summarization aids doctors in working faster, more affordably, and with greater efficiency.

9. FUTURE SCOPE

Our application has been meticulously designed to streamline the storage and retrieval of healthcare records, prioritizing efficiency and ease of access. Through robust encryption protocols, we ensure the utmost safety and security of stored data. However, we recognize the potential for future enhancements.

Presently confined to India, our application holds promise for global expansion, enabling patients worldwide to access their medical history from their time in India, while providing hospitals with comprehensive international patient records. Such global accessibility stands to significantly expedite and optimize treatment processes for both patients and medical facilities.

Moreover, as cyber threats continue to proliferate, fortifying the security of medical records is paramount. While our current encryption algorithms provide formidable protection, ongoing adaptation and refinement are imperative to safeguard against unauthorized access, tampering, or any form of cyber intrusion.

This vision for the future of our project not only underscores our commitment to advancing healthcare technology but also underscores our dedication to ensuring the utmost privacy and security for patients and healthcare providers alike.

10. REFERENCES

[1] V. Ved, V. Tyagi, A. Agarwal and A. S. Pandya, "Personal Health Record System and Integration Techniques with Various Electronic Medical Record Systems," 2011 IEEE 13th International Symposium on High-Assurance Systems Engineering, Boca Raton, FL, USA, 2011, pp. 91-94, doi: 10.1109/HASE.2011.63. keywords: {Medical services;Servers;DICOM;Insurance;Information systems;Computer architecture;Personal Health Record System;EHR (Electronic health records);EMR (Electronic medical records);CDO (care delivery organizations)}

[2] Cai Xiufen and Xu Yabin, "Computer-based patient record data integration method based on ontology," 2011 IEEE International Symposium on IT in Medicine and Education, Guangzhou, China, 2011, pp. 551-554, doi: 10.1109/ITiME.2011.6132170. keywords: {Ontology;CPR;Data Integration}

[3] S.T.Argaw, N-E Bempong, B.E.Chauvin, A.Flahault, The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review, BMC medical informatics and decision making, 19:10, 2019, 1-11, DOI:10.1186/s12911-018-0724-5

[4] D. Ulybyshev et al., "Protecting Electronic Health Records in Transit and at Rest," 2020 IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS), Rochester, MN, USA, 2020, pp. 449-452, doi: 10.1109/CBMS49503.2020.00091. keywords: {Cryptography;Access control;Servers;Containers;Electronic medical records;Metadata;Watermarking;Electronic Health Records, data privacy, data leakage prevention, HIPAA, access control}

[5] H. Wang and R. Zhou, "The Application of Blockchain to Electronic Health Record Systems:A Review," 2021 International Conference on Information Technology and Biomedical Engineering (ICITBE), Nanchang, China, 2021, pp. 397-401, doi: 10.1109/ICITBE54178.2021.00092. keywords: {Electric potential;Precision medicine;Medical services;Blockchains;Safety;Electronic medical records;Information technology;Blockchain;Internet of Things;Electronic health record}

[6] A. Shibu, A. M, A. T. Anilkumar, A. Radhakrishnan and S. Izudheen, "Secure Storage and Retrieval of Electronic Health Records," 2022 International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS), Kochi, India, 2022, pp. 1-5, doi: 10.1109/IC3SIS54991.2022.9885484. keywords: {Data privacy;Privacy;Hospitals;Medical services;Encryption;Blockchains;Electronic medical records;Encryption;Electronic Health Records;AES;Blowfish;EHR;Secure storage}

[7] V. Shukla, A. Mishra and A. Yadav, "An Authenticated and Secure Electronic Health Record System," 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 2019, pp. 1-5, doi: 10.1109/CICT48419.2019.9066168. keywords: {Electronic medical records;Password;Radio transmitters;Encryption;Authentication;Authentication;Electronic Health Record (EHR);Encryption;Security}

[8] Q. Zhang, B. Lian, P. Cao, Y. Sang, W. Huang and L. Qi, "Multi-Source Medical Data Integration and Mining for Healthcare Services," in IEEE Access, vol. 8, pp. 165010-165017, 2020, doi: 10.1109/ACCESS.2020.3023332. keywords: {Data privacy;Data integration;Medical diagnostic imaging;Medical services;Distributed databases;Encryption;Service recommendation;Internet of Health;locality-sensitive hashing;user privacy;data integration}

[9] H. Jin, Y. Luo, P. Li and J. Mathew, "A Review of Secure and Privacy-Preserving Medical Data Sharing," in IEEE Access, vol. 7, pp. 61656-61669, 2019, doi: 10.1109/ACCESS.2019.2916503. keywords: {Medical services;Cloud computing;Blockchain;Biomedical imaging;Data privacy;Cryptography;Access control;blockchain;encryption;medical data;privacy;security}