DEPARTMENT OF INFORMATION TECHNOLOGY

## Providing Data Privacy of E-Healthcare Data

## A PROJECT REPORT

## Submitted by

## RAJIB KUMAR MAJUMDAR

## JYOTIRMAY SIKDAR

## SAPTARSHI MONDAL

## SUBHAJIT GHOSH

## Supervised by

## Ms. Sayantani Saha

***in partial fulfillment of the award of the degree***

***of***

**BACHELOR OF TECHNOLOGY**

***IN***

INFORMATION TECHNOLOGY



MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY,

WEST BENGAL

(FORMERLY KHOWS AS WEST BENGAL UNIVERSITY OF TECHNOLOGY)

NH-12, Haringhata, Nadia, Pin- 741249

**BONAFIDE CERTIFICATE**

Certified this project report “…………**Providing Data Privacy of E-Healthcare data**……….” is

the bonafide work of “…….**RAJIB KUAMR MAJUMDAR ……JYOTIRMAY SIKDAR…….SAPTARSHI MONDAL……..SUBHAJIT GHOSH……..”** Who carried out the project work under my supervision.

**SIGNATURE SIGNATURE**

**Dr. Somdatta Charkaborty Ms. Sayantani Saha**

**HEAD OF THE DEPARTMENT SUPERVISOR**

**Dept. of Information Technology Assistant Professor,**

**Dept.of Engineering**

**Technologies**

**MAKAUT, WB MAKAUT, WB**

**SIGNATURE**

**External Examiner:**

**SIGNATURE**

**External Examiner:**

**Table of Content**

|  |  |  |
| --- | --- | --- |
| Chapter No. | Title | Page No. |
| 1 | ABSTRACT | 4 |
| 2 | INTRODUCTION | 5 |
| 3 | Importance of Privacy in Health data | 5-6 |
| 4 | Advantages of E-health | 6 |
| 5 | Motivation | 6-7 |
| 6 | Literature Review | 7 |
| 7 | Main Goal | 7 |
| 8 | Aim and purpose | 8 |
| 9 | Methods and Resources | 9 |
| 10 | Implementation Details | 9-15 |
| 11 | Algorithm | 16 |
| 12 | Conclusion | 17 |
| 13 | Reference | 18 |

**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 securing stored 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, our project proposed model includes a patient data security mechanism that gives a high level of patient data confidentiality and authentication. Also, we develop a clean and clear user interface and developed efficient data collection using NoSQL keeping in mind that every hospital can also use these data and also can share it with other hospitals as well. Medical workers must want data for analyzing, improving, and giving service to our health system. Moreover, the privacy of the patients should be respected on humanitarian grounds.

.

**INTRODUCTION**

Everyone is talking about e-health these days, but few have provided a clear definition of this relatively new term. This term, which was barely in use before 1999, now appears to serve as a general "buzzword," used to characterize not only "Internet medicine," but also virtually everything related to computers and medicine. Rather than academics, it appears that industry leaders and marketing professionals were the first to use the term. They coined and used this term, along with other "e-words" such as e-commerce, e-business, e-solutions, and so on, in an attempt to convey the promises, principles, and excitement (and hype) surrounding e-commerce (electronic commerce) to the health arena, and to account for the new possibilities that the Internet is opening up in the field of health care. According to Intel, e-health is "a concerted effort undertaken by leaders in the health care and high-tech industries to fully harness the benefits available through the convergence of the Internet and health care." Because the Internet created new opportunities and challenges for the traditional healthcare information technology industry, it seemed appropriate to coin a new term to address these issues. These "new" challenges for the healthcare information technology industry were primarily (1) the ability of consumers to interact with their systems online (B2C = "business to consumer"); (2) improved data transmission possibilities between institutions (B2B = "business to business"); and (3) new consumer-to-consumer communication (C2C = "consumer to consumer"). Provide the benefits of streamlined operations, enhanced administration & control, superior patient care, strict cost control, and improved profitability. Hospital Management Systems are in high demand to handle increasing population needs and also aid the practicing doctors and hospital service and support staff with timely service and precision.

**Importance of Privacy in Health data**

Patient treatment-related data would be shared among different healthcare personnel. Moreover, healthcare data is considered to be sensitive data. Therefore, we need to consider the following points while handling healthcare data -

i) Patients strongly believe that their information should be shared only with people involved in their care.

ii) Patients do identify with the need for information sharing among physicians, though HIV patients are less likely to approve sharing of their health information.

iii) Many patients who agree to information sharing among physicians reject the notion of releasing information to third parties, including employers and family members.

And also, they don’t want to share unnecessary data with other health workers like paramedical staff, pharmacists, nurses, etc.

iv) The vast majority of patients who have undergone genetic testing believe that it is their responsibility to inform other at-risk family members of their test results.

v) Only about 28-35% of patients are agnostic about their health information, which includes age, gender, ethnicity, the reason for treatment, medical history, personal habits affecting health, type of treatment obtained, and side effects of treatment used for other purposes by physicians.

vi) However, only about 5-21% of patients expected their doctors to ask for permission to use their information.1

vii) Only about 10% of patients expected their doctors to ask for permission if they used their health information for a variety of purposes, such as combining data with other patients' data to provide better information to future patients, sharing treatment outcomes with other physicians, teaching medical professionals, and writing research articles about diseases and treatments.

1:Sensitivity of E-Health Data. (Shuchitted Mallick)

**Advantages of E-health**

Using E-Health concepts has numerous advantages. Electronic health records are a prime example. Before the use of E-health, we used a paper-based system to record patient health data. These paper-based systems may contain errors when entering patient records. When it comes to E-health, data is stored electronically, which is a more simple and more efficient way of storing data (Hayride, 2008)[9]. According to Grogan, there is evidence to suggest that E-health provides more comprehensive and error-free methods for storing patient data. (2006) (Grogan) [10]. There are numerous advantages to using E-health for various people such as doctors, patients, and so on. Doctor's orders, for example, can be placed electronically, avoiding incorrect elucidation of handwritten orders. Furthermore, with the help of E-health, most doctors reduce the time it takes to locate and read patient health information. The patient can gradually become aware of the importance of self-care management. Furthermore, it is convenient for maintaining only a few medical experts and application developers.

## Motivation

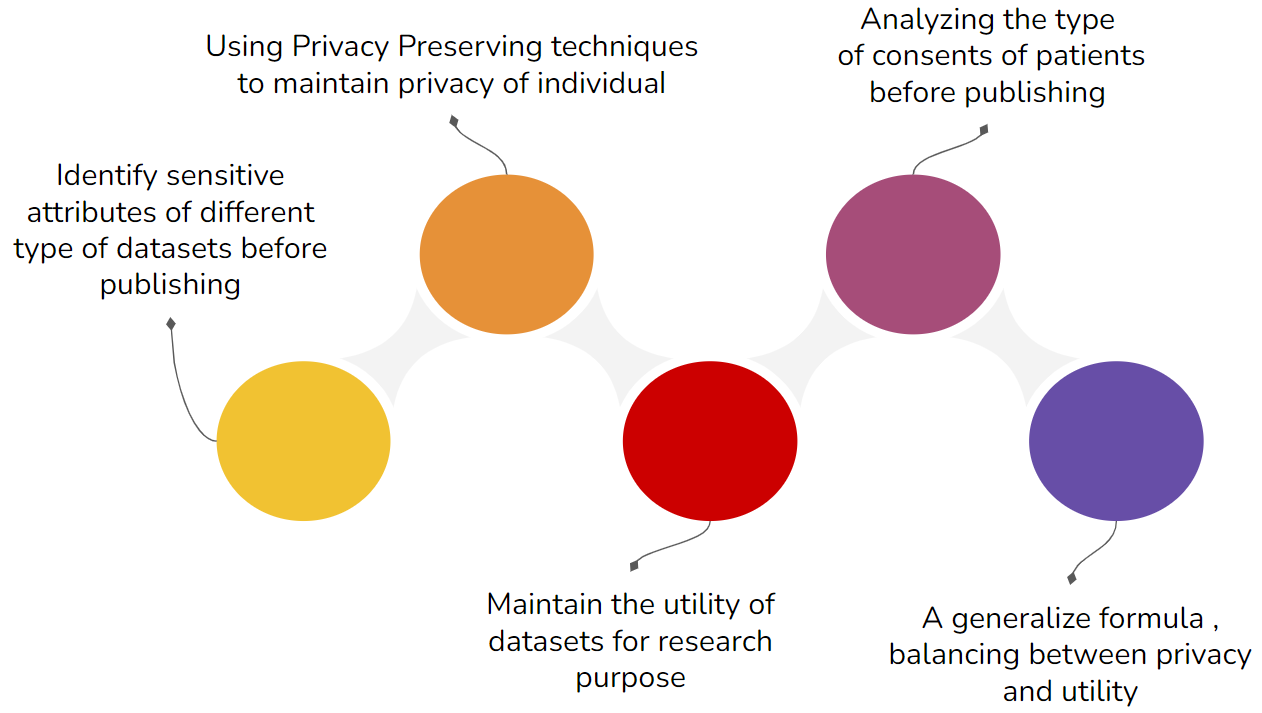
Health data is so sensitive data. Only legitimate users should get access to it. No other medical personnel should access the data without permission. So, data need to be protected with a proper cryptosystem. Now the traditional cryptosystem is not able to provide end-to-end security to the system. Encrypting each patient’s data with an encryption key and sharing the key with the user -- is a very common method to maintain security. However, this traditional approach is not very efficient. First, it is going to store a huge number of encryption, and decryption keys, and key sharing should be done in the proper way to secure the system. In case the user like a doctor or nurse or any other user is changed we need to re-encrypt the patient data with a new key. So the traditional approach is not found to be suitable. Moreover, the data revealed to the doctor, may not be required by the pharmacist or pathologist so we need to separate the patient data into smaller chunk and share it with the concerned user. For example, the pathologist need not access the data of medicine advice by the doctor or the pharmacist may not need the data of the pathological report. So here is the need to keep the data in an efficient data model system.

**Literature Review**

An Electronic Health Record (EHR) is a virtual platform that provides medical reports access to the EHRs and has the flexibility to supply information about patient care. Not only that the EHR demonstrated here to store and supply information for patients, but it also has an understanding of how data of the patient must be sent to users or staff of the HealthCare Center. This tool will also allow the patient to access their health data and give them better control over their health. The security part is an extensive part of this project, the security will be applied to the data which will be or are being sent to the different users or staff of the healthcare center. Currently, we are researching through the security of what type of security will be most appropriate and how to apply the security, and this is also the main challenge we are facing right now. The authors in paper [1] discussed the security challenges in the healthcare system.

**Main Goal**

Now, keeping the right balance between utility and privacy is our key priority. We must desire data to evaluate and enhance our healthcare system. On the other hand, we must treat patients with humanity and respect their right to privacy. Figure 1 shows the different factors that need to be considered while providing data privacy in the healthcare system.

Fig 1: Different aspects of Data privacy required in the Healthcare System 

**Aim and purpose**

The main goal of the project is to create a basic E-health-field system framework combined with responsive web design technology based on a cloud server. It provides a basic common model that can be used in the development of future E-health applications. It provides a valuable guideline on E-health web applications for people to manage their care. And the model is intended to be used to create a specific application aimed at diabetes self-care management.

The project’s main work is as follows:

1. **Systematic literature review and Internet search:**

We will conduct a systematic review of the literature on responsive web design, record the results, and analyze what others have done in the field so that we can begin work based on the available results**.**

1. **To establish an E-health web application frame:**

This project is primarily concerned with developing a responsive e-health system framework to provide a basic common model that can be used in the future by some specific e-health applications. On the one hand, we must choose an appropriate development platform and cloud platform. The frame, on the other hand, should concentrate on security issues such as access control and data storage.

1. **To design a reasonable web design method:**

The E-health framework will be created by combining various technologies (Bootstrap, HTML5, JavaScript, CSS). CSS, among these technologies, is in charge of the device's web visual style. So, by learning the existing related CSS method, we can improve and design a reasonable style transformation method. And we make every effort to ensure that the style can be automatically transformed and applied to a variety of devices. Then, because the system will be expanded in the future, we will create a guideline for it.

1. **Database Design:**

We brainstorm on how to store data for efficient data retrieval so we find in the long term we get so much NoSQL data. So, to avoid NULL values in SQL we used Mongo DB for storing data in collection format.

1. **Data privacy:**

We are learning various encryption cryptographical methods and finding the most appropriate one for storing and retrieving the data keeping in mind security and privacy.

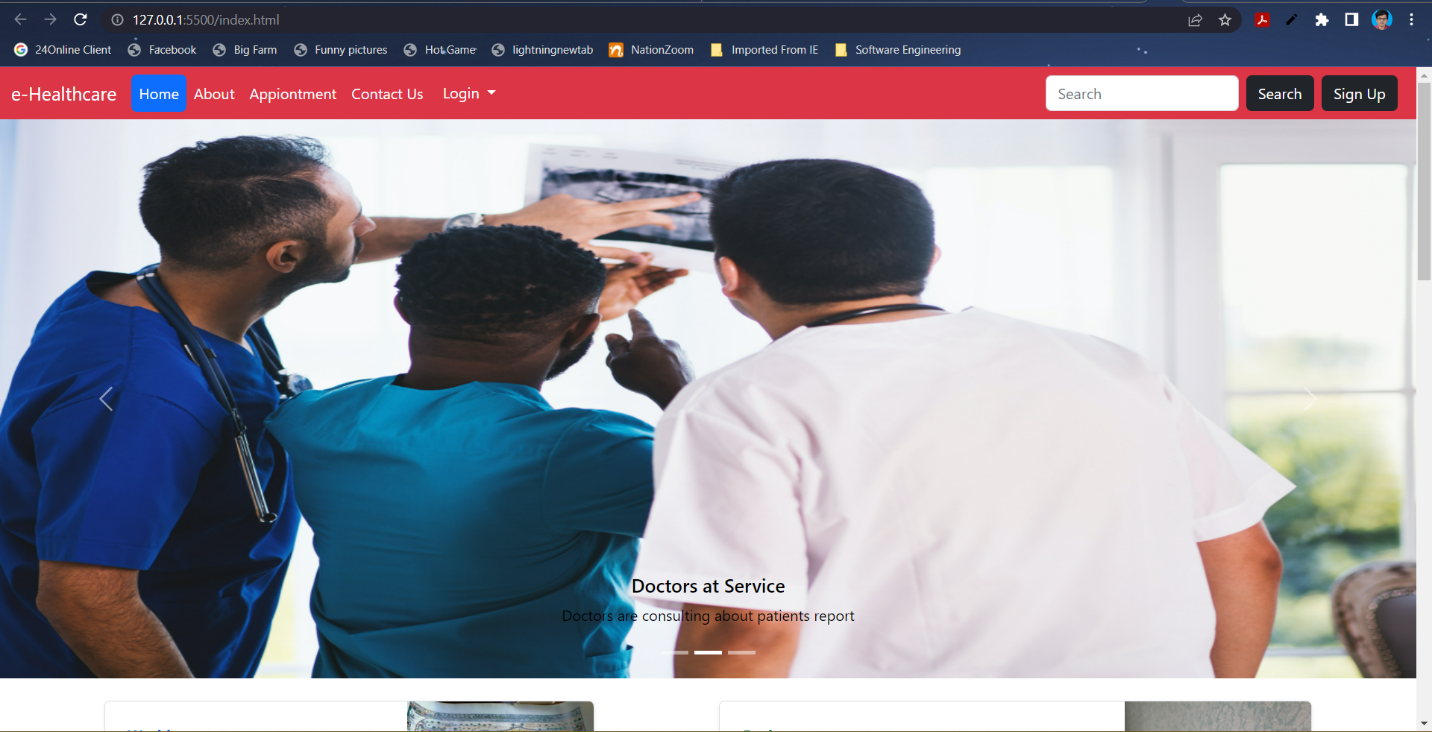
**Methods and Resources**

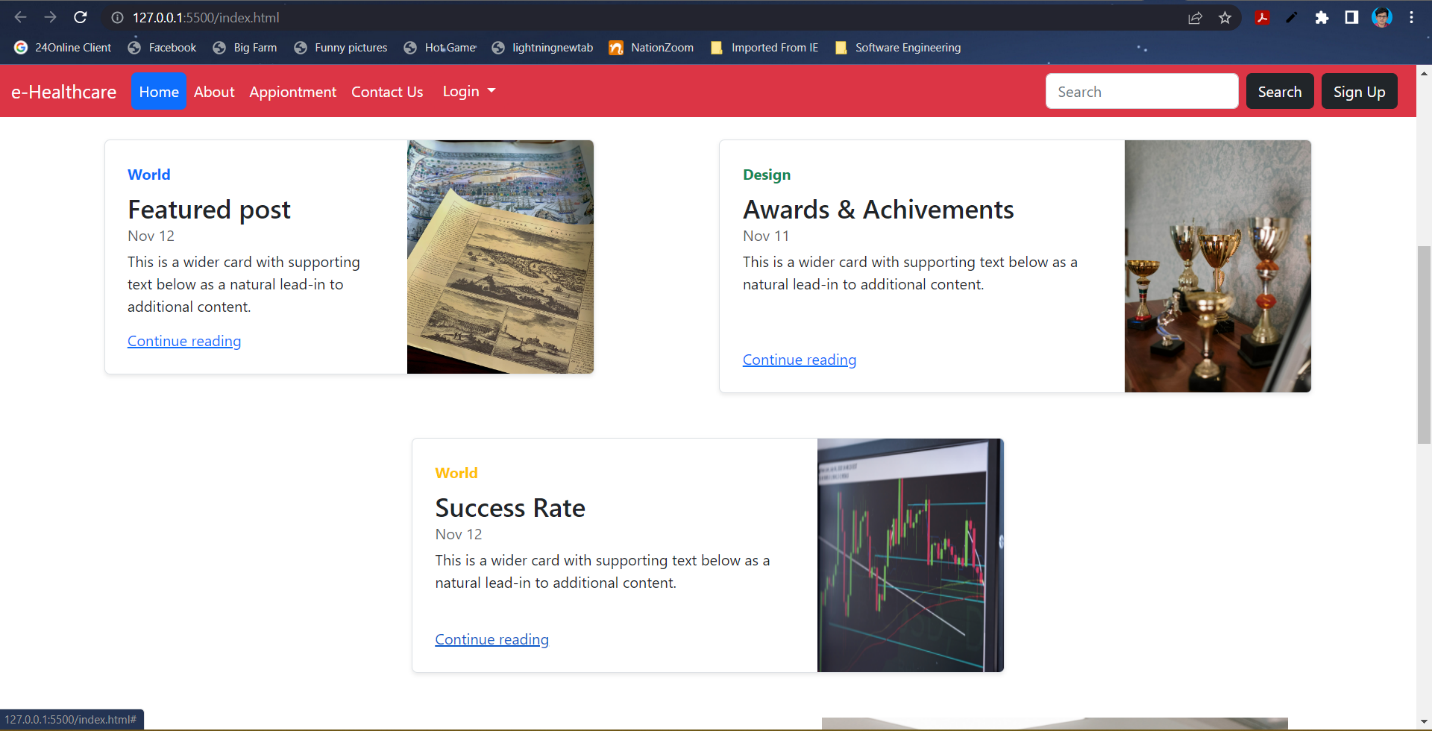
To generate meaningful results for our purpose, we conduct systematic research. To search for and evaluate the results, two major steps were taken: (1) It contains a broad search using the most relevant keywords for more potential hits when gathering sources. Furthermore, a good literature review necessitates the isolation of key themes or issues related to your research interests, so additional restrictions were added to filter the articles. (2)Evaluating sources and reading all final articles with the following questions in mind: Is the evidence consistent with the conclusion? Is the evidence or argument complete? Is there agreement among researchers, or are there differences? Finally, unusable articles with these merits are removed, and all remaining articles are classified. First and foremost, the Springer database was chosen as the data source for this literature review study because it is widely used in computer science research studies and is maintained by Springer-Verlag, one of the most well-known science and technology publishing companies. However, the articles in the Springer database that are related to Computer Science are mostly unrelated to E-health, so Google Scholar was also used to conduct this research. All keywords were classified into four groups: "Topic," "Technology," "Programming Language," and "Device."

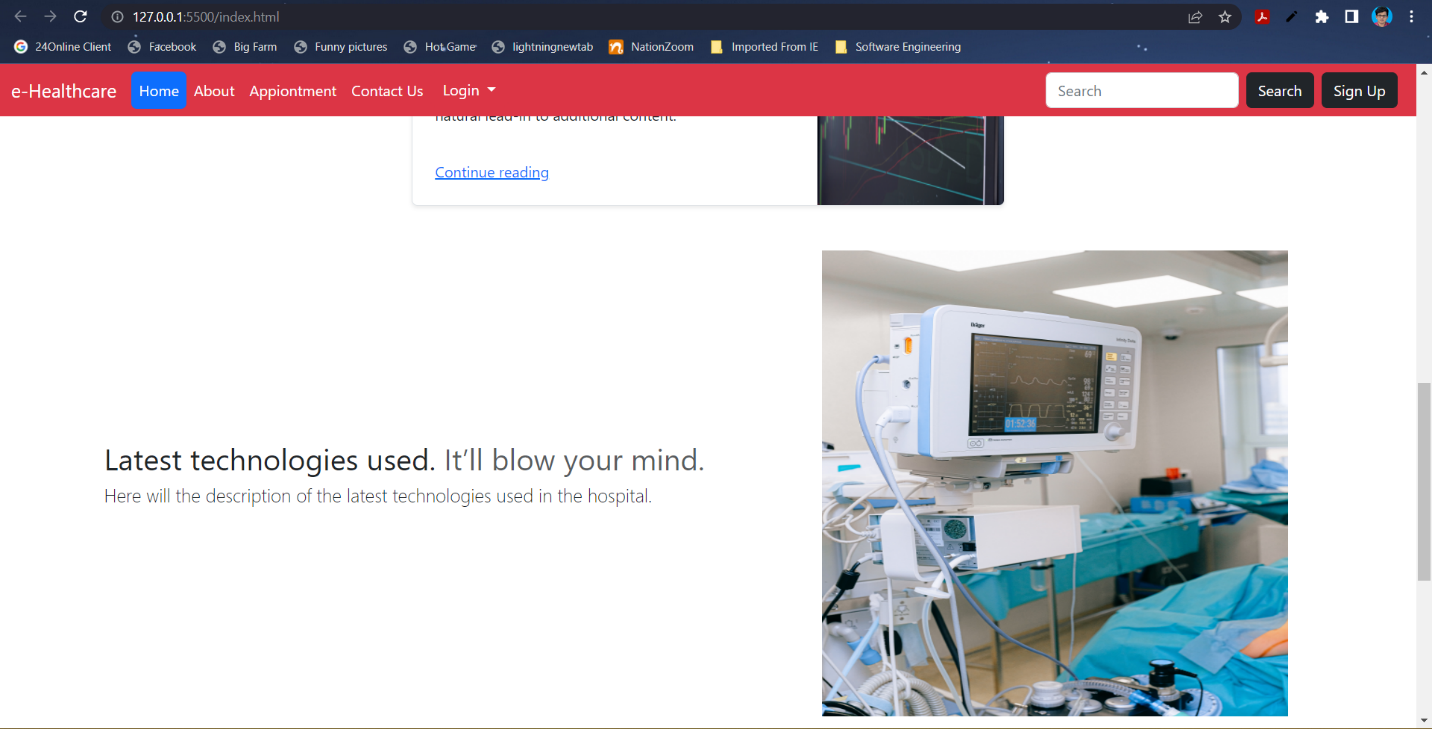
**Implementation Details**

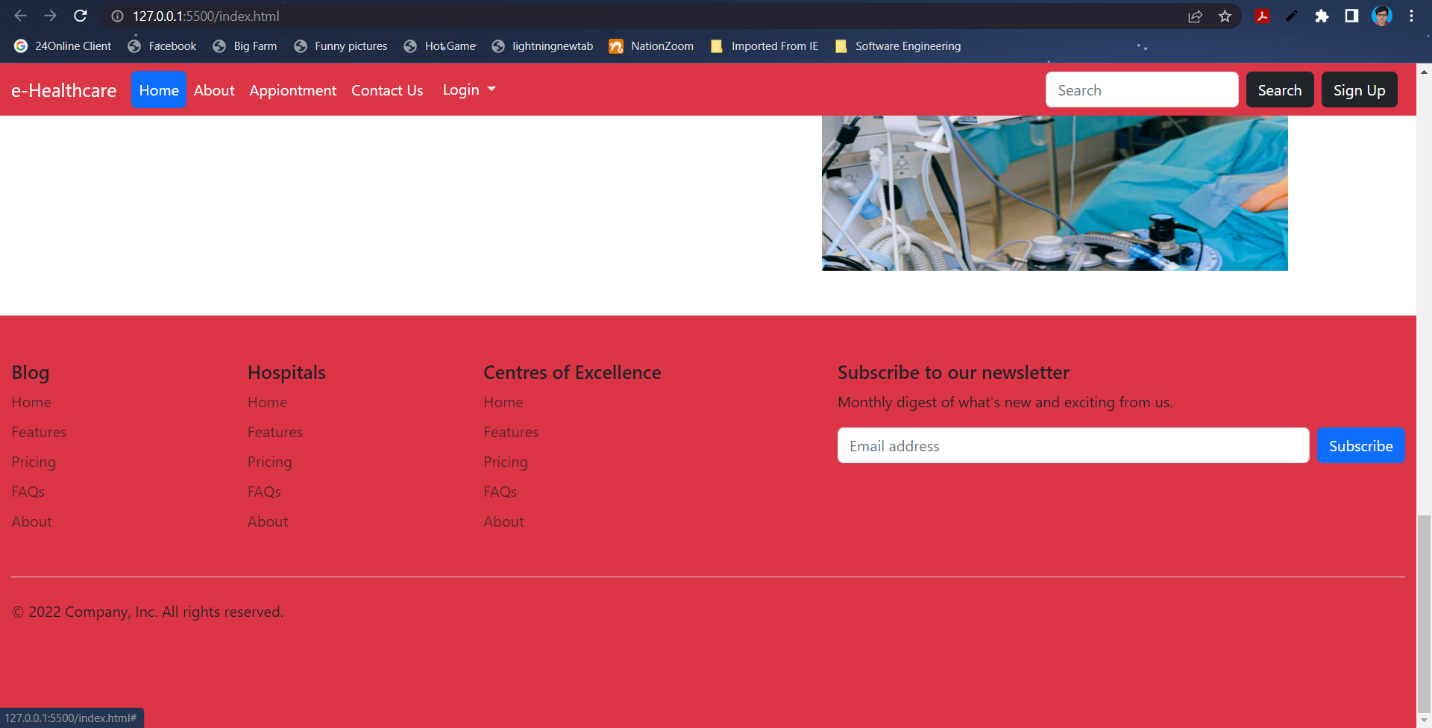
**Front End:-**

Home page of the framework

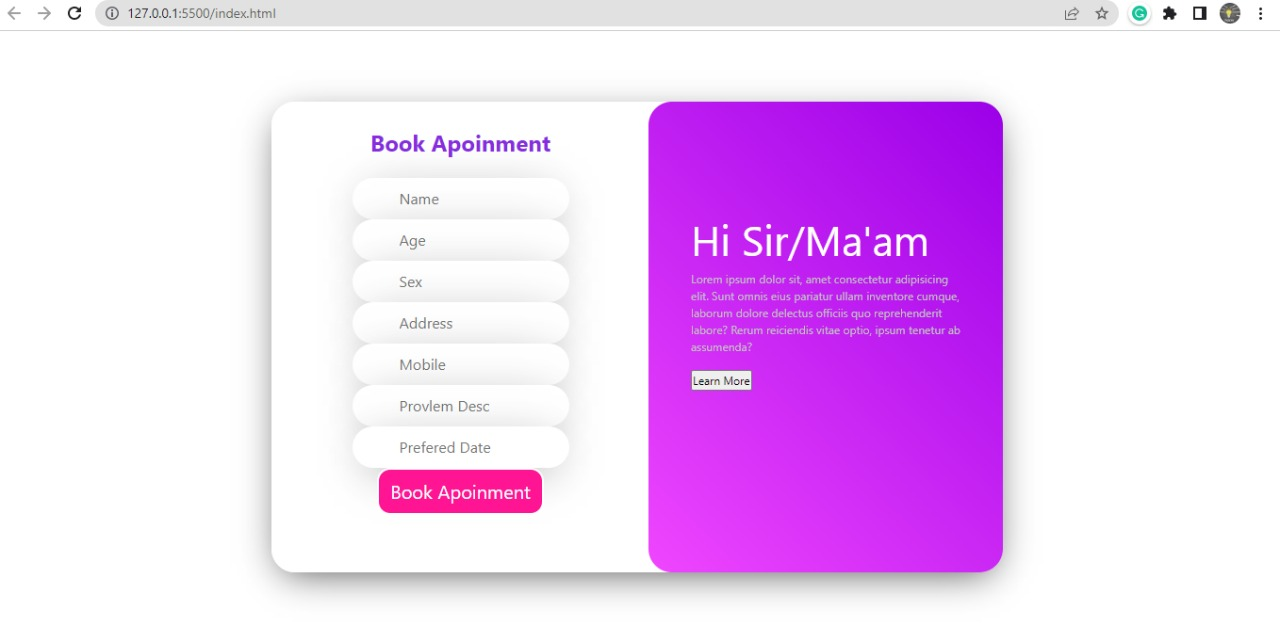




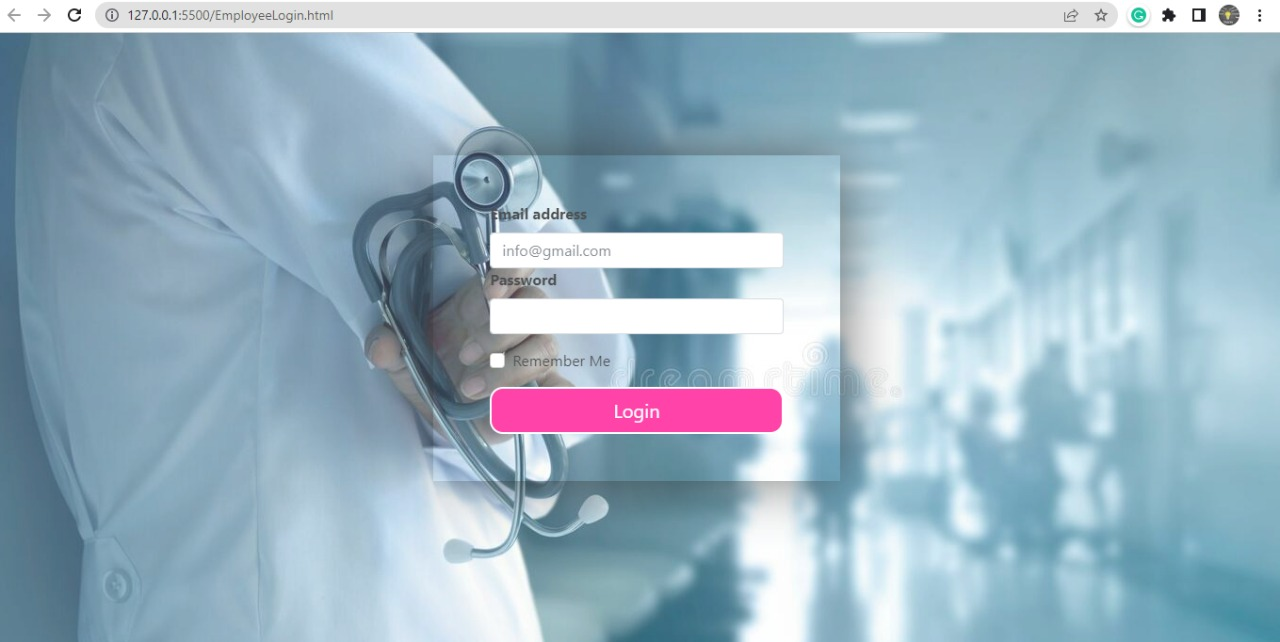




Appointment page where patients will make an appointment

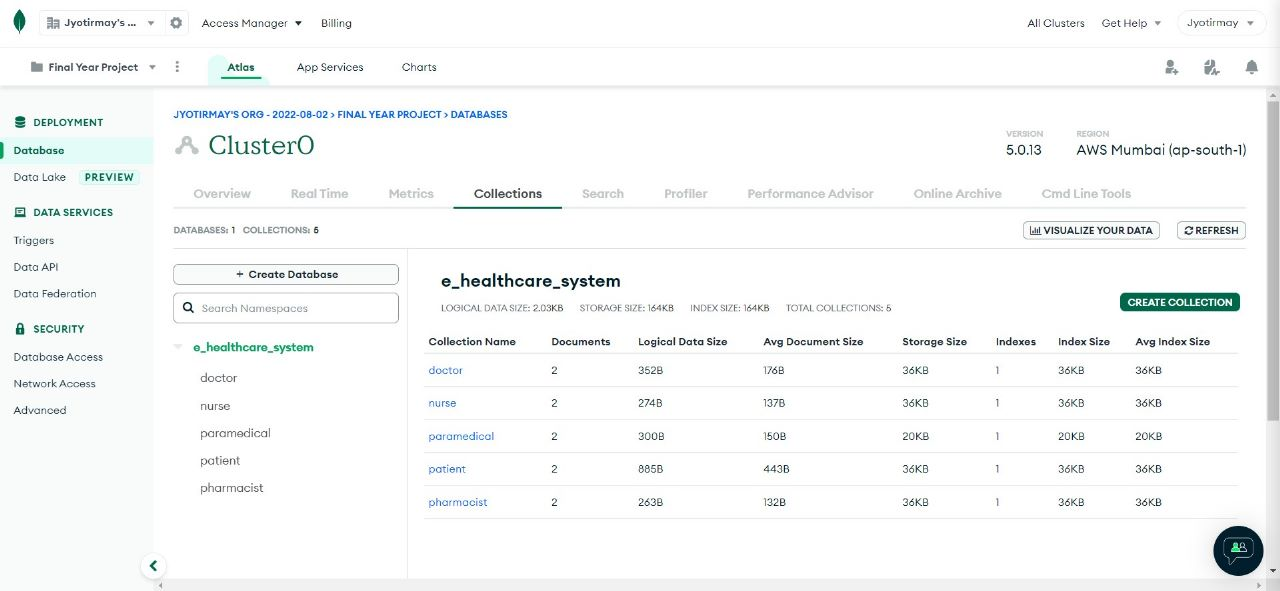


Login page where all patients and the staff will log in to their healthcare account

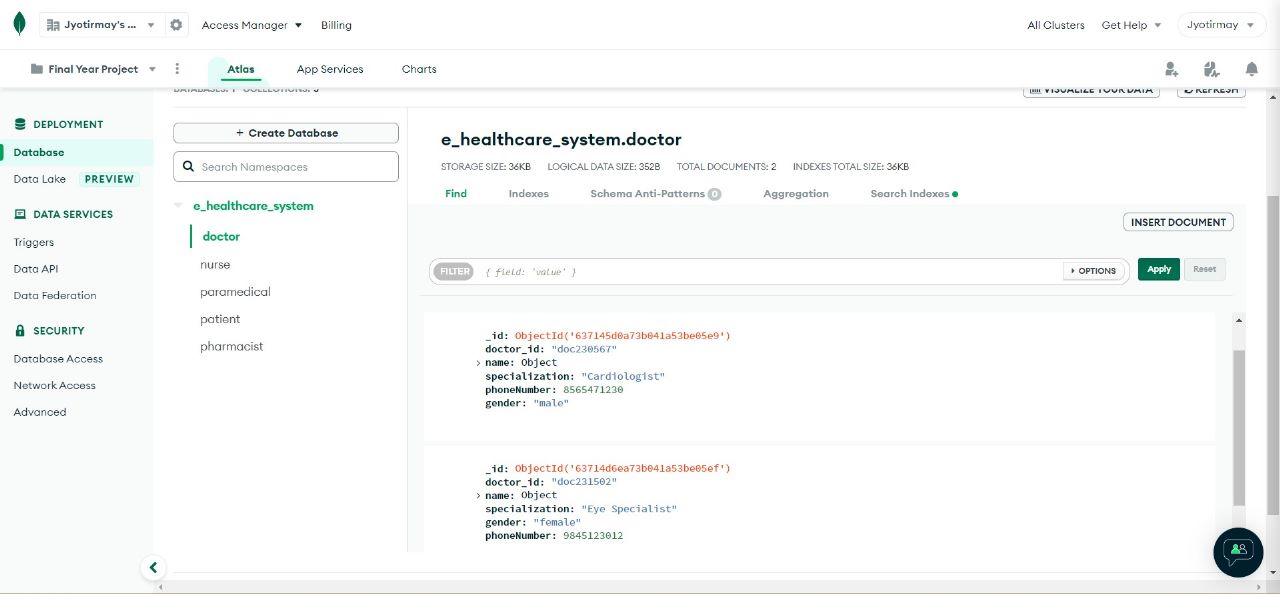


Database:-

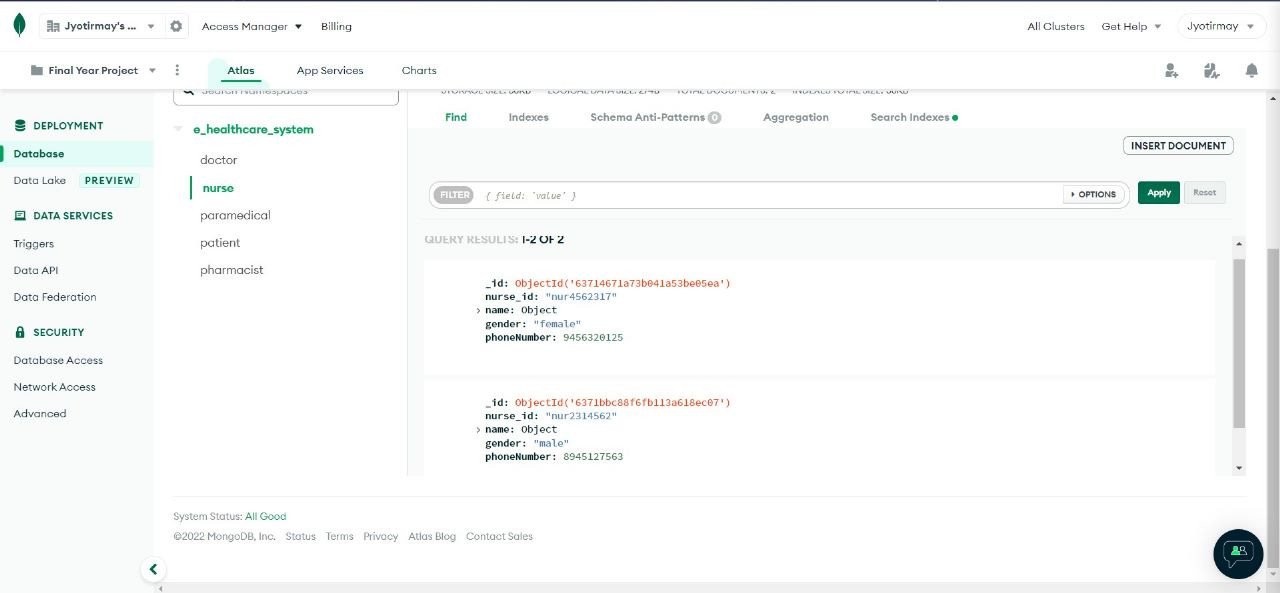
Database:- e\_healthcare\_system with its collections



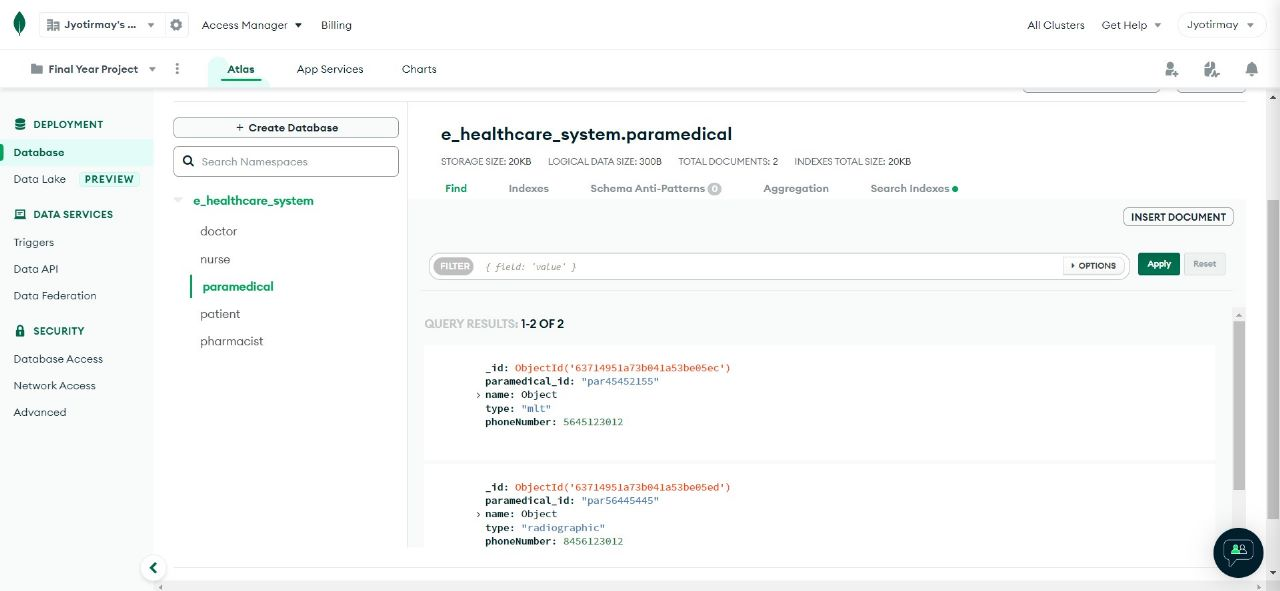
Doctor collection with documents



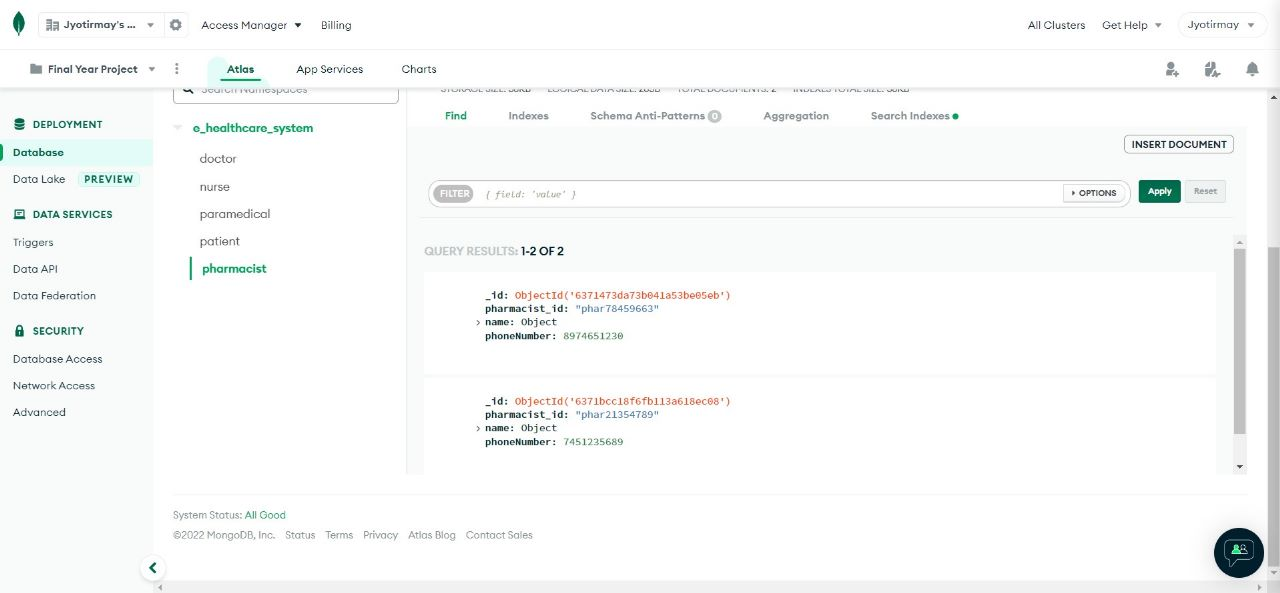
Nurse collection with documents



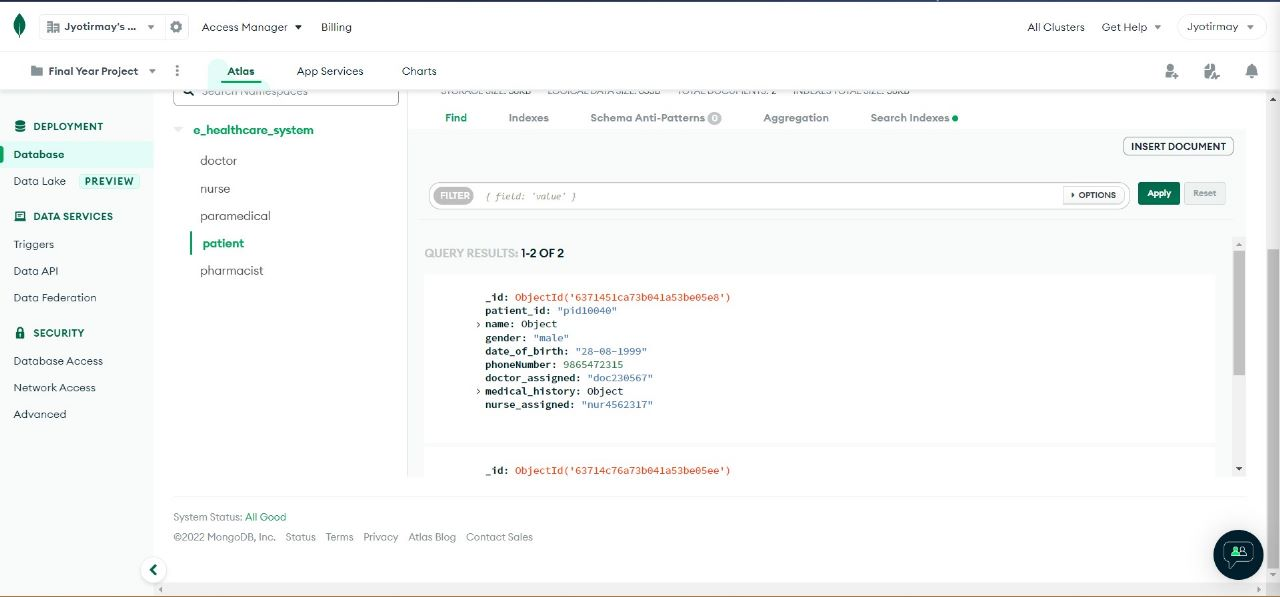
Paramedical collection with documents

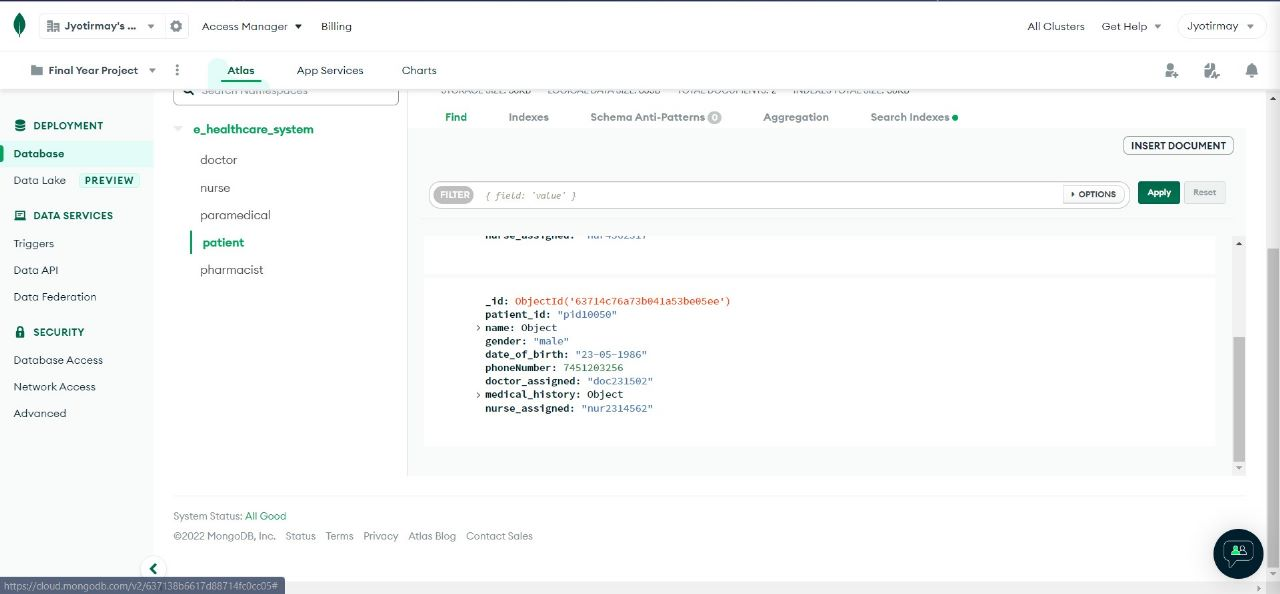


Pharmacist collection with documents



Patient collection with documents





**ALGORITHM**

Users sign in and create an account by entering their basic information. This application facilitates user communication. Encrypting critical data when sending data from one computer to another or storing data on a computer is the practice of cryptography. Fernet is a block cipher mechanism that ensures that the encrypted message cannot be changed or read if the key is not present. The keys are encoded using URL-safe encoding. Fernet also employs 128-bit AES in CBC mode with PKCS7 padding, as well as HMAC authentication based on SHA256. Python includes a cryptography package that aids in the encryption and decryption of data. The cryptography package's fernet module provides built-in functions for generating the key using the encrypt and decrypt methods. Using the encrypt and decrypt methods, the cryptography package's fernet module provides built-in functions for generating the key, converting plaintext to cipher text, and decrypting cipher text back to plaintext.

**i) Generate\_key():** Using this procedure, a new fernet key is generated. Because the key is required to decipher the ciphertext, it must be kept secure. If the key is lost, the user will be unable to decrypt the communication.

**ii) Encrypt(data):**  This encryption produces a "Fernet token," also known as ciphertext. The encrypted token included the current timestamp when it was generated in plaintext. The encrypting procedure will fail if the data is not in bytes. Token decryption (TTL = None): This procedure decrypts the Fernet token passed as a parameter. If the decryption is successful, the original plaintext is returned; otherwise, an exception is thrown. To decrypt the Fernet token (ciphertext), the token (bytes) is passed. The 'TTL' specifies how long a token is valid. To install the cryptography package, run the following command: cryptography pip install 'from cryptography The command fernet import Fernet' is used to load the Fernet module from the cryptography package.

**Conclusion**

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

The architecture offers a web-enabled framework that integrates with the activities of doctors, nurses, paramedical, patients, and pharmacists. Heath-care security should aim to enhance the quality of healthcare while cutting costs.

Our model aims at protecting health care from unauthorized user attacks. The research looks at the sophisticated multifaceted or authenticated health records that are secure in the system.

**Reference**

[1] “Enhanced Data Security in Cloud-base E-Health Care System” by Asha Bhadra S Kumar, Aswanthy N, Elizabeth K Jacob, Arya Binu, and Ms. Divya S B.

[2] <https://www.diva-portal.org/smash/get/diva2:647835/fulltext01.pdf>.

[3]   D. A. Garwin. (1993) Building a Learning Organization. Harvard Business Review. 73-91. Available: <https://hbr.org/1993/07/building-a-learning-organization>.

[5]        J. M. McGinnis, L. Stuckhardt, R. Saunders, and M. Smith, the *Best care at lower cost: the path to continuously learning health care in America*. National Academies Press, 2013.

[6]        J. Enticott, A. Johnson, and H. Teede, “Learning health systems using data to drive healthcare improvement and impact: a systematic review,” *BMC health services research,*vol. 21, no. 1, pp. 1-16, 2021. [Online]. Available: [**https://bmchealthservres.biomedcentral.com/articles/10.1186/s12913-021-06215-8#Tab3**](https://bmchealthservres.biomedcentral.com/articles/10.1186/s12913-021-06215-8#Tab3).

[7]        T. Foley and F. Fairmichael. “Professor Charles Friedman Interview.” The Learning Healthcare Project. [**https://www.learninghealthcareproject.org/section/evidence/25/50/professor-charles-friedman-%20interview**](https://www.learninghealthcareproject.org/section/evidence/25/50/professor-charles-friedman-%20interview)

[8]        The University of Michigan. “Revolutionizing Learning, Transforming Health.” The University of Michigan. [**https://medicine.umich.edu/dept/learning-health-sciences**](https://medicine.umich.edu/dept/learning-health-sciences)

[9]        MCBK. “Annual MCBK Public Meeting.” MCBK. [**https://mobilizecbk.med.umich.edu/news-events/annual-meetings**](https://mobilizecbk.med.umich.edu/news-events/annual-meetings)

[10]      MCBK. “Featured Events.” Mobilizing Computable Biomedical Knowledge (MCBK). [**https://mobilizecbk.med.umich.edu/news-events**](https://mobilizecbk.med.umich.edu/news-events)