Name: Sethumadhavan V

Reg.No: 19MIS0010

Project Title: Secure Data Sharing of Personal Health Records in MYSQL and Cloud Using AES Algorithm

Abstract:

New Advances in Cloud Computing Technology Enable rapid use of cloud platforms for business purposes it is increasing day by day. Aggregating data about companies Transactions, communications, business model architecture, etc. A lot of other information is stored on cloud platforms, Visit our business partners in Dubai together. Under consideration Security aspects of data stored in the cloud must be high Protected and accessible by authentication. Was suggested this system focuses on evaluating the integrity monitoring model of the cloud where security and data protection systems are located if checked, algorithms are used to determine data protection. The proposed model is developed using Cryptographic Algorithms where input data is stored in the cloud Bring Your Own Encryption Key (BYOEK) platform. Or the safety of the BYOEK model has been evaluated and verified from the following perspectives. For a given test model in terms of comparison of execution time and data trading.

Objection:

In this paper we focus on cryptographic algorithms where input data is stored in the cloud Bring Your Own Encryption Key (BYOEK) platform. Or the safety of the BYOEK model has been evaluated and verified from the following perspectives. For a given test model in terms of comparison of execution time and data trading.

Scope of Project:

The scope of the project is to provide a secure auditing method is to store the data on the cloud in a secure manner.

Problem Statement

Cloud computing is almost maintenance-free in terms of managing local storage. However, it becomes a potential security issue when the data owner outsources the data to the could as the cloud server usually is provided by an untrusted third party. with the data being shared in a group of users, cloud computing faces a challenge of managing access control of the encrypted data.

EXISTING SYSTEM:

The author presented a system that maintains the cloud auditing Protocol in which the medical data accounts are securely transferred with a privacy preserving model. Not perform the privacy preserving data communication protocol that enables the user to communicate the data in a secure Gateway with high level of encryption. The presented system is developed with a privacy preserving transform on a cloud platform with a secure encryption and decryption process. Homomorphic transform technique is used with appropriate differential models. To provide a health integrity approach on sending the patient records in a more secure way. The encryption process needs to be done before storing the data into the cloud. The presented system discusses the mobile based health care system. The author presented a system in which the ng techniques for Incorporated to achieve encrypted data. The proposed system focused on achieving efficient reliability.

PROPOSED SYSTEM:

The proposed model is developed using Cryptographic Algorithms where input data is stored in the cloud Bring Your Own Encryption Key (BYOEK) platform. Or the safety of the BYOEK model has been evaluated and verified from the following perspectives. For a given test model in terms of comparison of execute on time and data trading.

Advantage of the Project:

- Increase performance
- Improves reliability and flexibility
- Increase security
- improves privacy

Disadvantage of the Project:

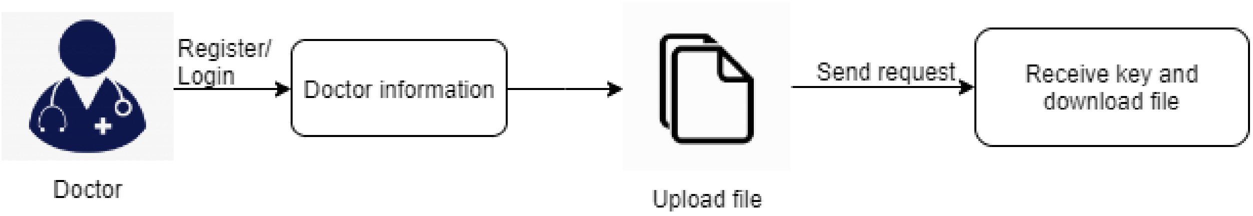
- Low performance
- Low flexibility
- Low on security
- Increased Cost
- Low on privacy

MODULES

- ➢ Doctor Models
- ➢ Patient Models
- ➢ Admin Models
- ➢ Cloud Models

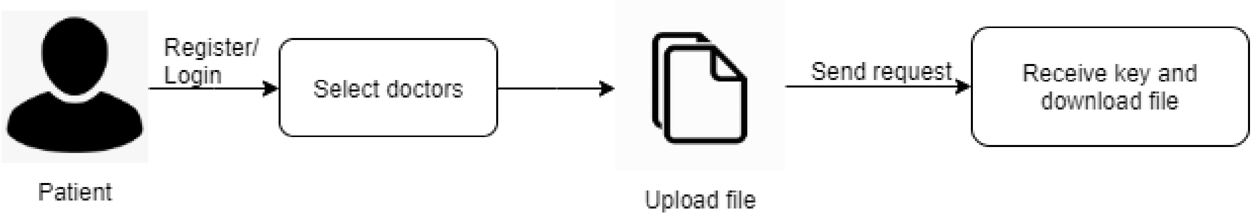
1. DOCTOR GIVES PRESCRIPTION:

Doctor register and login then enters the details of information then view the file which uploaded by the patient. Doctor send request the file. Doctor receive the secret key and download the file which patient given and know the message. Doctor reply for the patient queries and upload file.



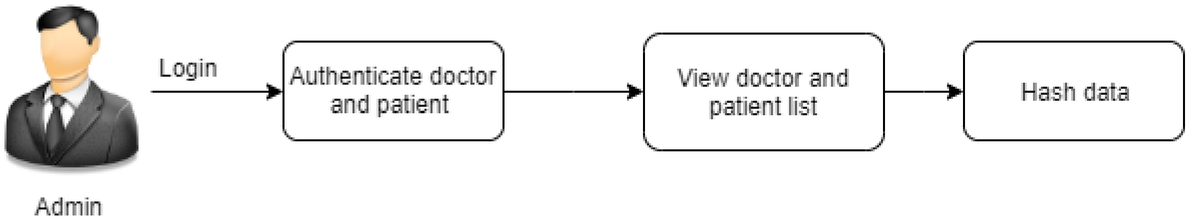
2. PATIENT SEND MESSAGE TO DOCTOR:

Patient Register and login then view the doctor list and select the doctor and send the problems in message file format. The file while upload it will be encrypted and stored. Patient can view file and send request. Patient receive the secret key and download the file which doctor given and know the message.



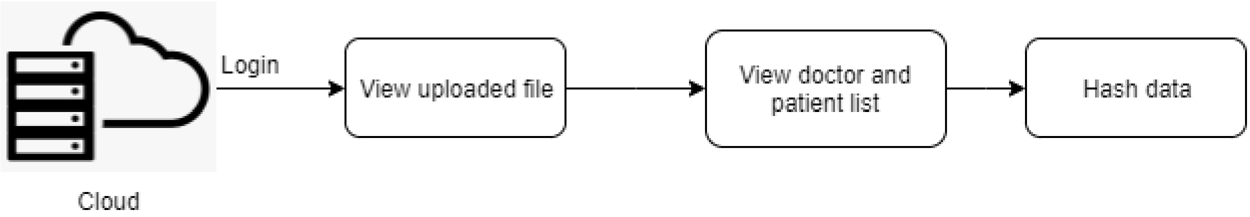
3 ADMIN AUTHENTICATE THE REQUESTS:

Admin login then authenticate doctor and accept the request given and the details will be converted into blocks of hash data and send key to doctor. Admin authenticate patient and accept the request given and the details will be converted into blocks of hash data and send key to patient and also has the doctor list and patient list.

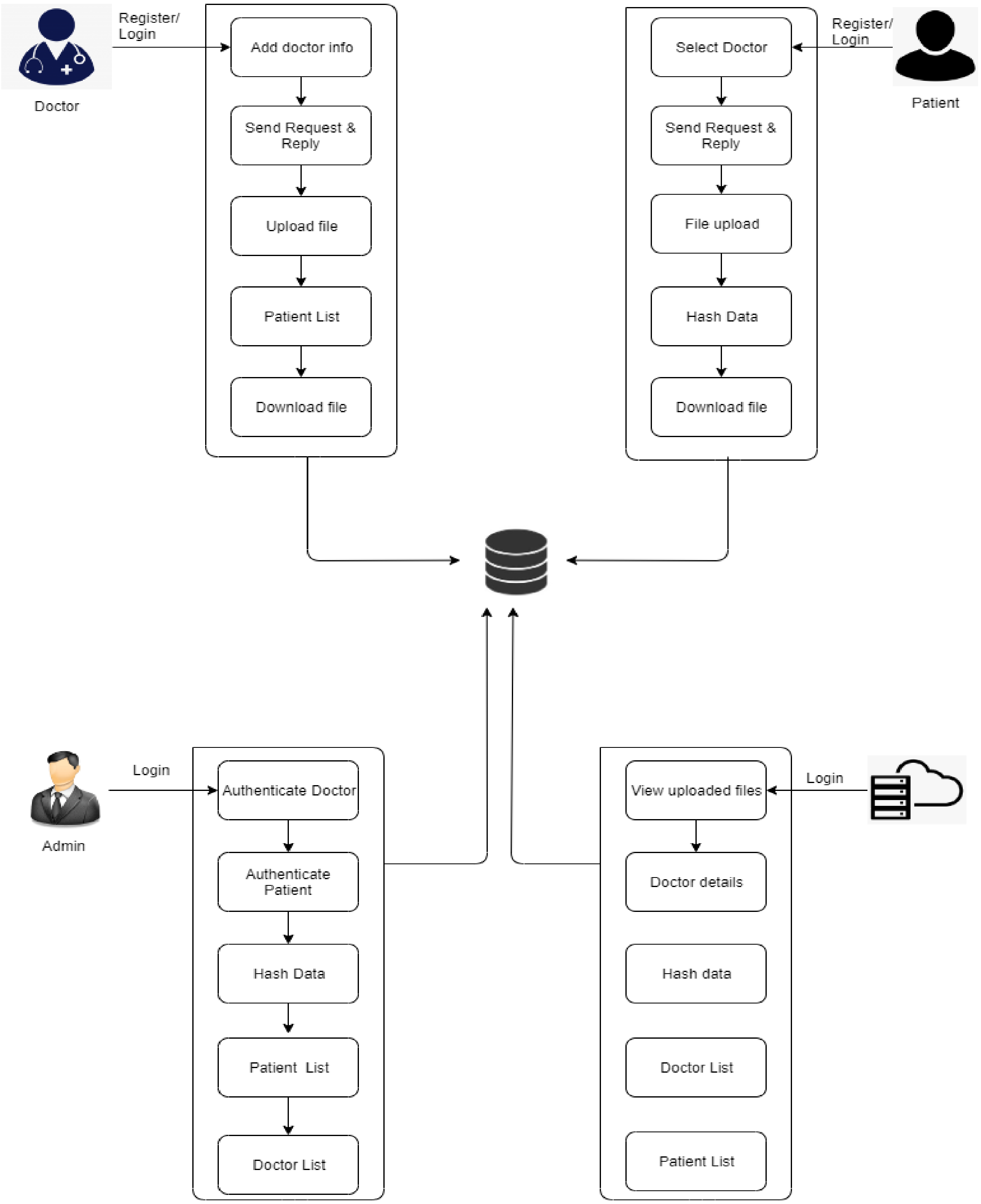


4 CLOUD MAINTAINS THE DETAILS:

Cloud login then maintains the details of uploaded files, doctor information, doctor list, hash data and patient list.



5. MODULE DIAGRAM:



ALGORITHM USED:

- SHA-512 Algorithm
- AES algorithm

1. AES ALGORITHM:

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback, but it was found slow.

The features of AES are as follows –

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Operation of AES:

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes.

These 16 bytes are arranged in four columns and four rows for processing as a matrix − Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

2. SHA-512 ALGORITHM:

SHA-512 is a hashing algorithm that performs a hashing function on some data given to it. Hashing algorithms are used in many things such as internet security, digital certificates and even blockchains. Since hashing algorithms play such a vital role in digital security and cryptography, this is an easy-to-understand walkthrough, with some basic and simple maths along with some diagrams, for a hashing algorithm called SHA-512. It's part of a group of hashing algorithms called SHA-2 which includes SHA-256 as well which is used in the bitcoin blockchain for hashing.

3. Hashing Functions:

Hashing functions take some data as input and produce an output (called hash digest) of fixed length for that input data. This output should, however, satisfy some conditions to be useful.

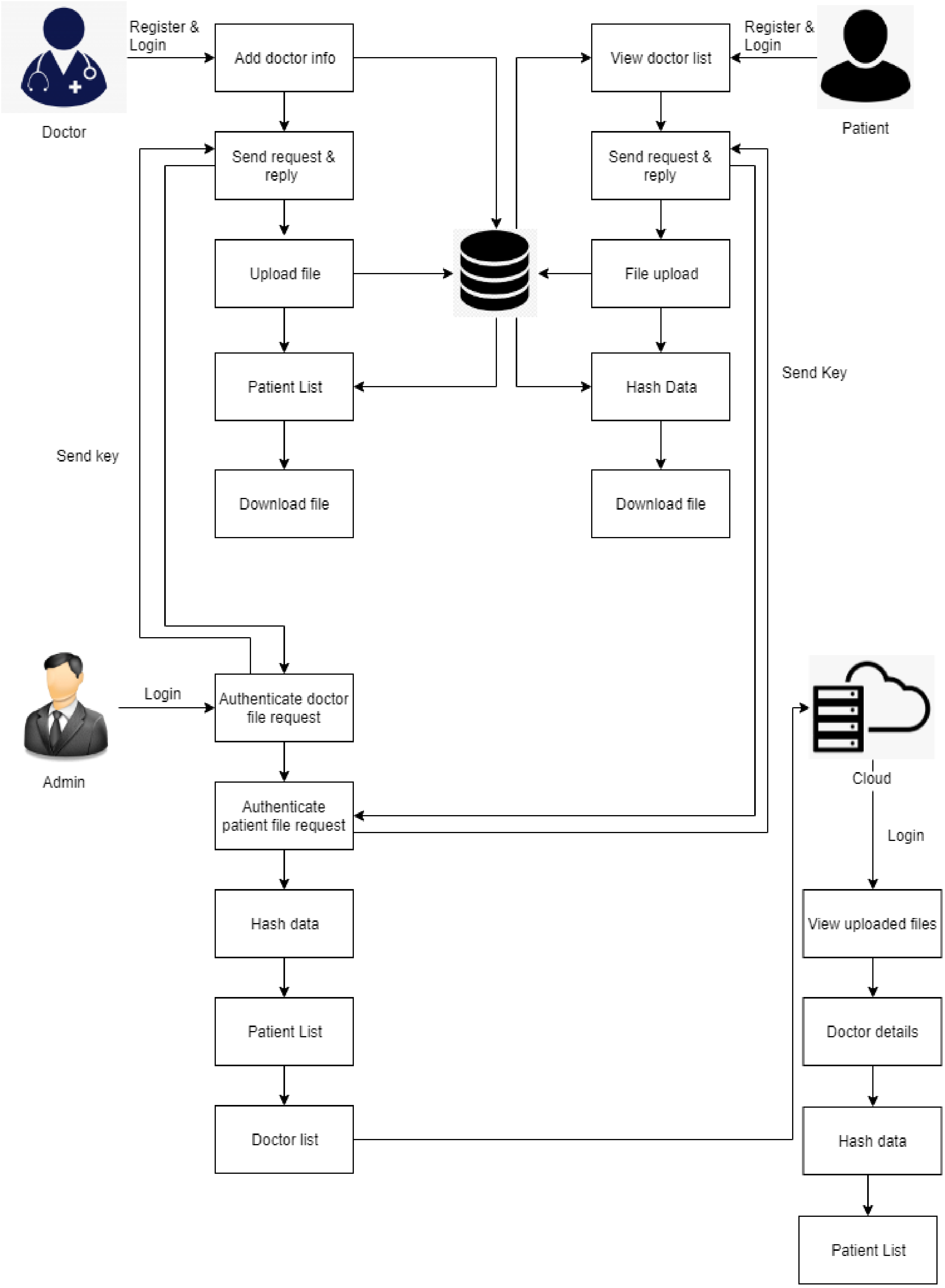
1. **Uniform distribution:** Since the length of the output hash digest is of a fixed length and the input size may vary, it is apparent that there are going to be some output values that can be obtained for different input values. Even though this is the case, the hash function should be such that for any input value, each possible output value should be equally likely. That is to say that every possible output has the same likelihood to be produced for any given input value.

2. **Fixed Length:** This is should be quite self-explanatory. The output values should all be of a fixed length. So, for example, a hashing function could have an output size of 20 characters or 12 characters, etc. SHA-512 has an output size of 512 bits.

3. **Collision resistance:** Simply speaking, this means that there aren't any or rather it is not feasible to find two distinct inputs to the hash function that result in the same output (hash digest).

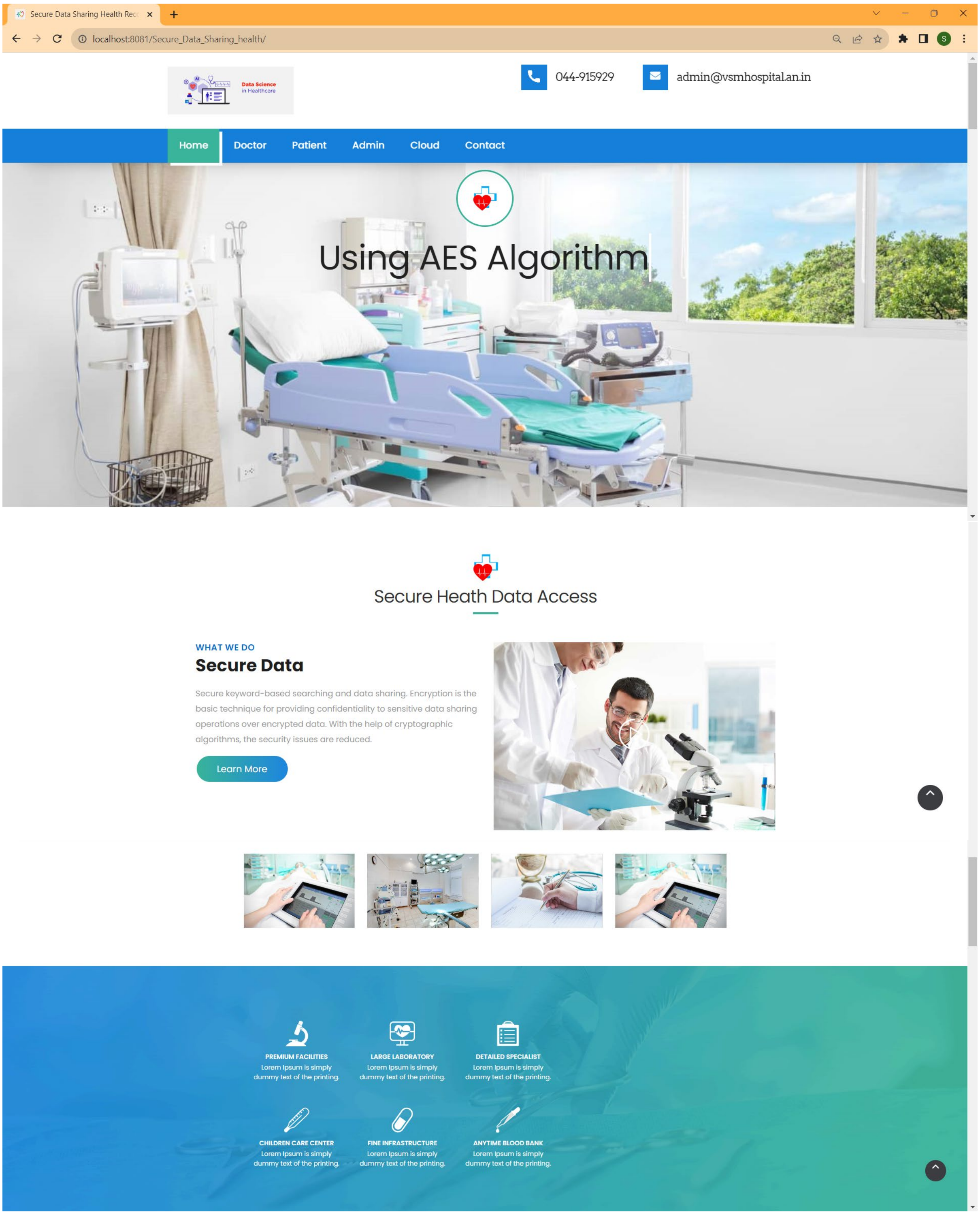
\

SYSTEM ARCHITECTURE:


Register & Login
Add doctor info
View doctor list
Register & Login
Doctor
Patient
Send request & reply
Send request & reply
Upload file
File upload
Patient List
Hash Data
Send Key
Send key
Download file
Download file
Admin
Login
Authenticate doctor file request
Cloud
Authenticate patient file request
Login
Hash data
View uploaded files
Patient List
Doctor details
Doctor list
Hash data
Patient List

OUTPUT:

Home pages:



Secure Data Sharing Health Rec
localhost:8081/Secure_Data_Sharing_health/
Data Science in Healthcare
Home
Doctor
Patient
Admin
Cloud
Contact
Learn More

044-915929

admin@vsmhospital.an.in

Using AES Algorithm

Secure Heath Data Access

WHAT WE DO

Secure Data

Secure keyword-based searching and data sharing. Encryption is the basic technique for providing confidentiality to sensitive data sharing operations over encrypted data. With the help of cryptographic algorithms, the security issues are reduced.

PREMIUM FACILITIES
Lorem Ipsum is simply dummy text of the printing.

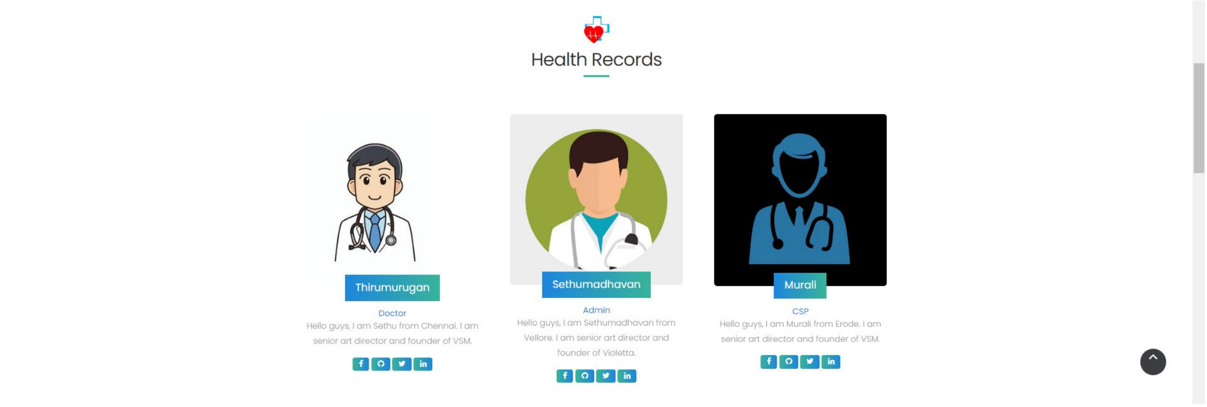
LARGE LABORATORY
Lorem Ipsum is simply dummy text of the printing.

DETAILED SPECIALIST
Lorem Ipsum is simply dummy text of the printing.

CHILDREN CARE CENTER
Lorem Ipsum is simply dummy text of the printing.

FINE INFRASTRUCTURE
Lorem Ipsum is simply dummy text of the printing.

ANYTIME BLOOD BANK
Lorem Ipsum is simply dummy text of the printing.



Health Records

Thirumurugan

Doctor

Hello guys, I am Sethu from Chennai. I am senior art director and founder of VSM.

Sethumadhavan

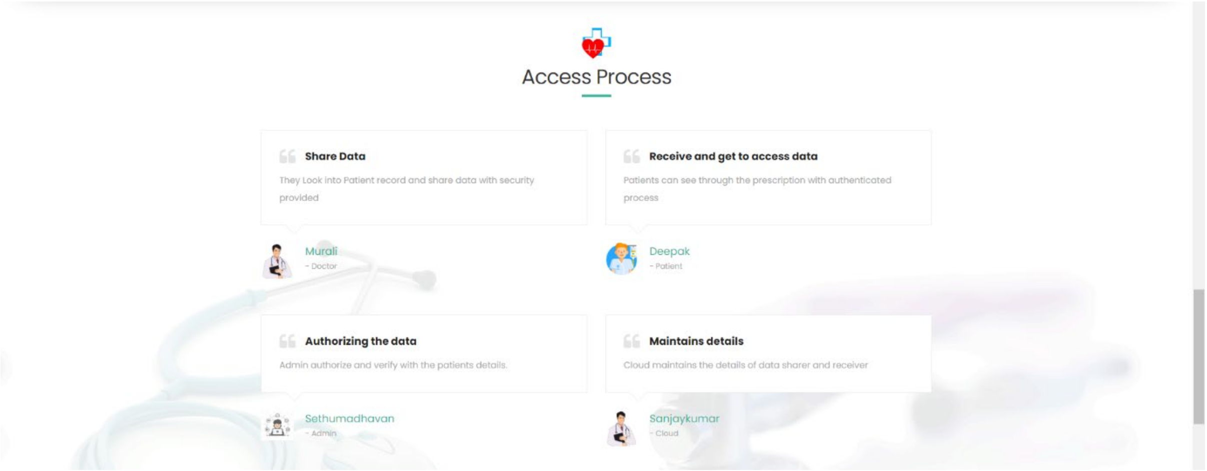
Admin

Hello guys, I am Sethumadhavan from Vellore. I am senior art director and founder of Violetta.

Murali

CSP

Hello guys, I am Murali from Erode. I am senior art director and founder of VSM.



Access Process

Share Data

They Look into Patient record and share data with security provided

Murali
- Doctor

Receive and get to access data

Patients can see through the prescription with authenticated process

Deepak
- Patient

Authorizing the data

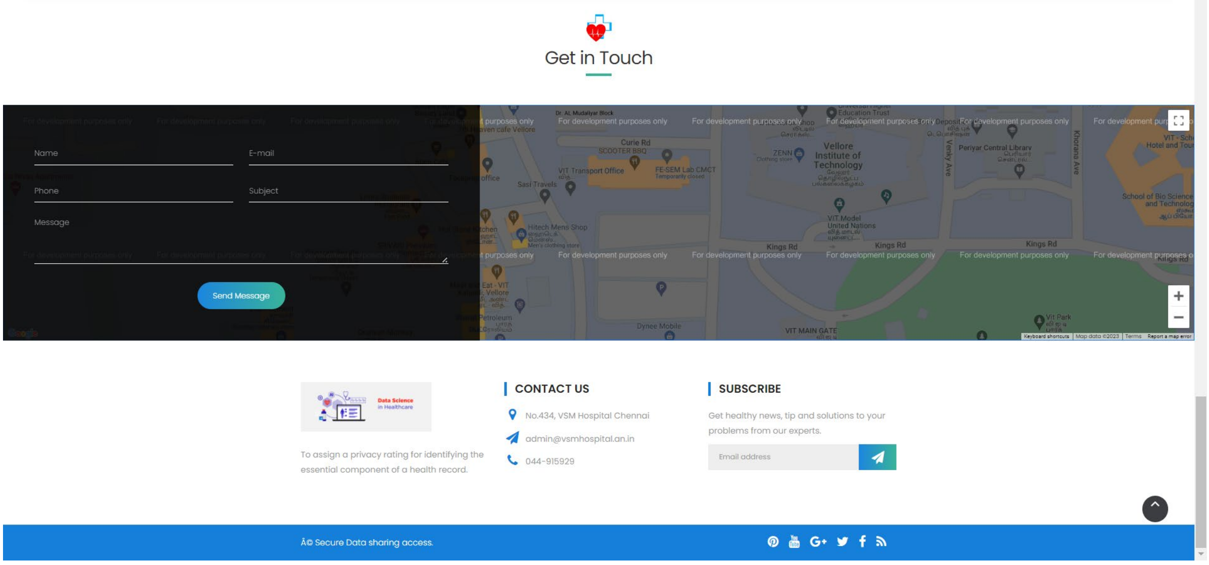
Admin authorize and verify with the patients details.

Sethumadhavan
- Admin

Maintains details

Cloud maintains the details of data sharer and receiver

Sanjaykumar
- Cloud



Get in Touch

Name

E-mail

Phone

Subject

Message

Send Message

Data Science in Healthcare

To assign a privacy rating for identifying the essential component of a health record.

CONTACT US

No.434, VSM Hospital Chennai

admin@vsmhospital.an.in

044-915929

SUBSCRIBE

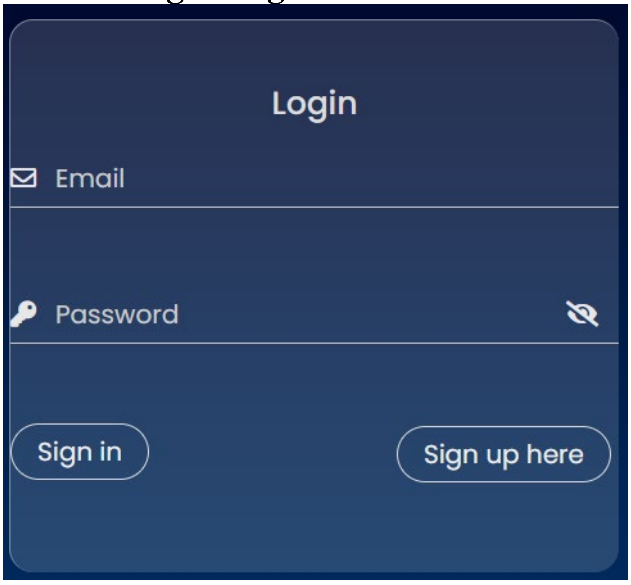
Get healthy news, tip and solutions to your problems from our experts.

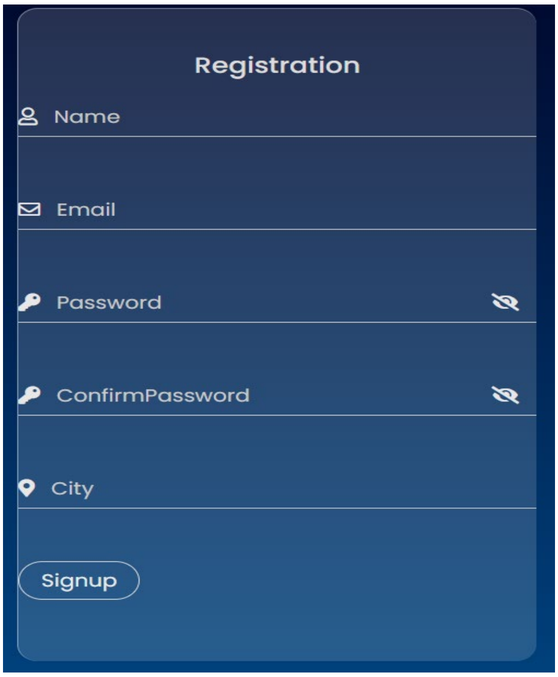
Email address

Â© Secure Data sharing access.

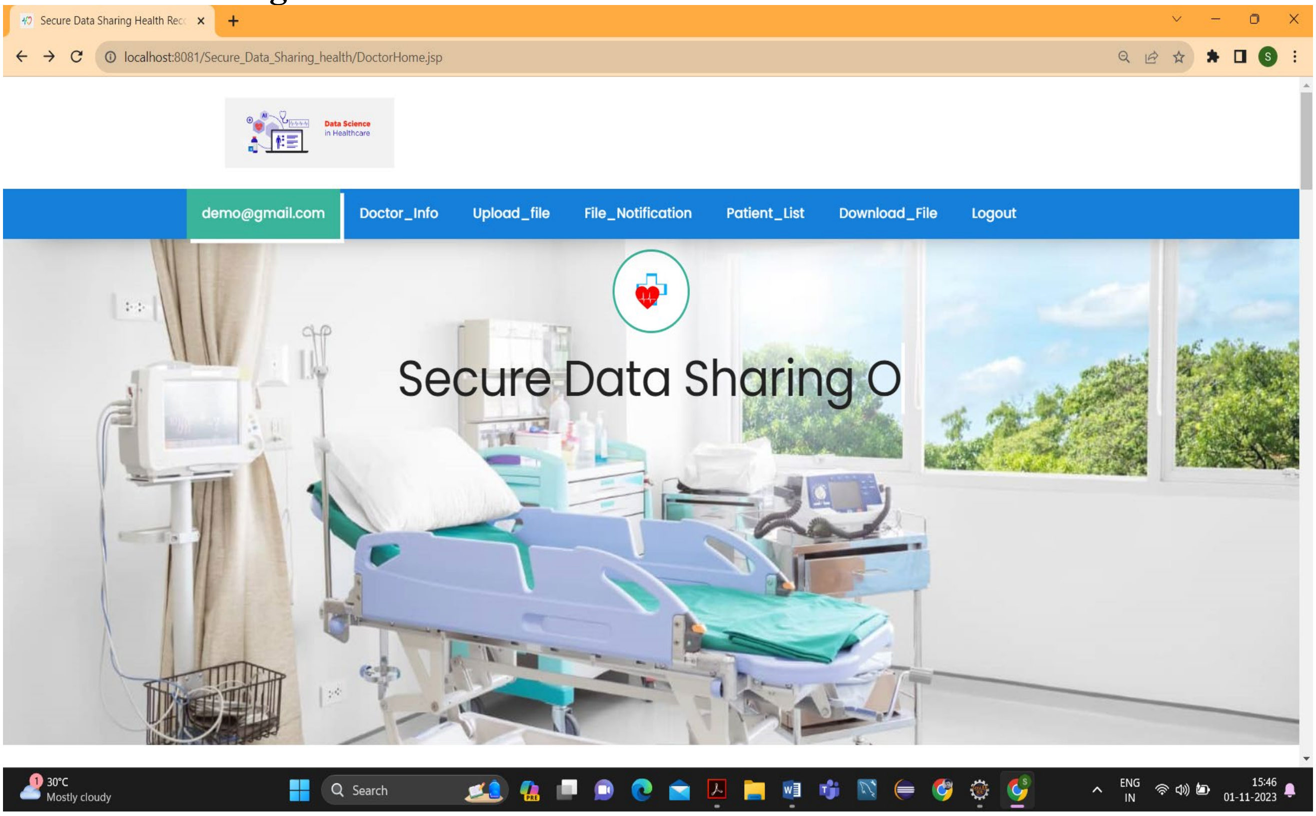
5.2.1 Doctor Modules:

Doctor Login Page:

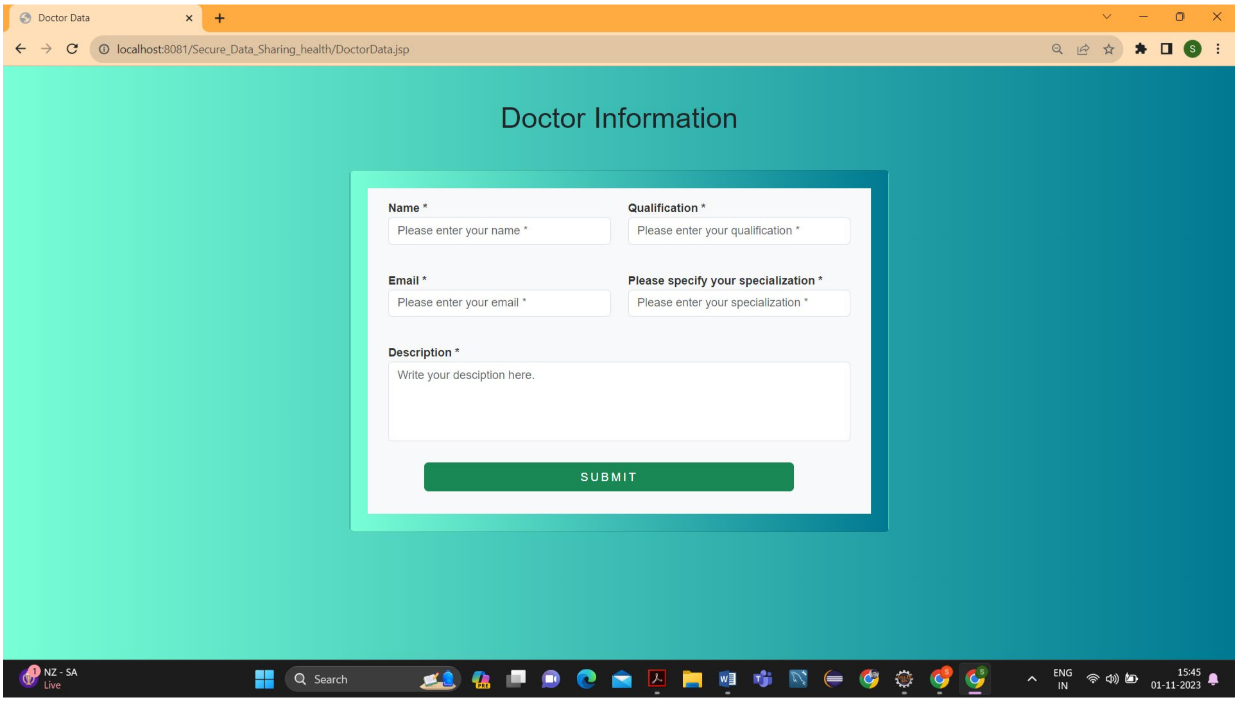




Doctor Home Page:



Doctor Information:



Doctor Data

localhost:8081/Secure_Data_Sharing_health/DoctorData.jsp

Doctor Information

Name *

Please enter your name *

Qualification *

Please enter your qualification *

Email *

Please enter your email *

Please specify your specialization *

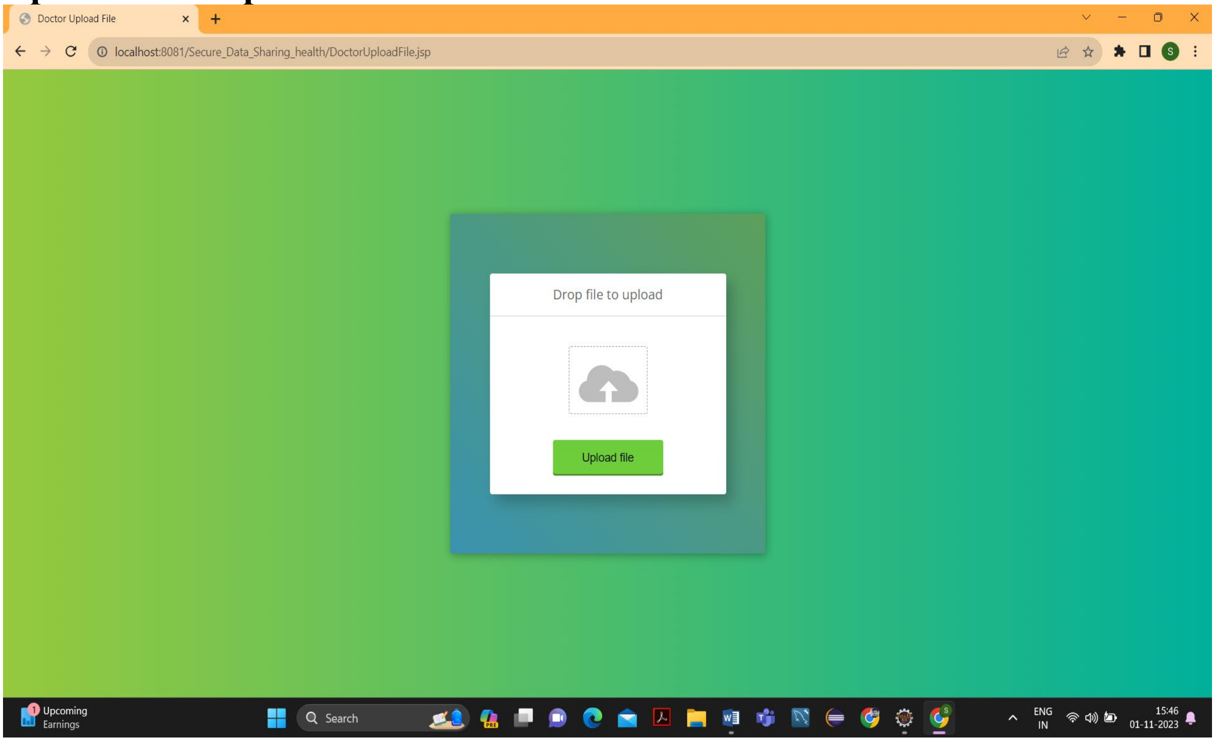
Please enter your specialization *

Description *

Write your desciption here.

SUBMIT

Upload Prescription File:



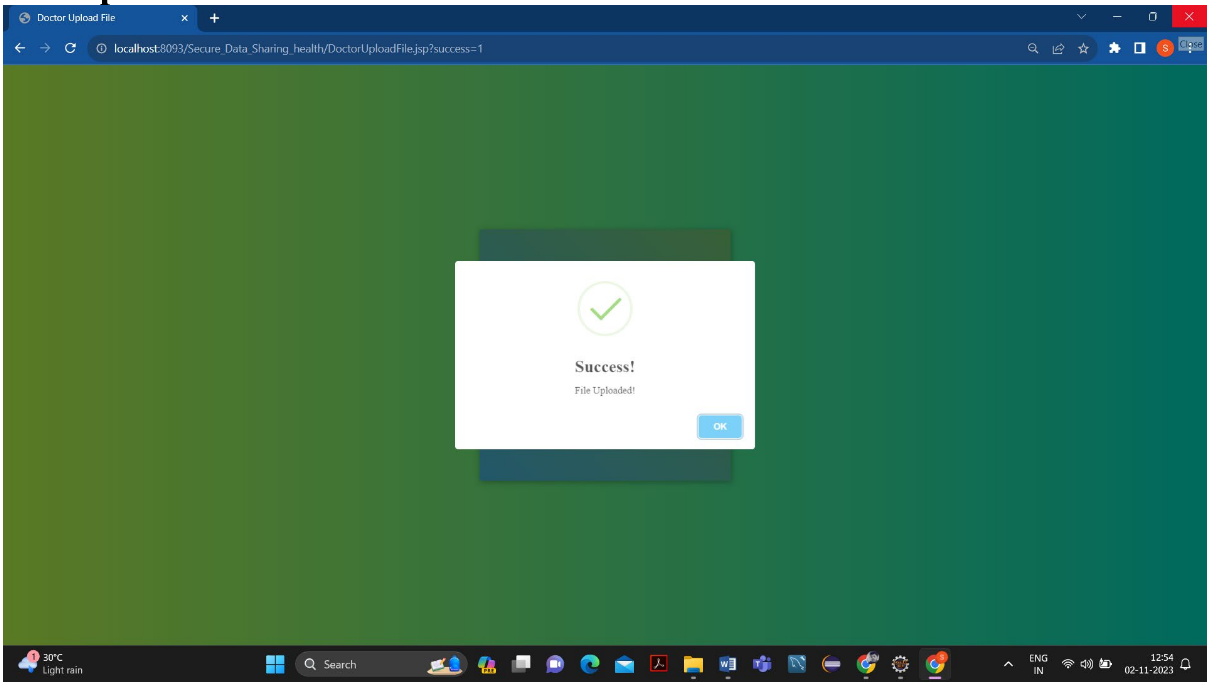
Doctor Upload File

localhost:8081/Secure_Data_Sharing_health/DoctorUploadFile.jsp

Drop file to upload

Upload file

File Uploaded Success:

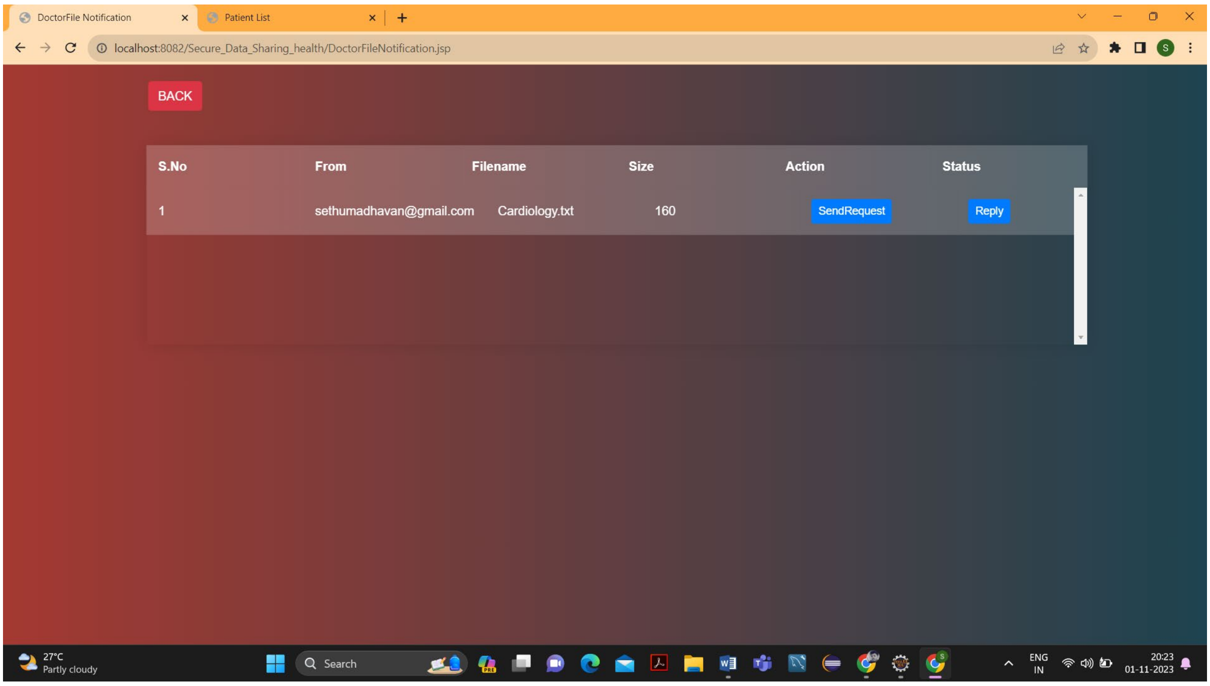


Success!

File Uploaded!

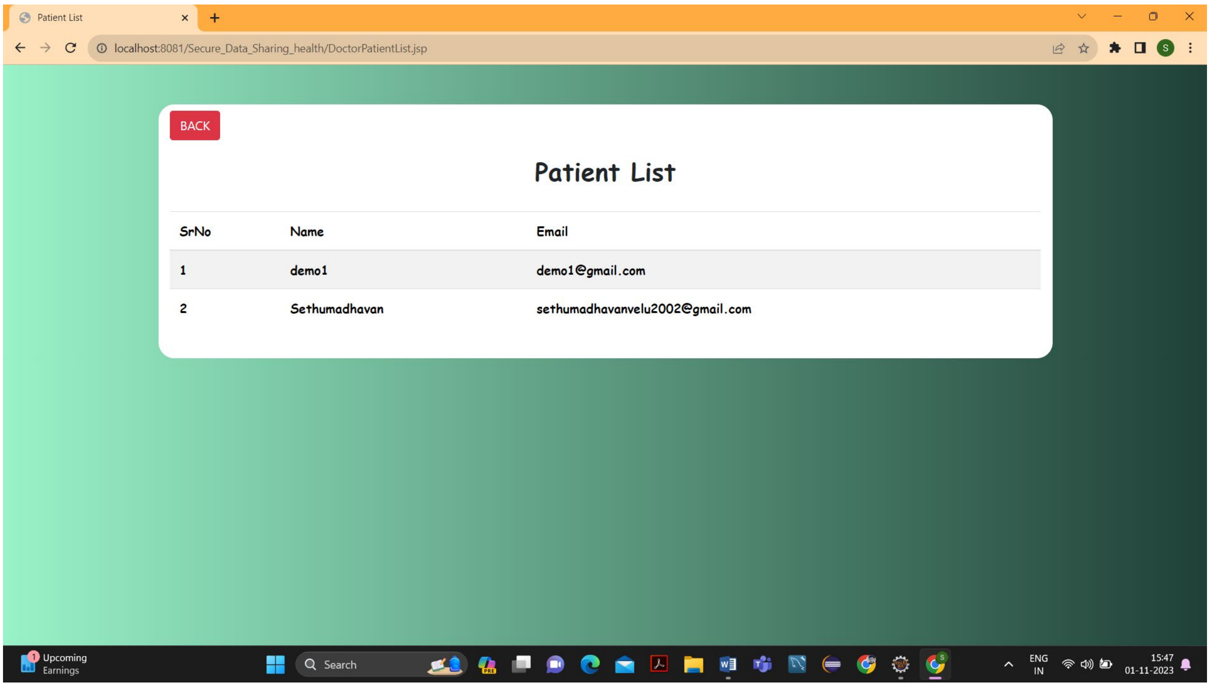
Doctor Upload File
localhost:8093/Secure_Data_Sharing_health/DoctorUploadFile.jsp?success=1
OK
30°C
Light rain
Search
ENG
IN
12:54
02-11-2023

File Notification:



S.No	From	Filename	Size	Action	Status
1	sethumadhavan@gmail.com	Cardiology.txt	160	SendRequest	Reply

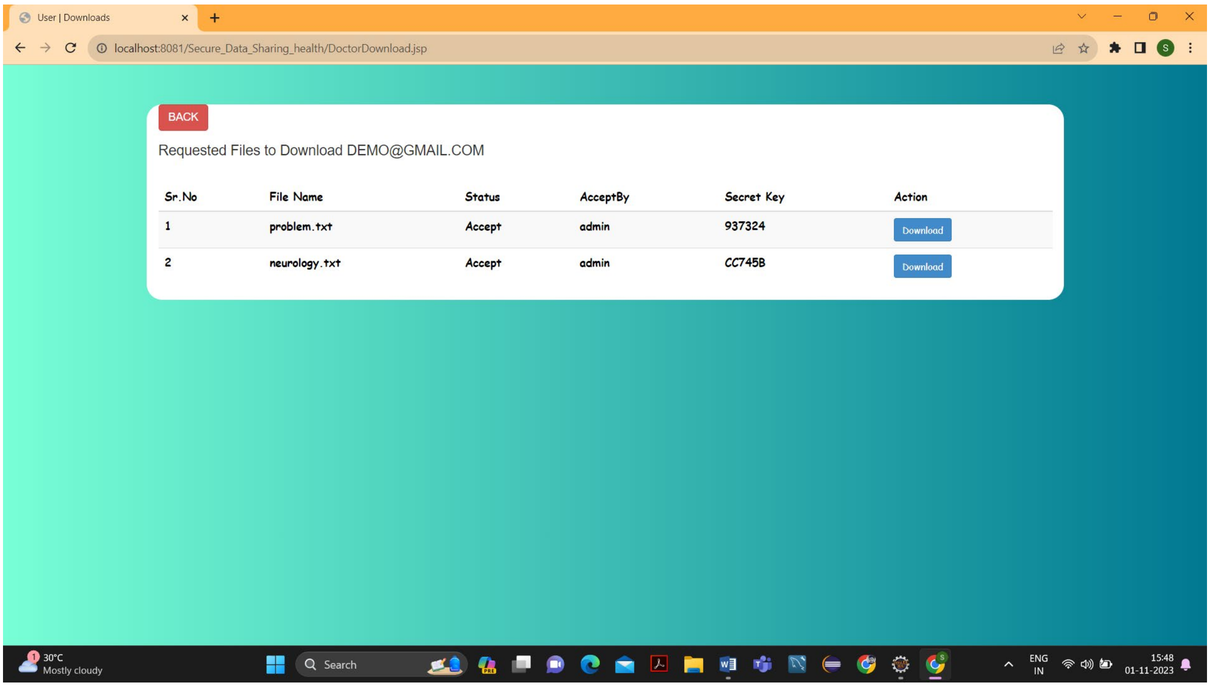
Patient List:


Patient List
localhost:8081/Secure_Data_Sharing_health/DoctorPatientList.jsp
BACK
Upcoming
Earnings
Search
ENG
IN
15:47
01-11-2023

Patient List

SrNo	Name	Email
1	demo1	demo1@gmail.com
2	Sethumadhavan	sethumadhavanvelu2002@gmail.com

Download File:

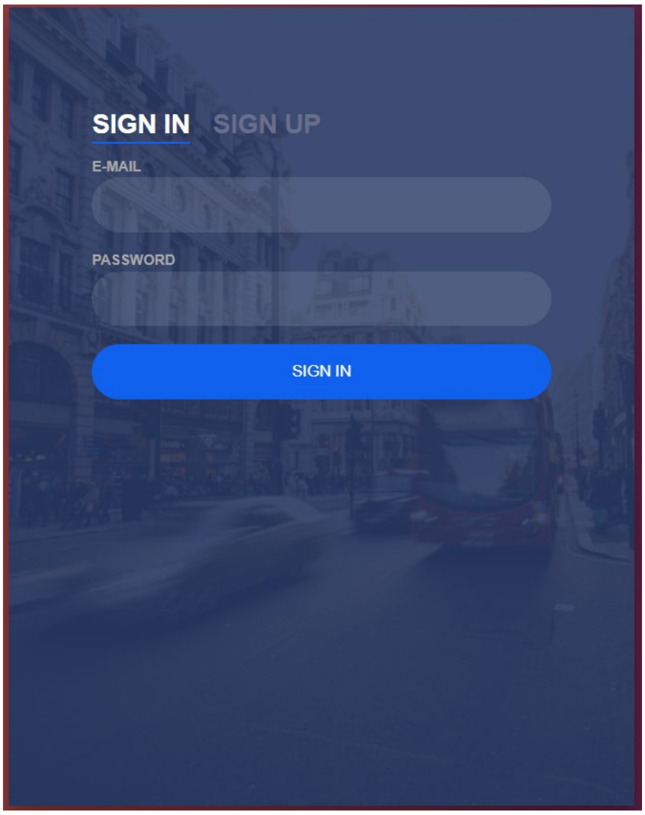


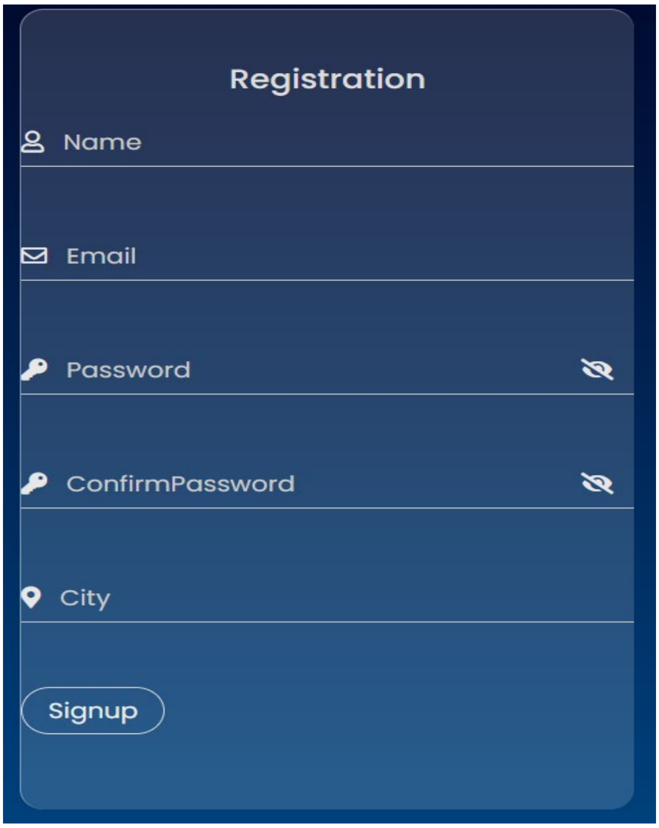
Requested Files to Download DEMO@GMAIL.COM

Sr.No	File Name	Status	AcceptBy	Secret Key	Action
1	problem.txt	Accept	admin	937324	Download
2	neurology.txt	Accept	admin	CC745B	Download

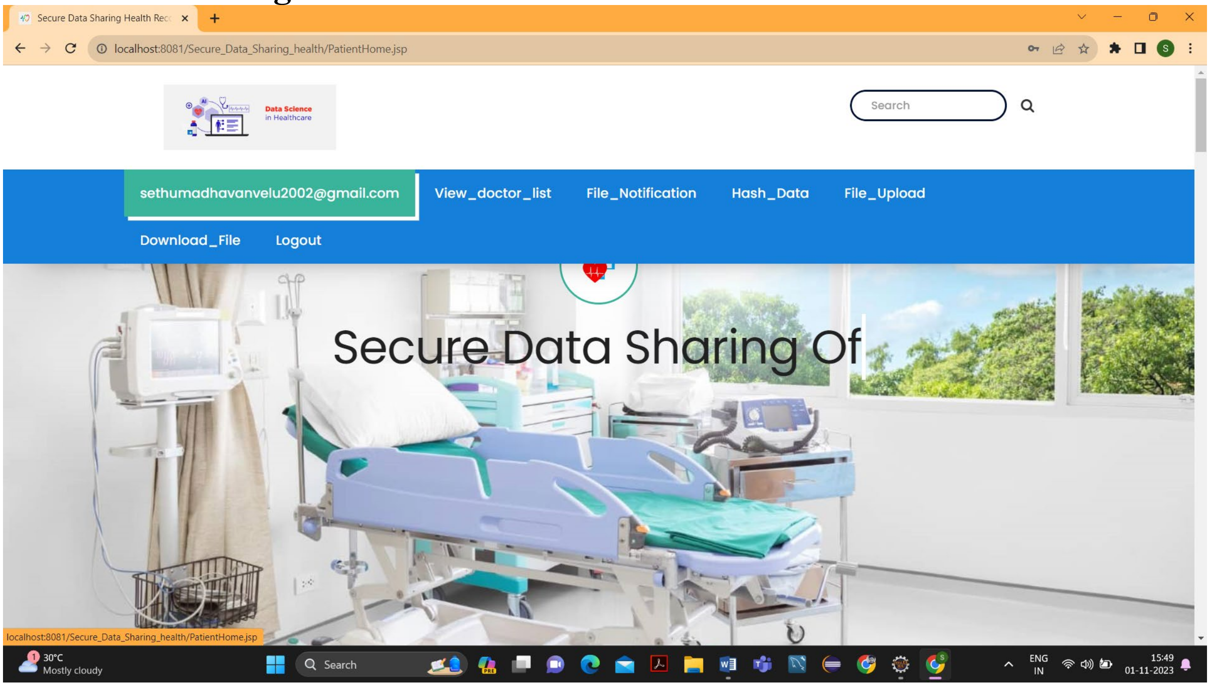
5.2.2Patients Modules:

Patient Login Page:

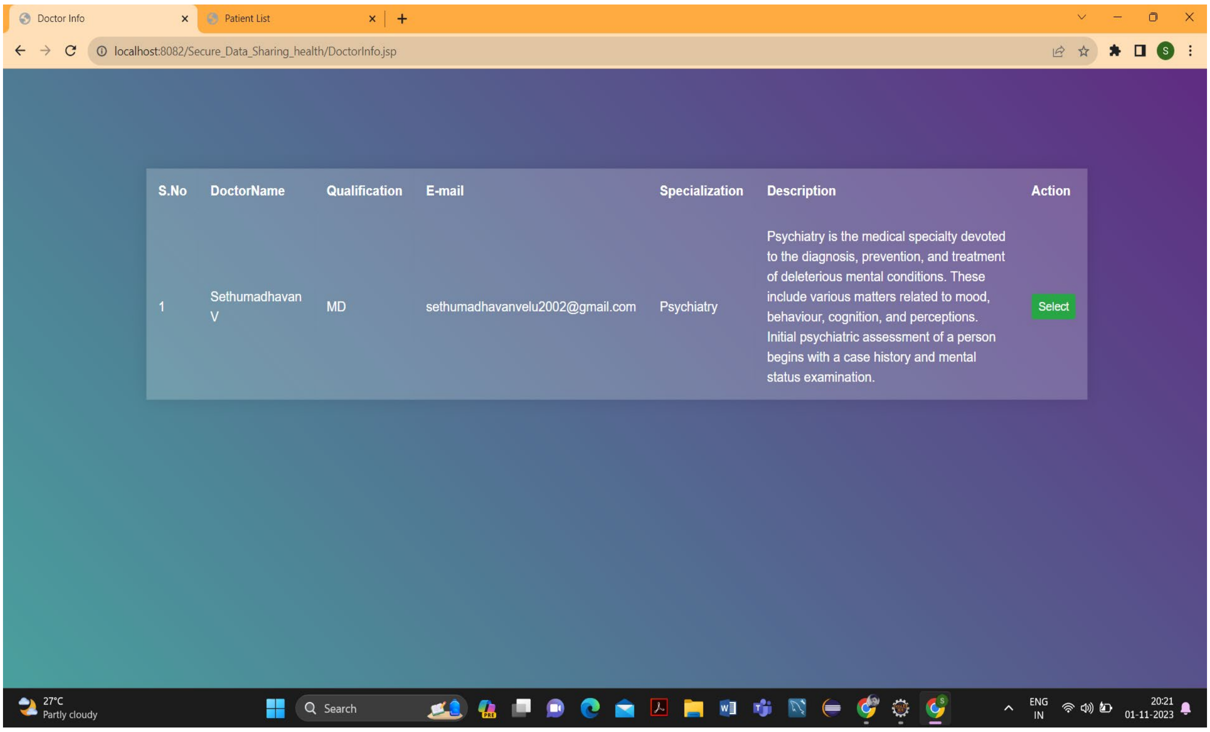




Patient Home Page:

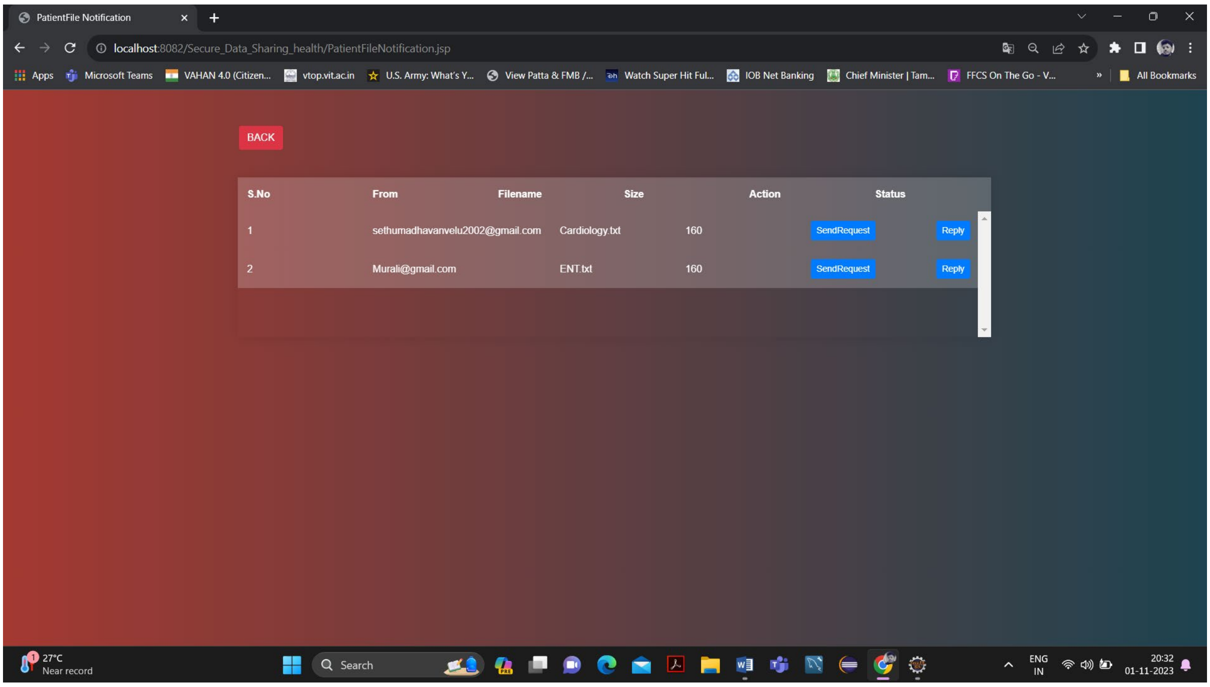

Secure Data Sharing Health Rec
localhost:8081/Secure_Data_Sharing_health/PatientHome.jsp
Data Science in Healthcare
Search
sethumadhavanvelu2002@gmail.com
View_doctor_list
File_Notification
Hash_Data
File_Upload
Download_File
Logout
Secure Data Sharing Of
localhost:8081/Secure_Data_Sharing_health/PatientHome.jsp
30°C
Mostly cloudy
Search
ENG
IN
15:49
01-11-2023

View Doctor List:



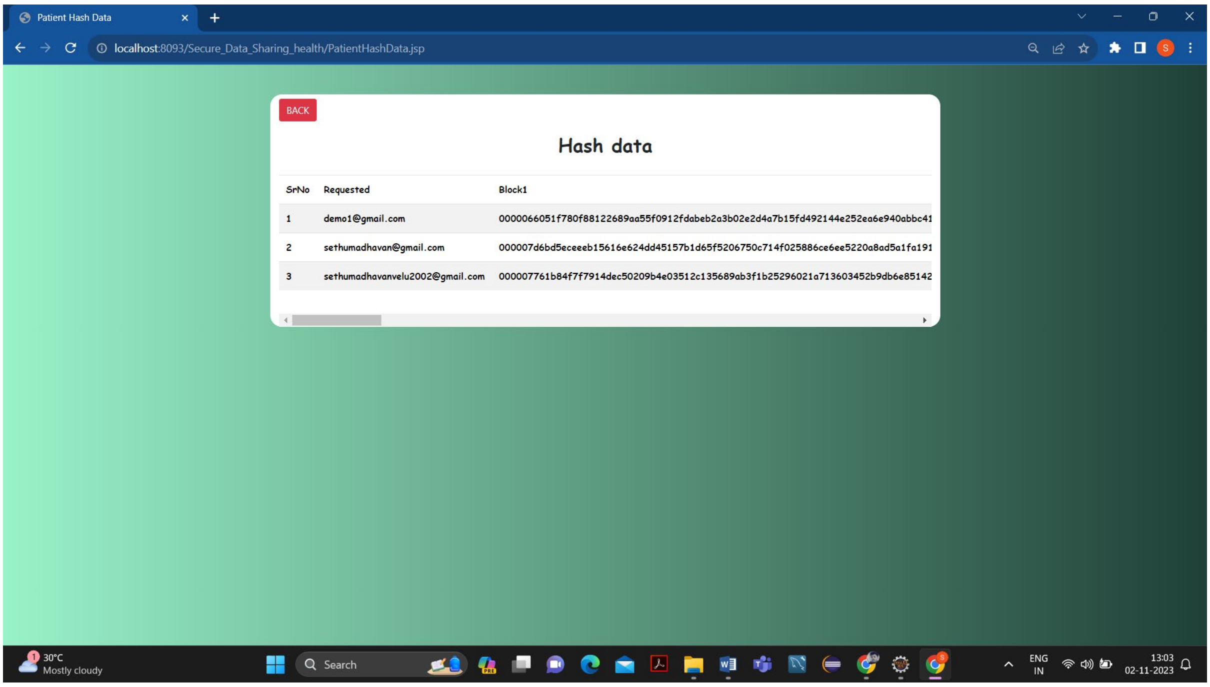
S.No	DoctorName	Qualification	E-mail	Specialization	Description	Action
1	Sethumadhavan V	MD	sethumadhavanvelu2002@gmail.com	Psychiatry	Psychiatry is the medical specialty devoted to the diagnosis, prevention, and treatment of deleterious mental conditions. These include various matters related to mood, behaviour, cognition, and perceptions. Initial psychiatric assessment of a person begins with a case history and mental status examination.	Select

File Notification:



S.No	From	Filename	Size	Action	Status
1	sethumadhavanvelu2002@gmail.com	Cardiology.txt	160	SendRequest	Reply
2	Murali@gmail.com	ENT.txt	160	SendRequest	Reply

Hash Data:

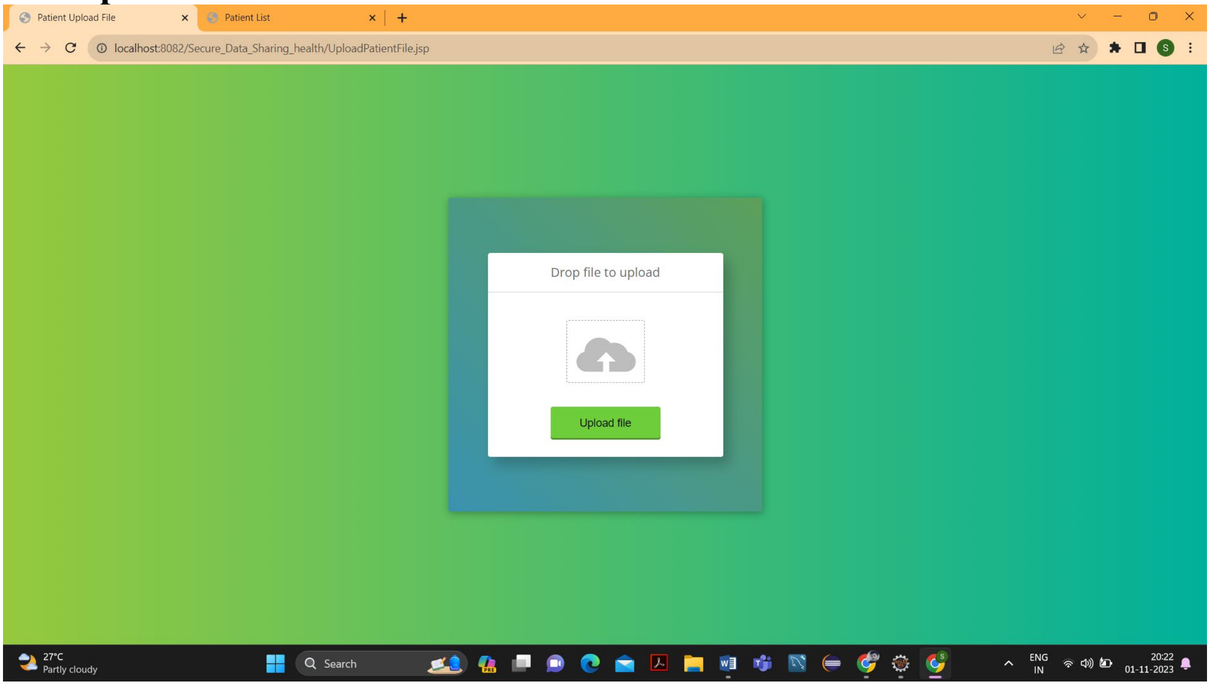


Patient Hash Data
localhost:8093/Secure_Data_Sharing_health/PatientHashData.jsp
BACK

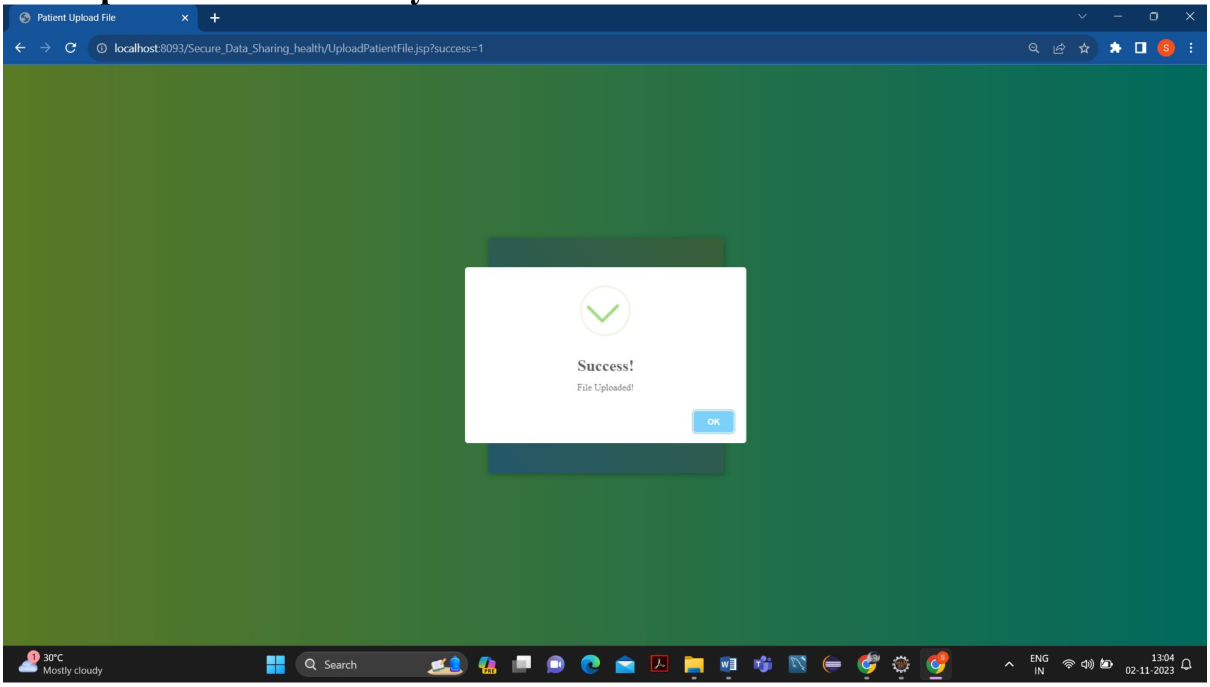
Hash data

SrNo	Requested	Block1
1	demo1@gmail.com	0000066051f780f88122689aa55f0912fdabeb2a3b02e2d4a7b15fd492144e252ea6e940abbc41
2	sethumadhavan@gmail.com	000007d6bd5eceeeb15616e624dd45157b1d65f5206750c714f025886ce6ee5220a8ad5a1fa191
3	sethumadhavanvelu2002@gmail.com	000007761b84f7f7914dec50209b4e03512c135689ab3f1b25296021a713603452b9db6e85142

File Upload:



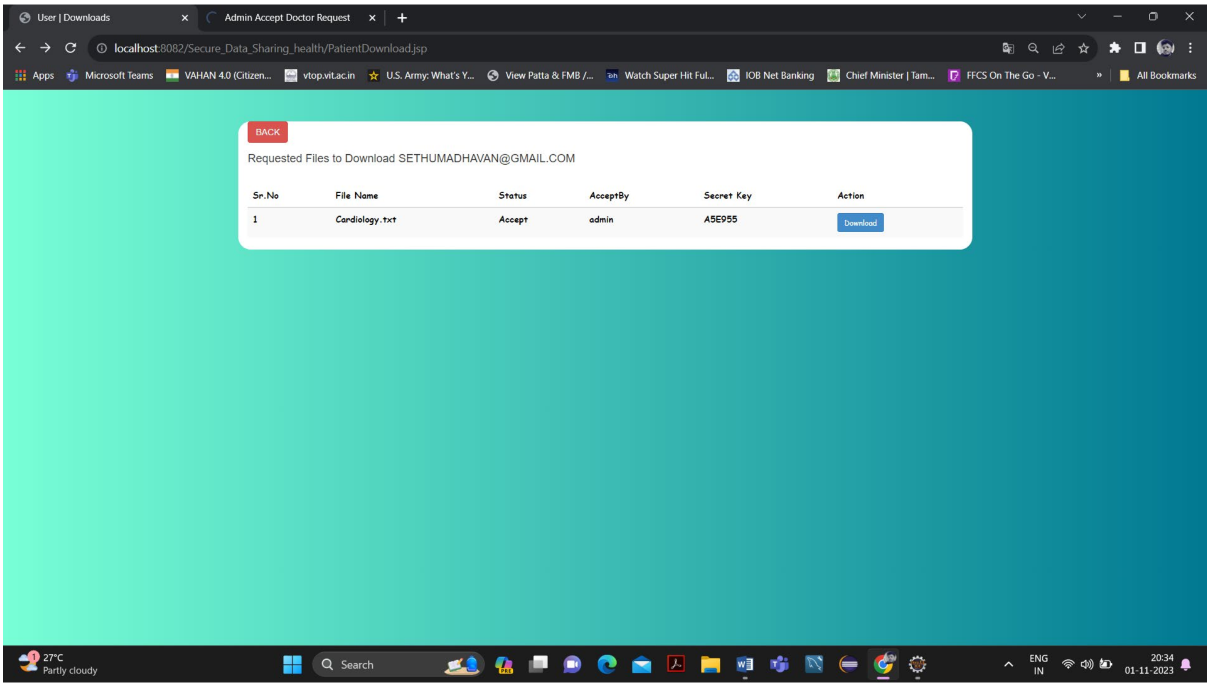
File Uploaded Successfully:


Patient Upload File
localhost:8093/Secure_Data_Sharing_health/UploadPatientFile.jsp?success=1
OK
30°C
Mostly cloudy
Search
ENG
IN
13:04
02-11-2023

Success!

File Uploaded!

Download File:

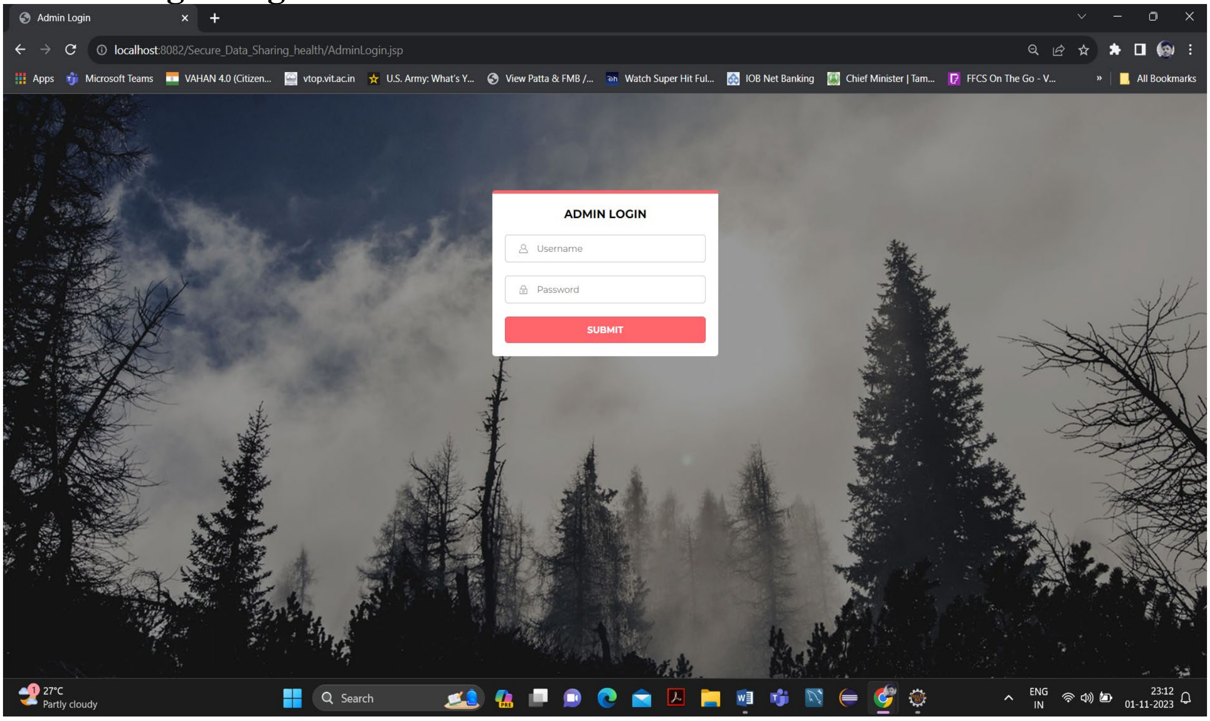


Requested Files to Download SETHUMADHAVAN@GMAIL.COM

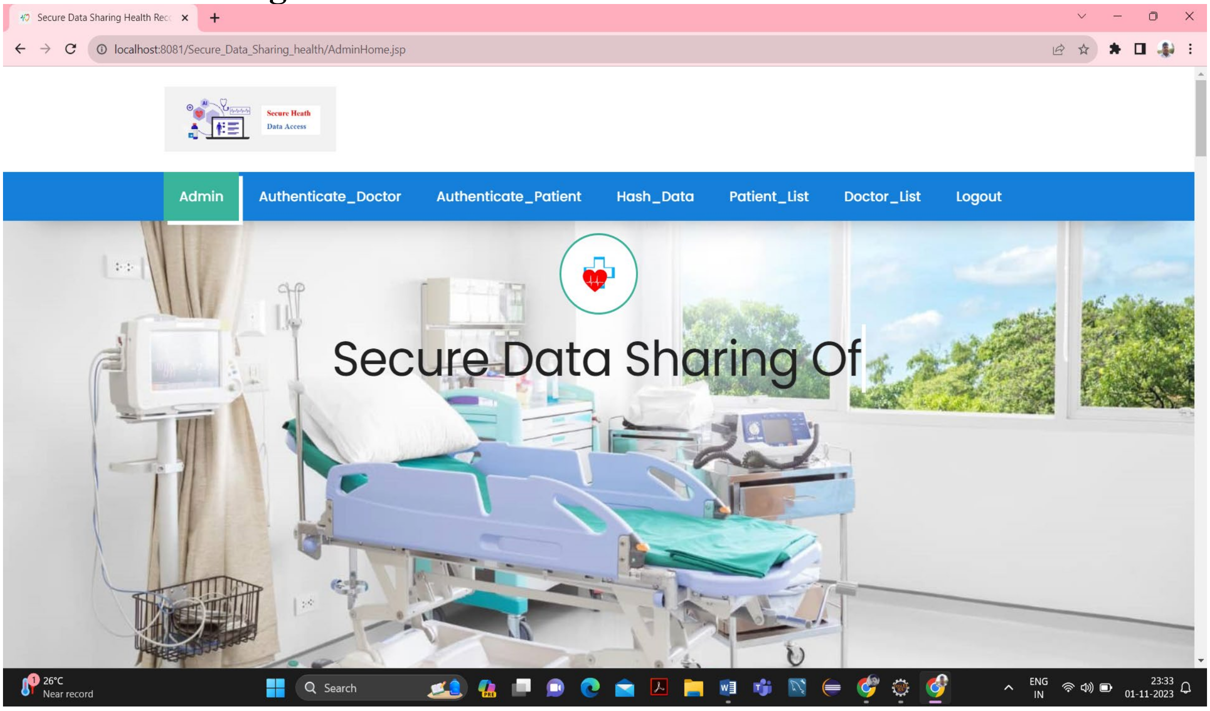
Sr.No	File Name	Status	AcceptBy	Secret Key	Action
1	Cardiology.txt	Accept	admin	A5E955	Download

5.2.3. Admin Modules:

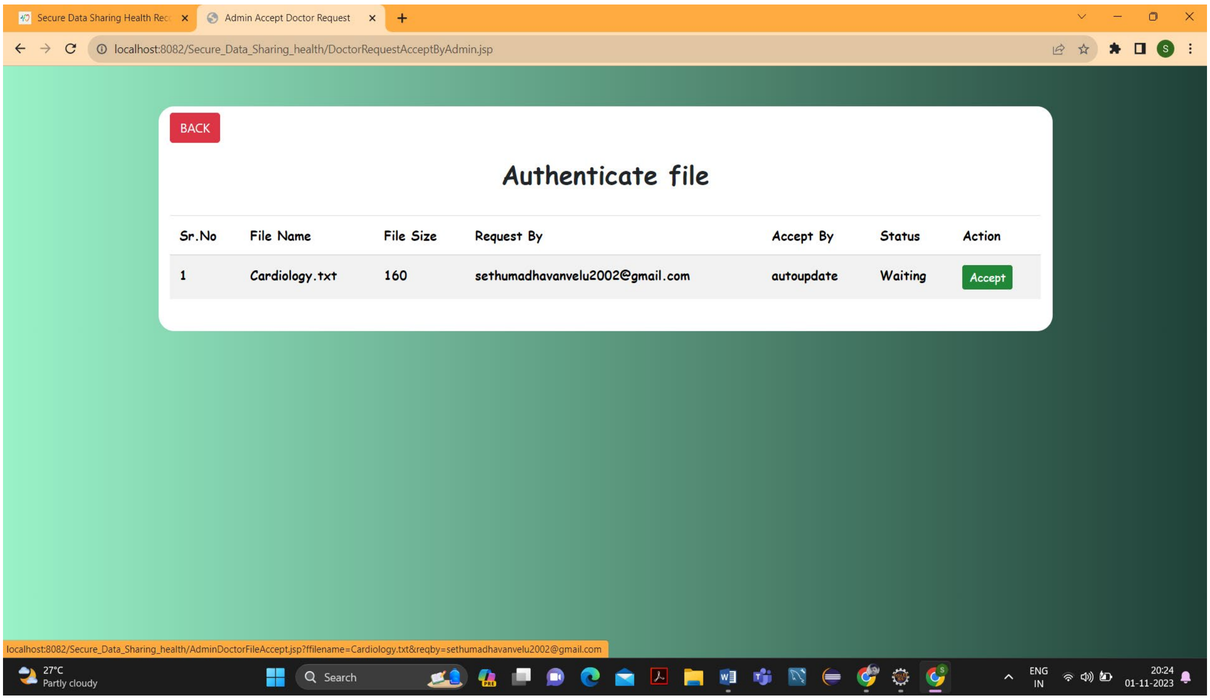
Admin Login Page:



Admin Home Page:



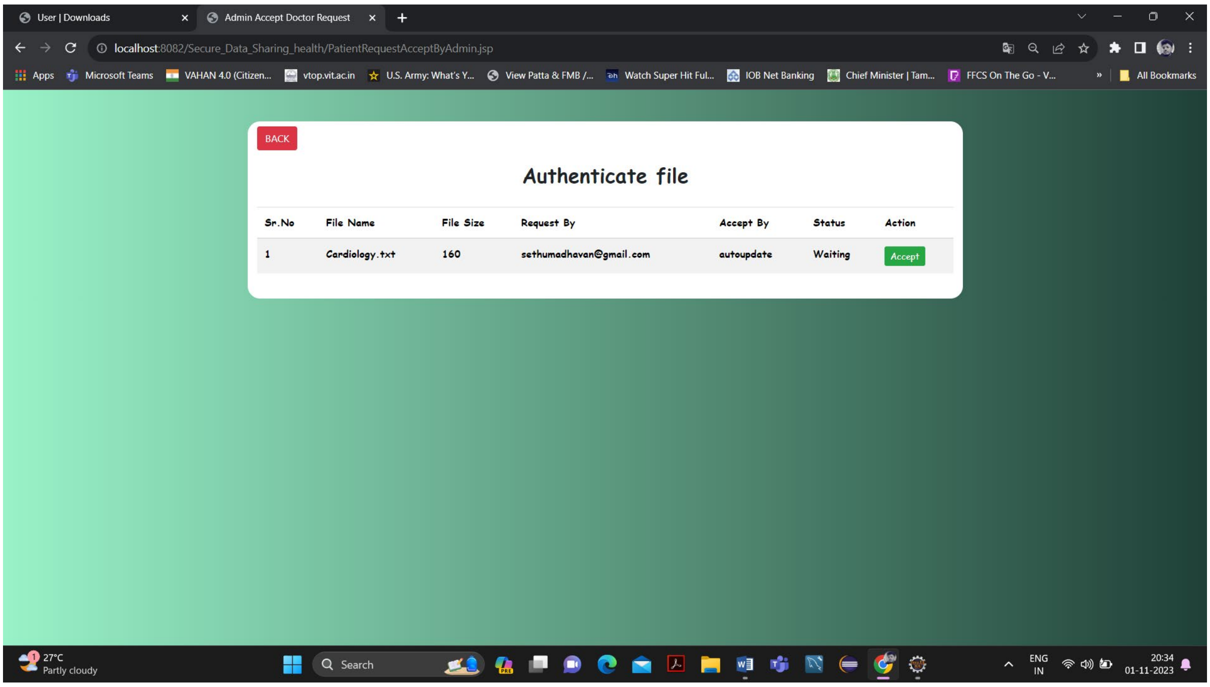
Authenticate Doctor:


Secure Data Sharing Health Rec
Admin Accept Doctor Request
localhost:8082/Secure_Data_Sharing_health/DoctorRequestAcceptByAdmin.jsp
BACK
localhost:8082/Secure_Data_Sharing_health/AdminDoctorFileAccept.jsp?filename=Cardiology.txt&reqby=sethumadhavanvelu2002@gmail.com
27°C
Partly cloudy
Search
ENG
IN
20:24
01-11-2023

Authenticate file

Sr.No	File Name	File Size	Request By	Accept By	Status	Action
1	Cardiology.txt	160	sethumadhavanvelu2002@gmail.com	autoupdate	Waiting	Accept

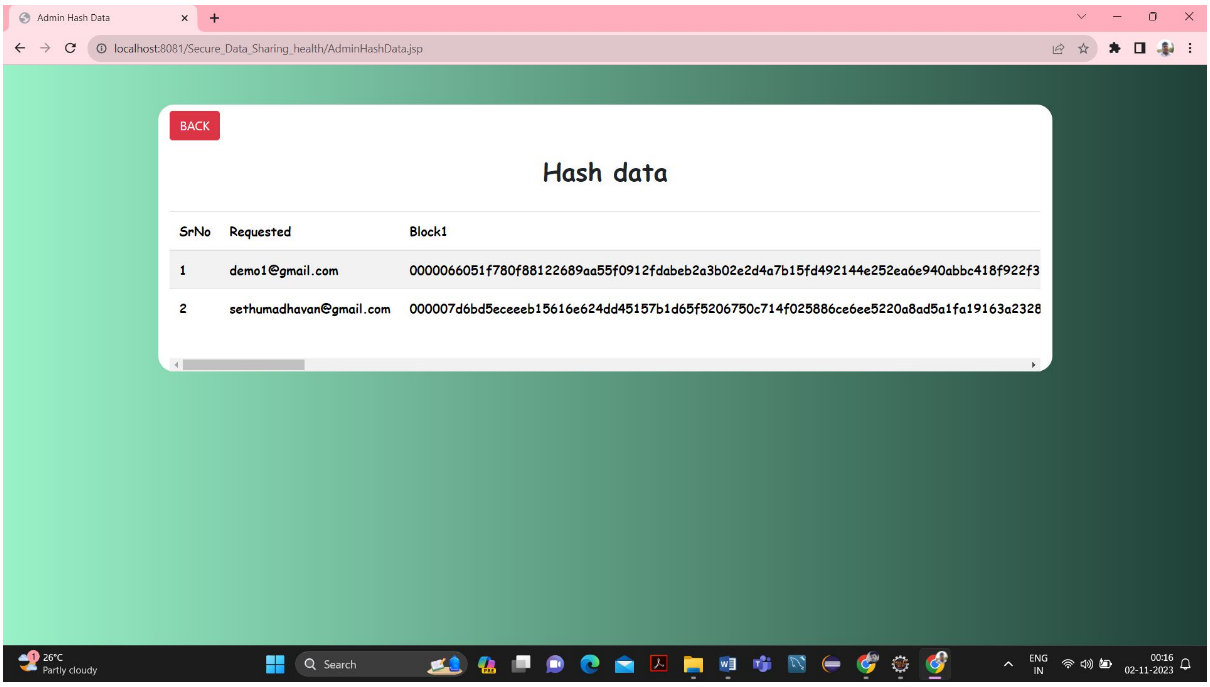
Authenticate Patient:



Authenticate file

Sr.No	File Name	File Size	Request By	Accept By	Status	Action
1	Cardiology.txt	160	sethumadhavan@gmail.com	autoupdate	Waiting	Accept

Hash Data:



Admin Hash Data

localhost:8081/Secure_Data_Sharing_health/AdminHashData.jsp

BACK

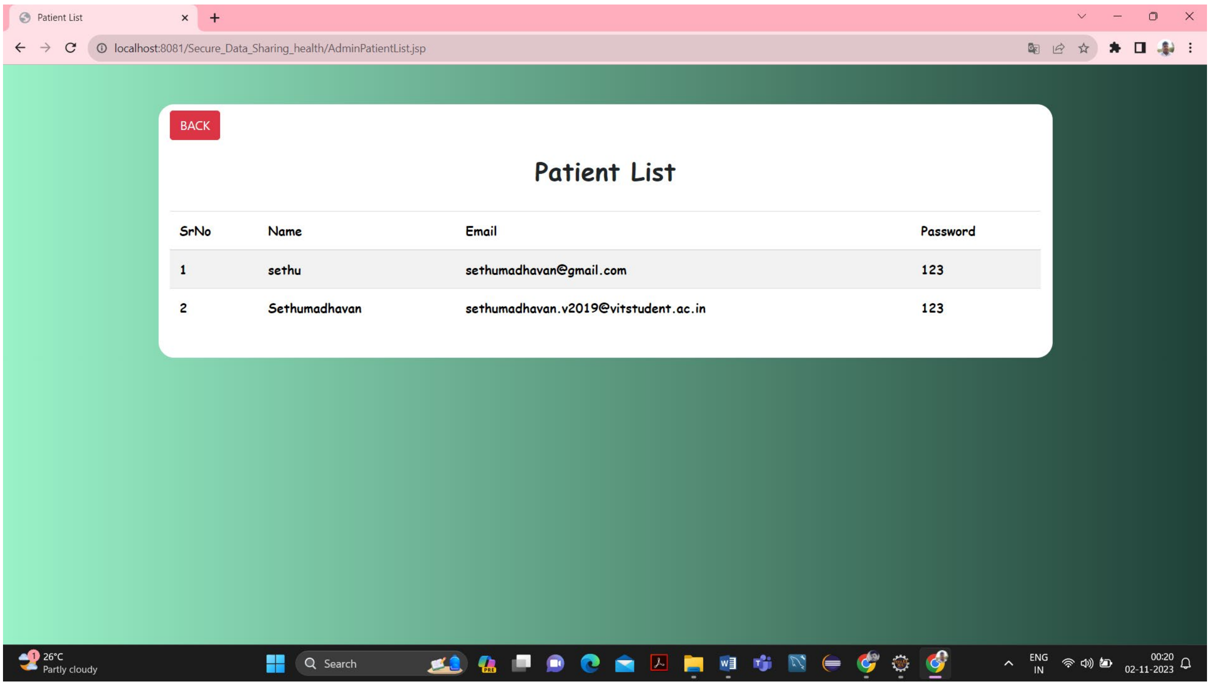
Hash data

SrNo	Requested	Block1
1	demo1@gmail.com	0000066051f780f88122689aa55f0912fdabeb2a3b02e2d4a7b15fd492144e252ea6e940abbc418f922f3
2	sethumadhavan@gmail.com	000007d6bd5eceeeb15616e624dd45157b1d65f5206750c714f025886ce6ee5220a8ad5a1fa19163a2328

26°C
Partly cloudy

00:16
02-11-2023

Patient List:



Patient List

localhost:8081/Secure_Data_Sharing_health/AdminPatientList.jsp

BACK

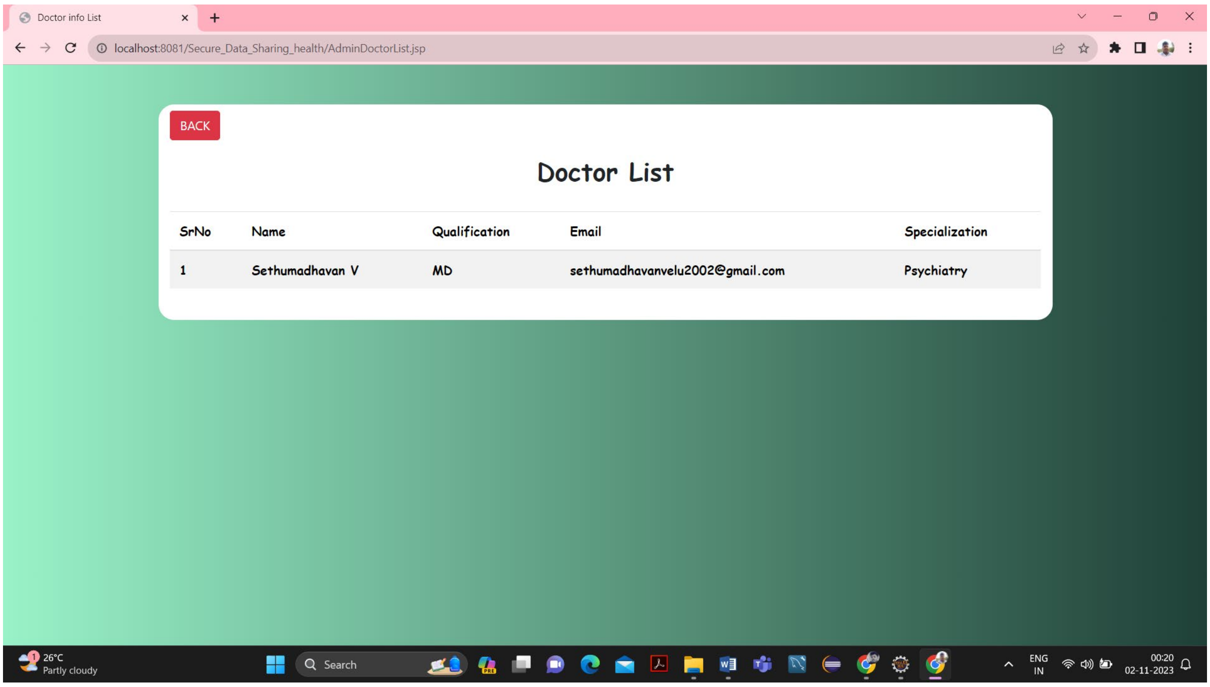
Patient List

SrNo	Name	Email	Password
1	sethu	sethumadhavan@gmail.com	123
2	Sethumadhavan	sethumadhavan.v2019@vitstudent.ac.in	123

26°C
Partly cloudy

00:20
02-11-2023

Doctor List:



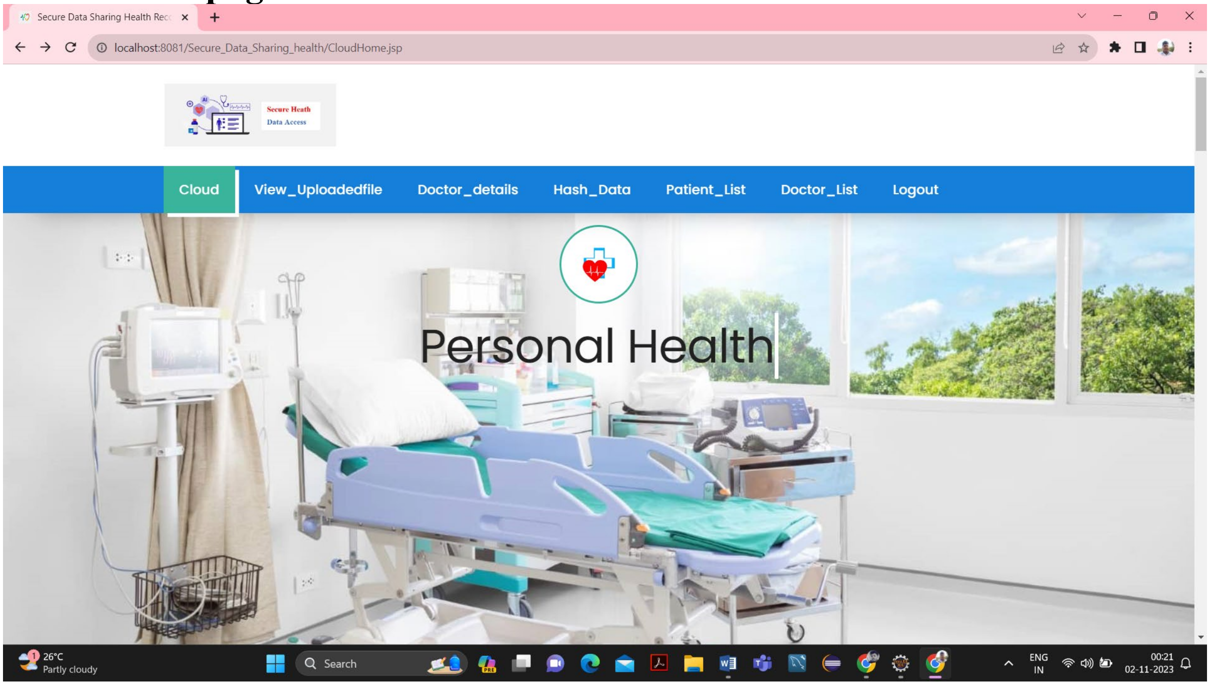
Doctor info List
localhost:8081/Secure_Data_Sharing_health/AdminDoctorList.jsp
BACK

Doctor List

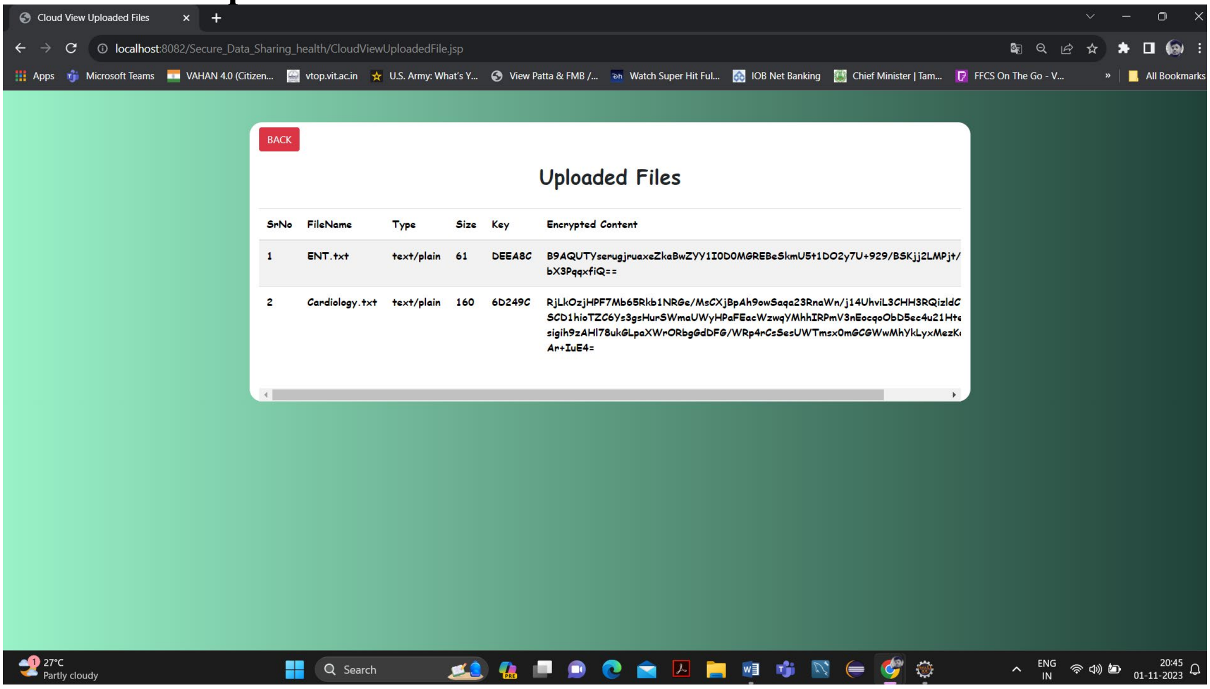
SrNo	Name	Qualification	Email	Specialization
1	Sethumadhavan V	MD	sethumadhavanvelu2002@gmail.com	Psychiatry

5.2.4. Cloud Modules:

Cloud Homepage:



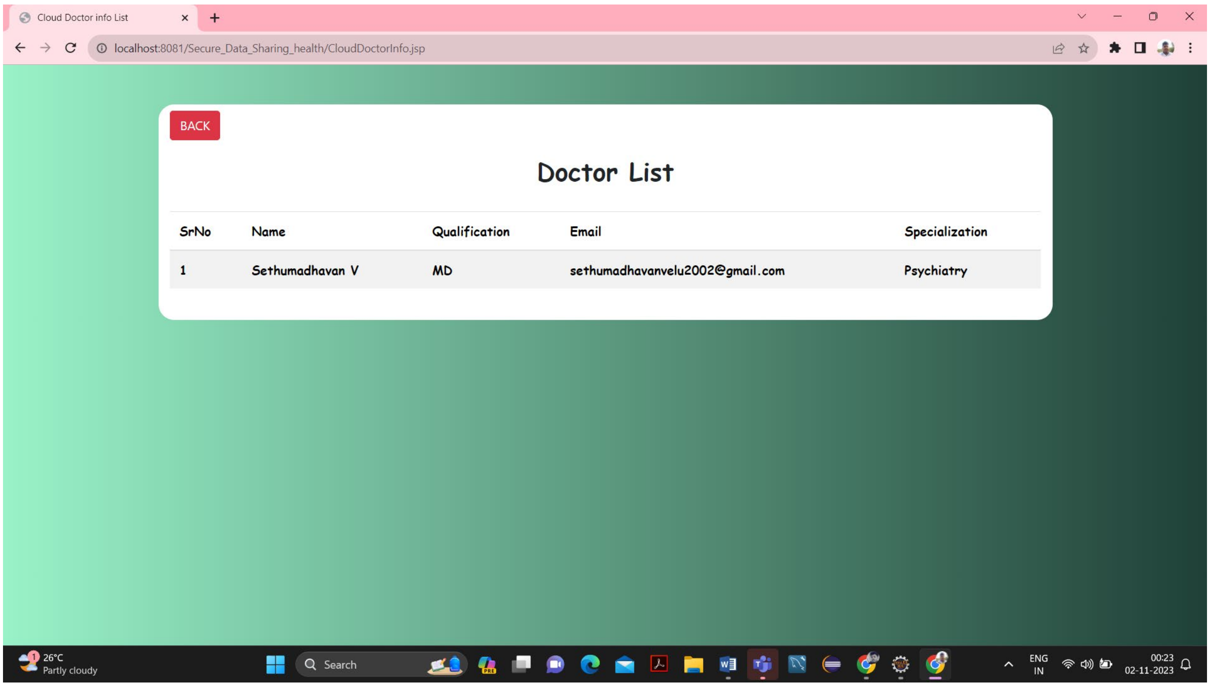
Cloud View Uploaded File


Cloud View Uploaded Files
localhost:8082/Secure_Data_Sharing_health/CloudViewUploadedFile.jsp
BACK

Uploaded Files

SrNo	FileName	Type	Size	Key	Encrypted Content
1	ENT.txt	text/plain	61	DEEA8C	B9AQUTYserugjruaxeZkaBwZYY1I0D0MGREBeSkmU5t1DO2y7U+929/BSKjj2LMPjt/ bX3PqqxfiQ==
2	Cardiology.txt	text/plain	160	6D249C	RjLkOzjHPF7Mb65Rkb1NRGe/MsCXjBpAh9owSaqa23RnaWn/j14UhviL3CHH3RQizldC SCD1hioTZC6Ys3gsHurSWmaUWyHPaFEacWzwqYMhhIRPmV3nEocqoObD5ec4u21Hte sigih9zAHl78ukGLpaXWrORbgGdDFG/WRp4rCsSesUWTmsx0mGCGWwMhYkLyxMezK Ar+IuE4=

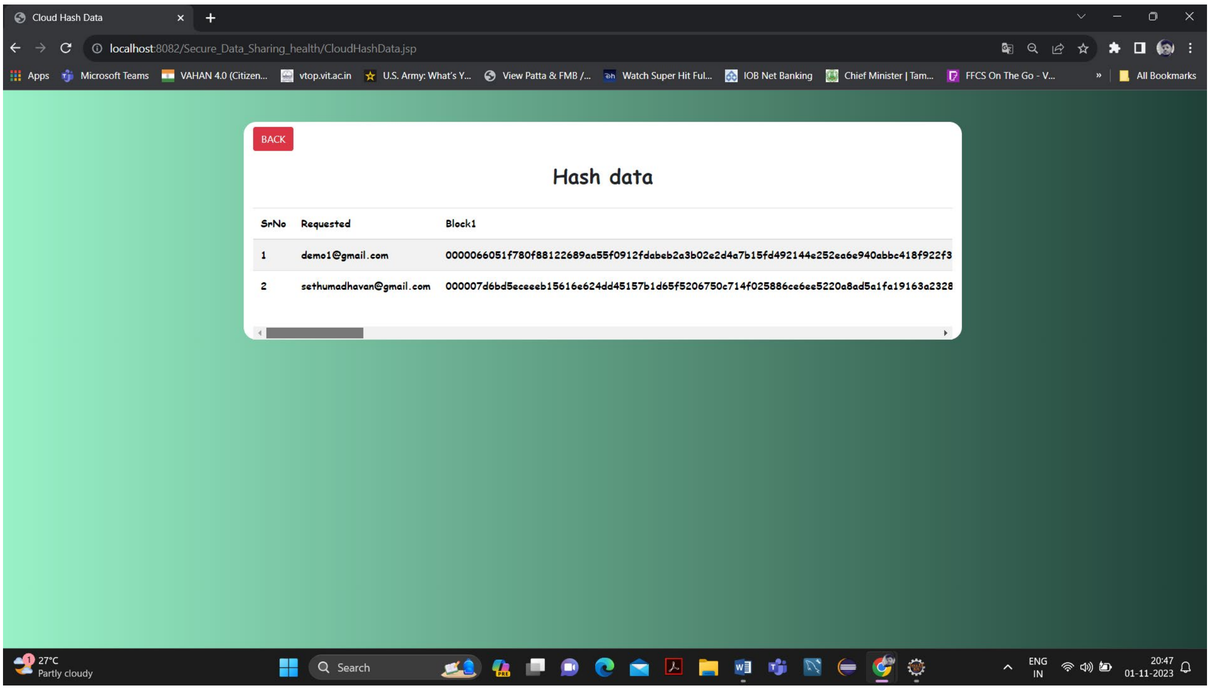
Doctor Information:


Cloud Doctor info List
localhost:8081/Secure_Data_Sharing_health/CloudDoctorInfo.jsp
BACK

Doctor List

SrNo	Name	Qualification	Email	Specialization
1	Sethumadhavan V	MD	sethumadhavanvelu2002@gmail.com	Psychiatry

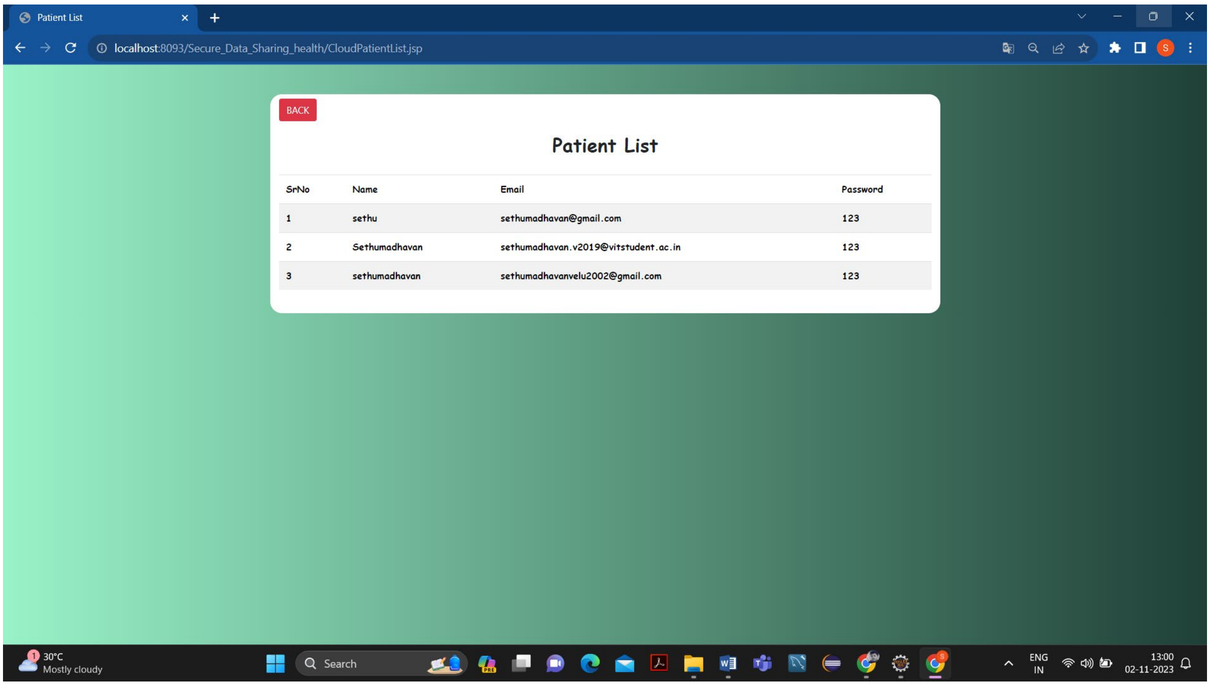
Hash Data:



Hash data

SrNo	Requested	Block1
1	demo1@gmail.com	0000066051f780f88122689aa55f0912fdabeb2a3b02e2d4a7b15fd492144e252ea6e940abbc418f922f3
2	sethumadhavan@gmail.com	000007d6bd5eceeeb15616e624dd45157b1d65f5206750c714f025886ce6ee5220a8ad5a1fa19163a2328

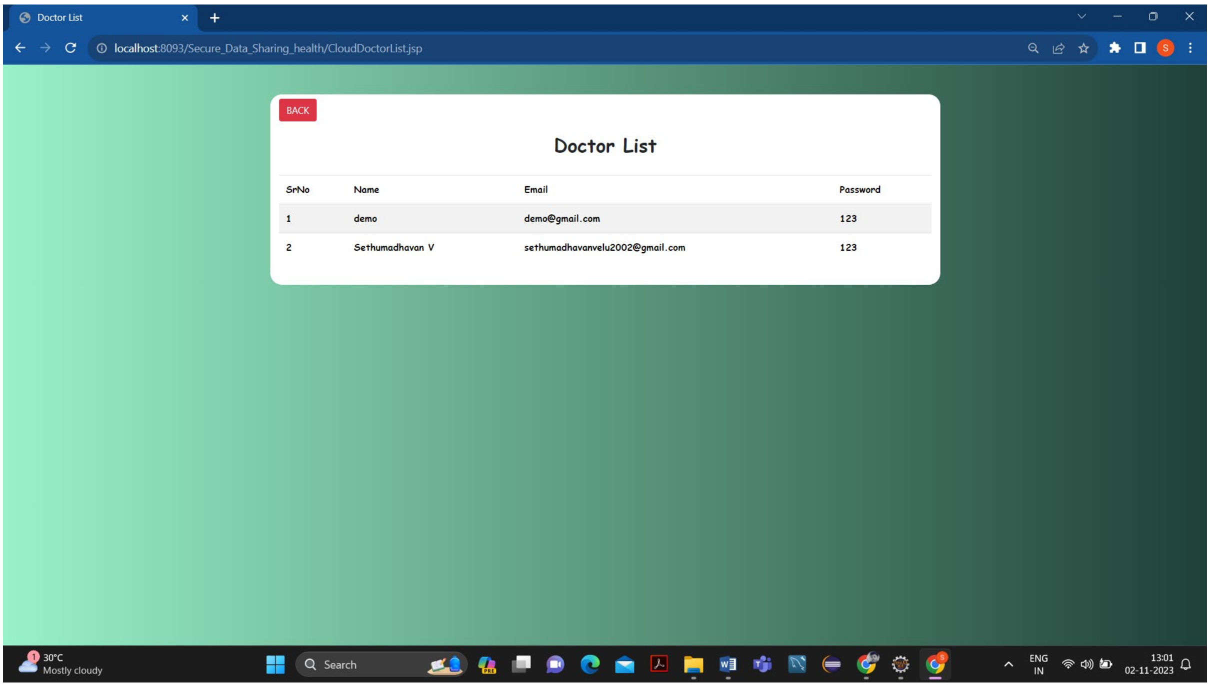
Patient List:


Patient List
localhost:8093/Secure_Data_Sharing_health/CloudPatientList.jsp
BACK

Patient List

SrNo	Name	Email	Password
1	sethu	sethumadhavan@gmail.com	123
2	Sethumadhavan	sethumadhavan.v2019@vitstudent.ac.in	123
3	sethumadhavan	sethumadhavanvelu2002@gmail.com	123

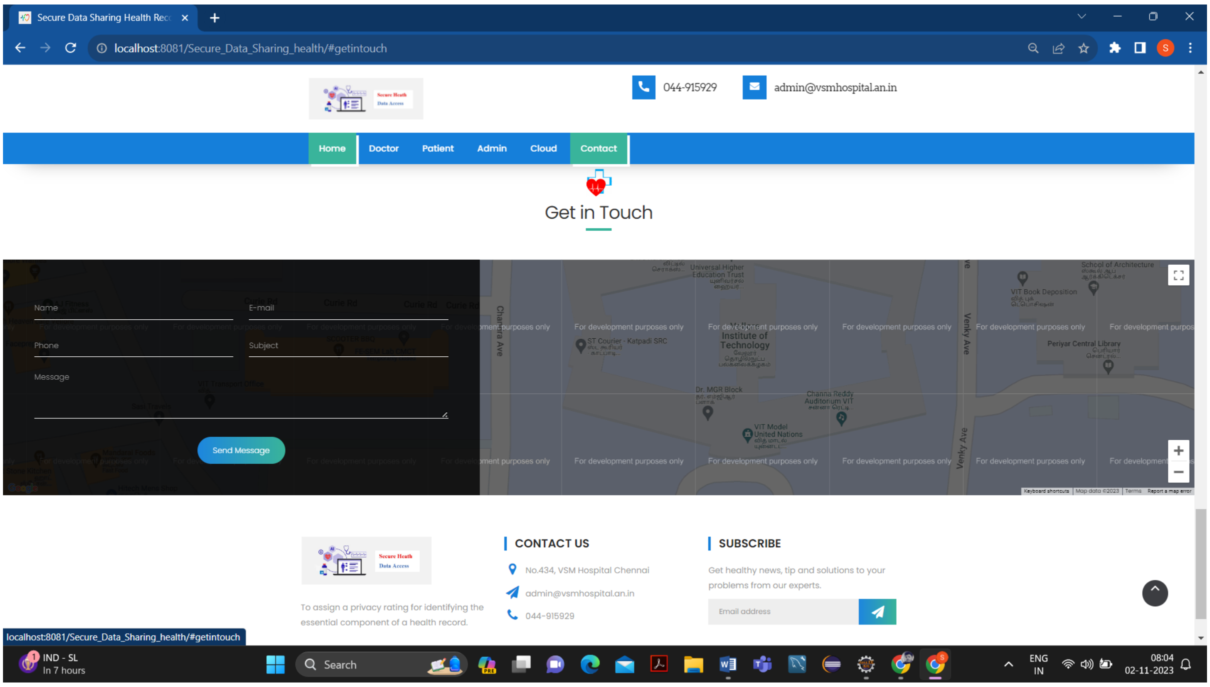
Doctor List:


Doctor List
localhost:8093/Secure_Data_Sharing_health/CloudDoctorList.jsp
BACK
30°C
Mostly cloudy
Search
ENG
IN
13:01
02-11-2023

Doctor List

SrNo	Name	Email	Password
1	demo	demo@gmail.com	123
2	Sethumadhavan V	sethumadhavanvelu2002@gmail.com	123

Contact Us Home page:



044-915929 admin@vsmhospital.an.in

Get in Touch

To assign a privacy rating for identifying the essential component of a health record.

CONTACT US

No.434, VSM Hospital Chennai
admin@vsmhospital.an.in
044-915929

SUBSCRIBE

Get healthy news, tip and solutions to your problems from our experts.

CONCLUSION:

Overall, the research work's method offers a design that makes it possible to create a secure framework for controlling public health employing cloud computing to record. Such advanced healthcare systems would undoubtedly assist patients in terms of security and strengthen our country's ability to manage the infrastructure of the healthcare sector. This part includes a reliable mechanism for managing community keys that will improve the security of identity-based encryption. Additionally, to guarantee that this research work offers a suitable key protection, encryption & decryption, and authentication procedure.

FUTURE ENHANCEMENTS:

In the future, we plan to research on applying the principles of AES algorithm using secure data sharing for improvising encryption performance.