IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Secure Data Sharing & Authorized Search In E – Health Using Cloud

[1]Mr.Arham Momin, [2]Mr.Sahil Chouhan, [3]Mr.Faraz Shaikh, [4]prof.Sneha Sankhe
[1 2 3]UG student, [4]Assistant Professor
[1 2 3 4]Department of Information Technology,
[1 2 3 4]Theem college of engineering, Boisar, India

Abstract: In the e-healthcare system, patients can gain an increasing number of high-quality medical services by sharing encrypted personal healthcare records (PHRs) with doctors or medical research institutions. However, a critical issue is that the encrypted PHRs result in loss of data content effectiveness by preventing an effective search for information. Another issue is that the medical treatment process requires the doctor to remain online at all times, which may be infeasible for all doctors (e.g., off duty under certain emergencies). Through our scheme, (1) the patients' healthcare records collected by the devices are encrypted before uploading to the cloud; the encryption only allows the medical service provider to search over the collected patient data, (2) the proxy re-encryption (PRE) technology allows for the secure re-encryption of the collected PHRs from the medical service provider to any independent third-party research institutions, and (3) we combine the secret splitting technique and the channel codes for designing a privacy-preserving technique to guarantee that the remote PHRs monitoring process can be correctly continued, even if the medical service provider terminates service or drops offline during the remote PHRs monitoring process. We show that it is provably secure and preserves privacy of the PHR contents under the one-more-DMHE assumption, and provide experimental results to demonstrate the effectiveness and its performance.

***Keywords* – Proxy re-encryption, proxy invisibility, Searchable encryption, mobile healthcare sensor networks.**

I. INTRODUCTION

These days, with the quick advancement of counterfeit insights and the progression of wearable gadgets and sensors, E - healthcare sensor organize has come to a arrange of development for appropriation and arrangement at a commercial scale. E - healthcare sensor organize serving as a versatile stage significantly advantage patients to get restorative treatment of tall quality and productivity. As appeared in Fig.1, patients' gadgets collect a huge sum of individual healthcare records through sensor gadgets, which empower specialists to more successfully analyze and go to the require of the patients through utilizing this information. Such data too empowers restorative analysts and investigators to perform analytics to pick up way better experiences on ailments and plan way better medications. All things considered; this information may be put away on cloud capacity given by third-party benefit suppliers which present potential security issues such as information spillage.

Usually since not one or the other the patients is the specialists have control of the data once the information is outsourced. This implies the security and secrecy of these outsourced information ought to be secured in such an environment. For occurrence, a few therapeutic teach collect and store expensive sum of PHRs on cloud servers and authorize the utilization of these information to the Center for Malady Control and Avoidance (CDC). To encourage malady avoidance and control, specialists in CDC are permitted to consider these data with information mining innovation. Be that as it may, within the handle of collecting case data from restorative educate and the execution of conventional information mining innovation, the CDC may unavoidably uncover touchy information of patients. How to store manage and retrieve the PHRs securely and efficiently may be challenge. E-healthcare system requires stronger security and privacy guarantees for practices in terms of both data and access to data. In order to prevent information leakage from the stored PHRs, all PHRs stored on the cloud should be encrypted.

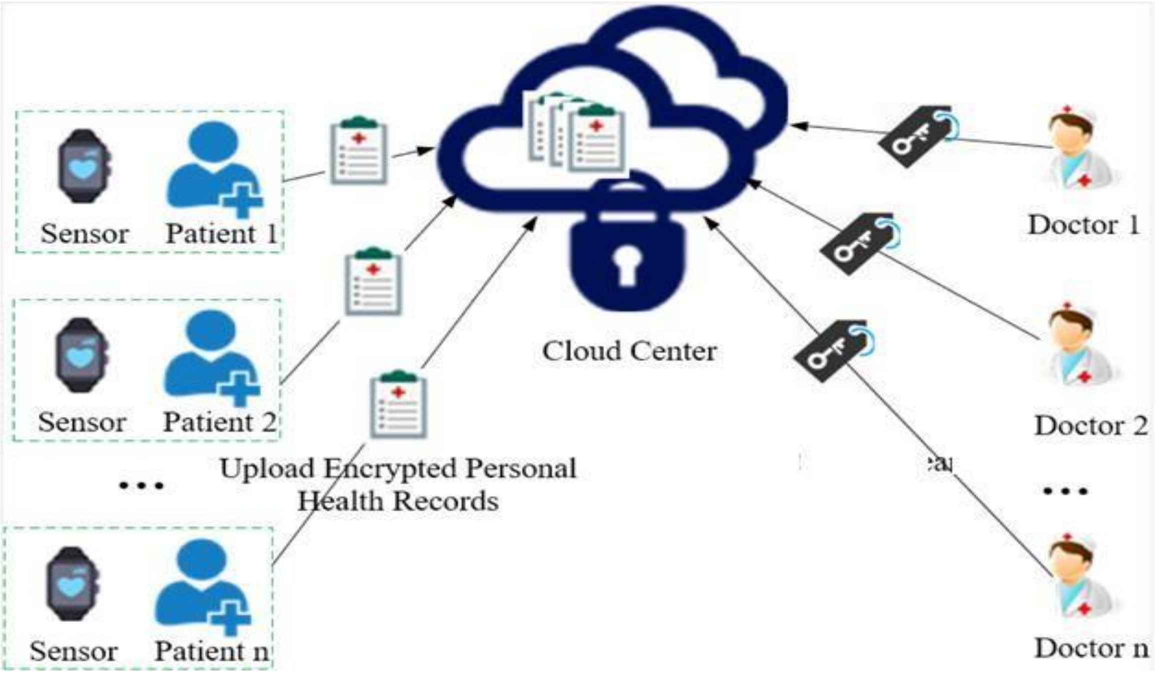
II. LITERATURE SURVEY

A efficient writing survey may be a of assessing and translating all accessible inquire about important to a specific inquire about address, point or wonder of intrigued. The logical databases with full content paper, and the other accessible logical articles within the field of social sciences were utilized within the inquire about. All logical and other papers and works written within the time span from 2009 to Walk 2020 are taken into consideration within the comes about selection.

Sr no.	Paper Title (Reference)	Author Name	Advantages	Disadvantage
[1]	A survey on Blockchain technology and its security.	MOHAMMAD MOUSSA MADINE, et al.	Initial implementation and setup costs can be high. There may be a learning curve for healthcare providers to use the system.	Initial implementation and setup costs can be high. There may be a learning curve for healthcare providers to use the system.
[2]	Blockchain Based identity verification model.	LINLIN XUE,et al.	patients' healthcare records collected by the devices are encrypted before uploading to the cloud server ensuring privacy and confidentiality of PHR.	Not suitable for a distributed environment and it is not scalable.
[3]	A Review of Secure and Privacy-Preserving Medical Data Sharing.	HAO JIN , YAN LUO.	privileges were mapped into various roles with ABE access structures	storage of health information is located in a centralized server
[4]	An Overview of Smart Contract: Architecture, Applications and Future Trends.	Guo et al.	Users are permitted to access based on their privileges without disclosing their attributes and identities.	There is no room for collaborative sharing of medical data across different domains. It lacks interoperability.
[5]	A Blockchain-Based Identity Verification Mechanism.	T. Bhatia, A. K.Verma, and G. Sharma	The ubiquitous and timely access to personal health records help physicians to take critical decisions and save lives.	A lightweight and pairing free single-hop unidirectional certificateless proxy.

III. SYSTEM ARCHITECTURE

The patient details are also shown on the main page; for instance, if a patient is sent from Hospital A to Hospital B for treatment, Hospital B can review the patient’s past records. The CSV file is matched with the patients' CS Vid. If a corresponding id is found, the specifics are presented in a row. A secure data sharing and authorized search for E-healthcare systems using cloud computing typically comprises several key components to ensure robust security and efficient data management. At the core of the architecture lies a secure cloud infrastructure, providing the foundation for storing and processing healthcare data. This infrastructure is fortified with encryption mechanisms to safeguard data both in transit and at rest. Access control mechanisms, such as role- based access control (RBAC) or attribute-based access control (ABAC), are implemented to enforce granular permissions, ensuring that only authorized users can access sensitive information. Authentication mechanisms, including multi-factor authentication (MFA) and biometric authentication, verify the identity of users before granting access to the system. A dedicated secure communication layer facilitates encrypted communication between different system components and users. Additionally, a comprehensive audit trail mechanism records all interactions with the system, enabling accountability and traceability of data access and modifications.



3.1 Requirement Analysis

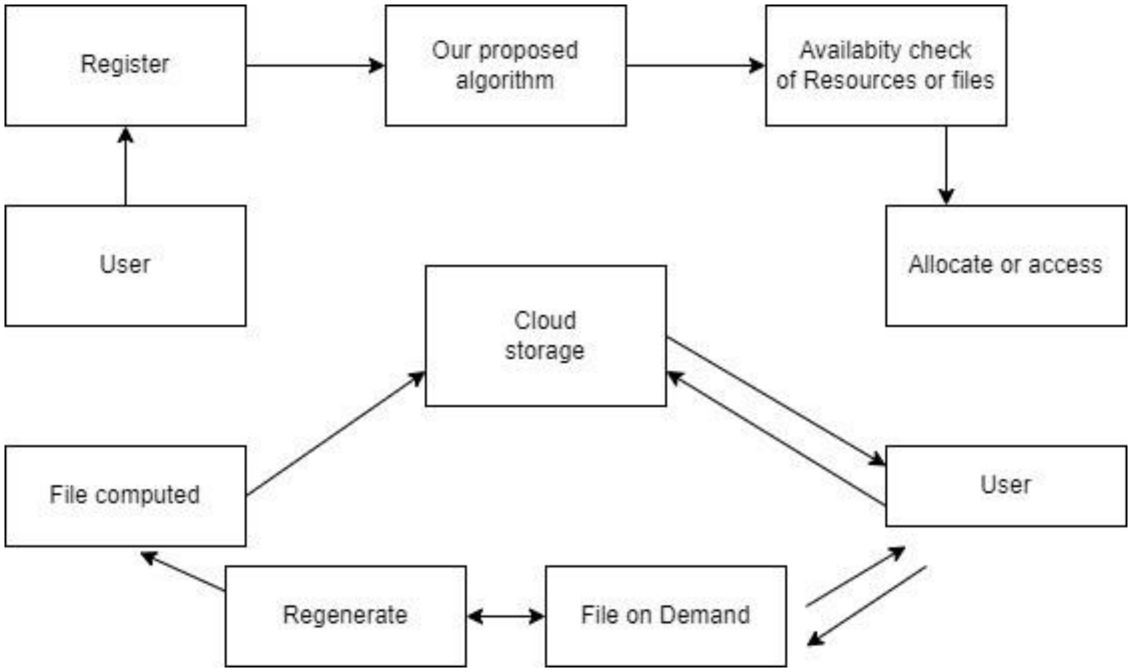
For any program venture there are distinctive sorts of necessities to be satisfied in arrange to guarantee smooth running of the forms. Clearly characterized necessities are vital markers on the street to effective extend. They set up a formal assertions between the client and the benefit supplier that both are working towards the same objective. The taking after are the distinctive sorts of necessity for our extend.

Software Requirements	Hardware Requirements
Chrome	Windows 11 or latest version
Java	8 GB RAM
VS Code	Intel core processor i3
Ethereum MetaMask	Wi-Fi Router

3.2 PROPOSED SYSTEM

We propose a proxy-invisible condition-hiding proxy re-encryption scheme with keyword search to address the issues of inefficiency and condition privacy in the e-healthcare system. Encrypting is considered to be a simple and efficient solution to guarantee data confidentiality, but it also makes search over encrypted data extremely difficult. Searchable encryption technology realizes the search operation of encrypted data without decryption, and solves the problem that users cannot control remotely because of data encryption. Hence, searchable is necessary in the e-healthcare system.

In this proposed system, we aim to design an efficient, searchable and privacy preserving e-healthcare system. Framework plan is the method of arranging framework components such as design, modules and components, the different interfacing of these components, and the information passing through the framework. The objective of the system design handle is to supply adequate gritty data and information. data almost the framework and its framework components so that the implementation is consistent with the structural units characterized within the models and sees of the framework engineering.



IV. PROBLEM DEFINITION

The purpose of this project is to provide the correct data with security to the users. For some of the users the data might be lost during the transmission process in the network and for some, the data might be changed by the unauthorized person in the network and there are some other security problems in the network. Our application will give you more Security to the data present in the network and there will be able to reduce the loss of data in the network which will be transmitted from the sender to the receiver using the latest technologies.

V. RESULT

It comprises the creating detail and methods for information arrangement and those steps are vital to put exchange information in to a usable frame for handling can be accomplished by assessing the computer to studied information from a composed or printed report or it can happen by having individuals keying the information straightforwardly into the framework. The plan of input centers on controlling the sum of input required, controlling the mistakes, dodging delay, maintaining a strategic distance from additional steps and keeping the method straightforward. The input is outlined in such a way so that it gives security and ease of utilize with holding the security. It is accomplished by making user-friendly screens for the information section to handle expansive volume of information. The objective of designing input is to form information section less demanding and to be free from blunders. The information passage screen is planned in such a way that all the information control can be performed. It moreover provides record seeing offices. When the information is entered it'll check for its legitimacy.

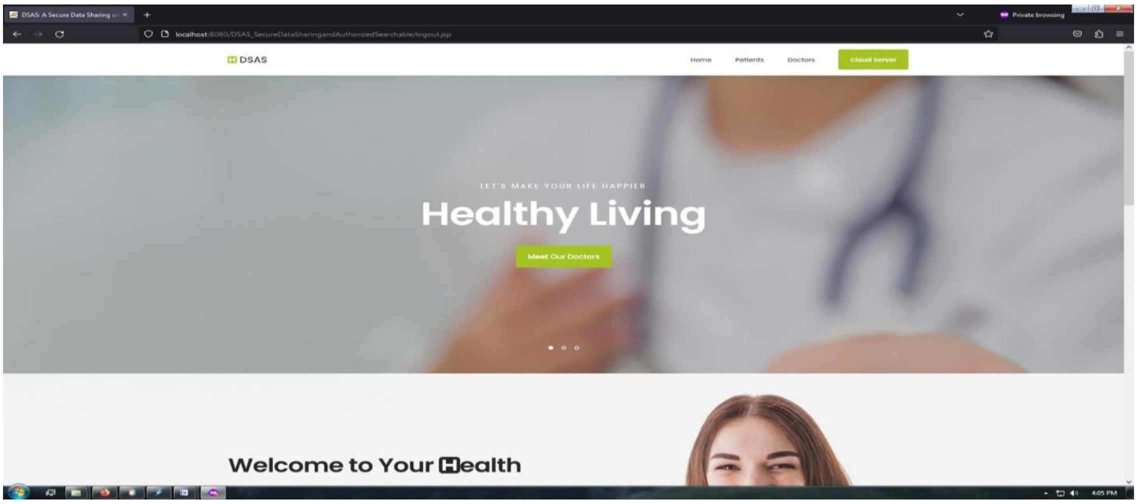

DSAS: A Secure Data Sharing a
Private browsing
localhost:8080/DSAS_SecureDataSharingandAuthorizedSearchable/logout.jsp
DSAS
Home
Patients
Doctors
Cloud Server
LET'S MAKE YOUR LIFE HAPPIER
Healthy Living
Meet Our Doctors
Welcome to Your Health
4:05 PM

Fig1: Homepage for user interface

This is a homepage of the system where three administration tabs can be seen like Patients, Doctors & Cloud Server. There is a slider of images that give user-friendly interactions. And if scroll to the end of page you will find contact numbers, emails & address. It has a minimal design so that user won't have any difficulties to access any features of it. We invite healthcare institutions and professionals to join our mission to revolutionize healthcare delivery. By partnering with us, you can be at the forefront of a more efficient, secure, and patient-centric healthcare system.

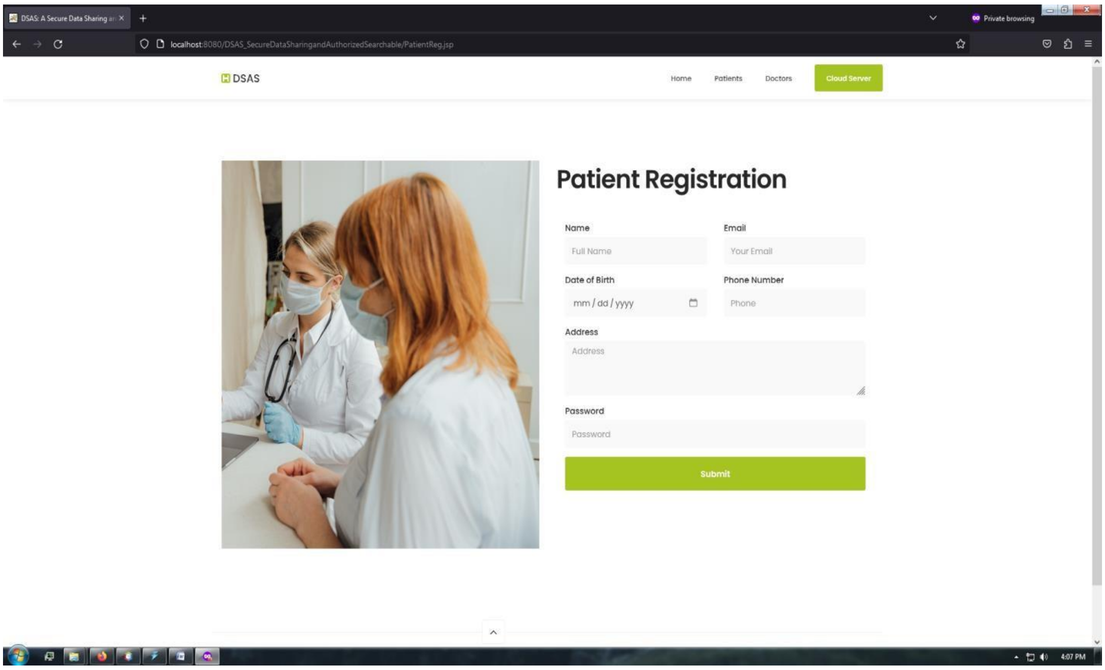
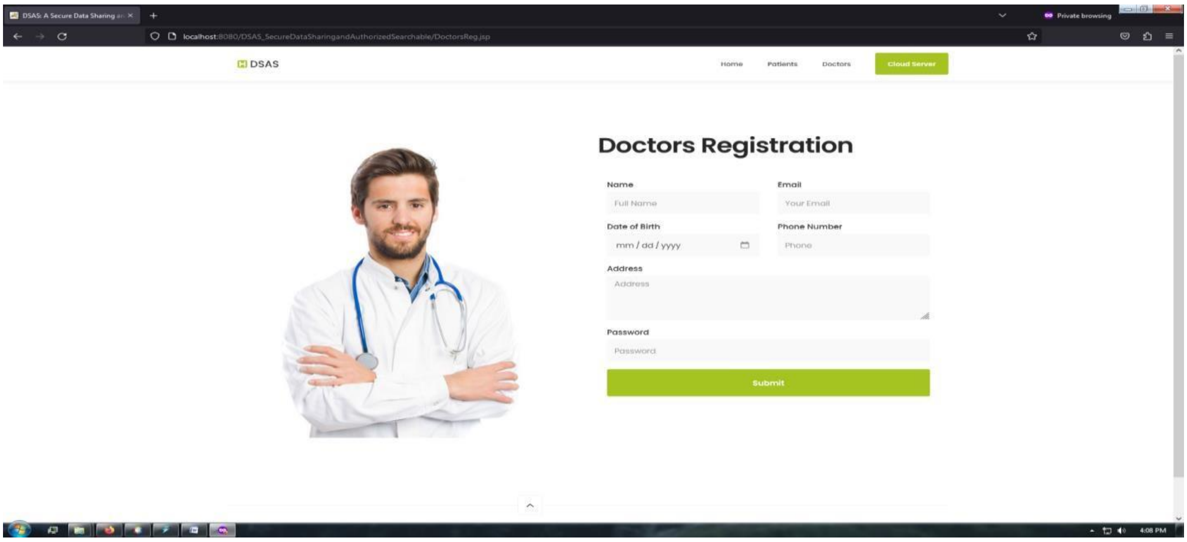


Fig2: Patient Registration Form

The key elements and features of the patient registration page, with a particular focus on data security and authorization in an e-healthcare system using cloud technology. It ensures a smooth and secure registration process for patients while emphasizing the project's commitment to privacy and security. Our registration page is designed to be responsive, ensuring an optimal experience on various devices, including smartphones, tablets, and desktop computers.


DSAS: A Secure Data Sharing an
Private browsing
localhost:8080/DSAS_SecureDataSharingandAuthorizedSearchable/DoctorsReg.jsp
DSAS
Home
Patients
Doctors
Cloud Server

Doctors Registration

Name: Full Name

Email: Your Email

Date of Birth: mm / dd / yyyy

Phone Number: Phone

Address: Address

Password: Password

Fig3: Doctor Registration

This description provides a clear overview of the doctor registration page, highlighting the importance of data security and authorization in an e-healthcare system using cloud technology. The doctor can fill their details in this registration form & can register themselves on the system. Once they register the admin can view their form and check on it and then the request of account will get approved. Once the request is approved the doctor can login and check the data of the patients that has been assigned to them.

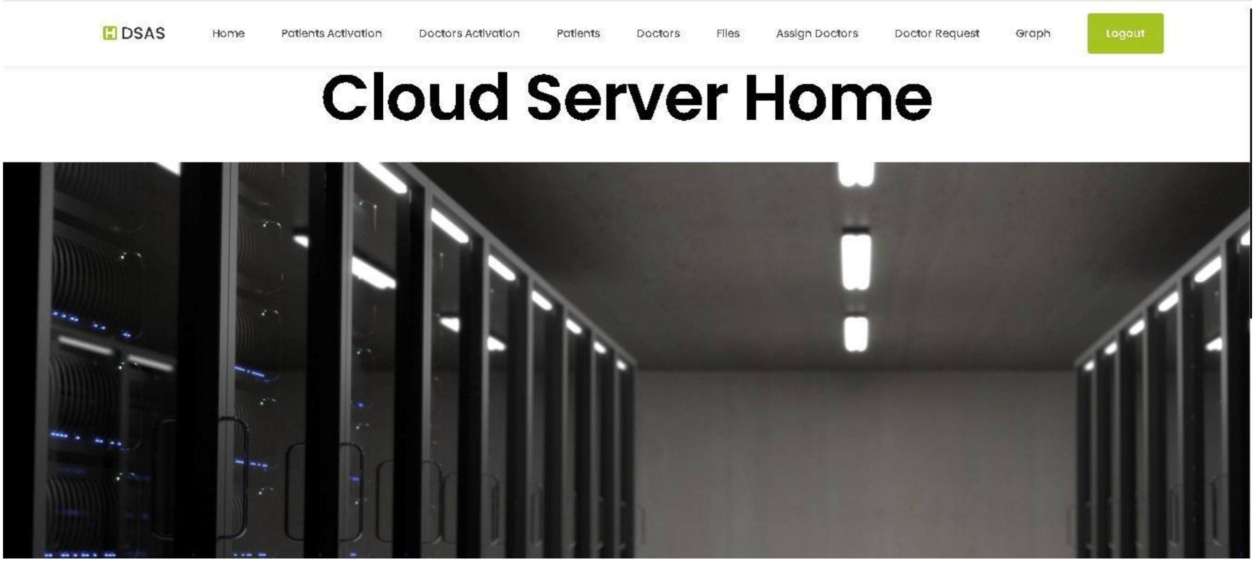
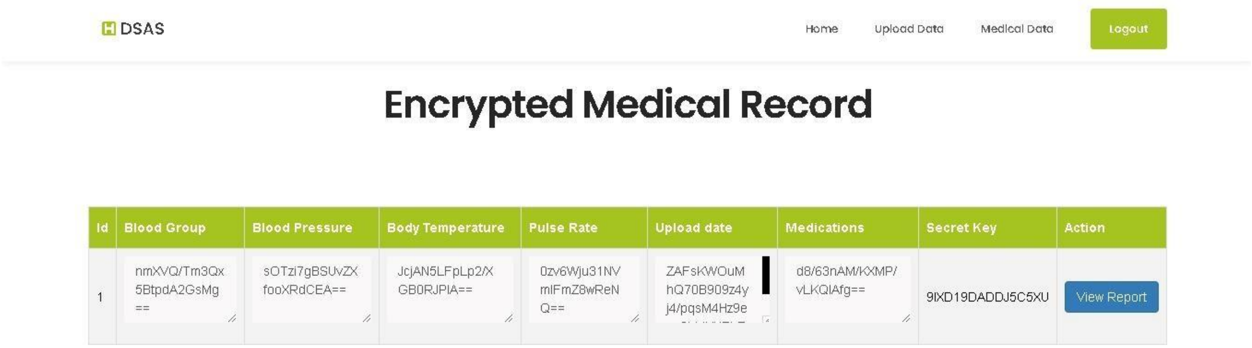


Fig4: Cloud server

This description provides a clear overview of the Cloud Server page, highlighting the importance of data security and authorization in an e-healthcare system of cloud technology. It shows tabs of Patient Activation, Doctors Activation, Patients, Doctors, Files, Assign Doctors, Doctor Request & Graph. All the authority of providing access to data is controlled by Cloud Server.

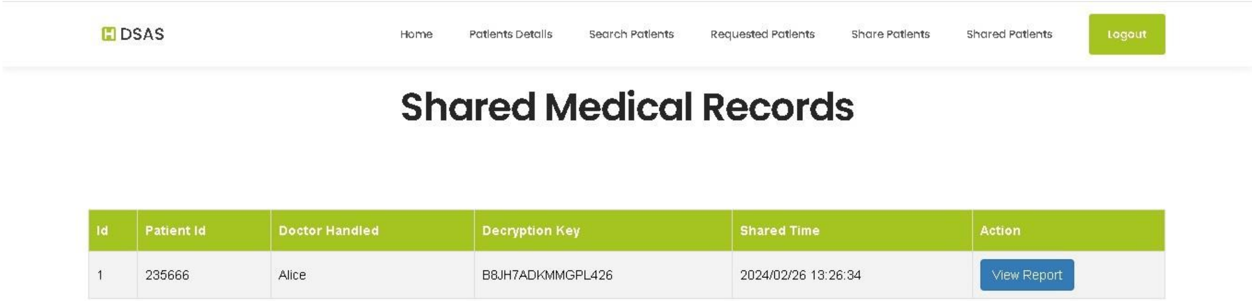


Encrypted Medical Record

Id	Blood Group	Blood Pressure	Body Temperature	Pulse Rate	Upload date	Medications	Secret Key	Action
1	nmXVQ/Tm3Qx 5BtpdA2GsMg ==	sOTzi7gBSUvZX fooXRdCEA==	JcjAN5LFpLp2/X GB0RJPIA==	0zv6Wju31NV mIFmZ8wReN Q==	ZAFsKWOuM hQ70B909z4y j4/pqsM4Hz9e	d8/63nAM/KXMP/ vLKQIAfg==	9IXD19DADDJ5C5XU	View Report

Figure5: Screenshot of Encryption of Medical Data

Here when the doctor is assigned to the patient that doctor can only get the encrypted key and by using that the doctor can view & edit the data of the assigned patient.



Shared Medical Records

Id	Patient Id	Doctor Handled	Decryption Key	Shared Time	Action
1	235666	Alice	B8JH7ADKMMGPL426	2024/02/26 13:26:34	View Report

Figure6: Decryption of Medical Data

When the doctor shares patient's data to another doctor then the other doctor can use the decrypted key and can access the data. The other doctor can only view the data it can't be edited other than the assigned doctor.

VI. CONCLUSION

A Presented a proxy-invisible condition-hiding proxy re-encryption scheme which supports keyword search that can be applied to securing data sharing and delegation in e-healthcare systems. With our new system, a doctor, Alice (delegator), may construct a conditional authorization for a doctor, Bob (delegate), by specifying a re-encryption key. With the re-encryption key, the cloud server can perform cipher text transformation so that Bob is able to access the PHRs original encrypted under Alice's public key, thus enabling secure delegation. The cloud server can operate search over encrypted PHRs on behalf of the doctor without learning information about the keyword or the underlying condition. Specifically, we achieved the property of proxy-invisible in the system. We have also obtained the property of collusion-resistance in the system, where a delegator's (Alice) private key is still secure even a dishonest cloud server colludes with the delegate (Bob). We have demonstrated security through a rigorous proof, and the performance analysis confirms that our proposed scheme DSAS is efficient and practical.

VII. FUTURE SCOPE

The current implementation of the system is suitable for small-scale deployments. Future work can focus on improving the scalability of the system to support large-scale e-healthcare systems with a high volume of patients and medical records. Although the system provides a high degree of privacy and security, there is still room for improvement. Future research can focus on developing more advanced privacy-preserving techniques to ensure that patient's personal healthcare records are protected even in the case of a breach or attack. Future work can focus on ensuring interoperability between different e-healthcare systems and enabling seamless sharing of encrypted PHRs between different providers. The system can be integrated with emerging technologies such as blockchain, AI, and IoT to enhance its functionality and security. For instance, blockchain can be used to create a decentralized, tamper-proof database for storing PHRs, while AI can be used for predictive analytics and personalized medicine. Finally, future work can focus on encouraging the adoption and implementation of the system in real-world e-healthcare systems. This can involve collaboration with healthcare providers, policymakers, and regulatory bodies to ensure that the system meets legal and ethical requirements and is compatible with existing healthcare systems.

REFERENCES

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone- Lee, G. Neven, P. Paillier, and

H. Shi, ``Searchable encryption revisited: Consistency properties, relation to anonymous IBE,

and extensions,&#39;&#39; in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2005, pp. 205222.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ``Improved proxy re- encryption schemes with

Applications to secure distributed storage,&#39;&#39; ACM Trans. Inf. Syst. Secur., vol. 9, no. 1, pp. 130, 2006.

[3] J. Baek, R. Safavi-Naini, and W. Susilo, ``Public key encryption with keyword search revisited,&#39;&#39; in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2008, pp. 12491259.

[4] T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing,&#39;&#39; Concurrency Comput., Pract. Exper., vol. 32, no. 5,
p. e5520, Mar. 2020.

[5] T. Bhatia, A. K.Verma, and G. Sharma, ``Secure sharing of mobile personal healthcare records using certicateless proxy re-encryption in cloud,&#39;&#39; Trans. Emerg. Telecommun. Technol., vol. 29, no. 6,
p. e3309, Jun. 2018.

[6] I. F. Blake, G. Seroussi, and N. Smart, ``Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series (317)), vol. 19. Cambridge, U.K.: Cambridge Univ. Press, no. 20, 2005, p. 666.

[7] M. Blaze, G. Bleumer, and M. Strauss, ``Divertible protocols and atomic proxy cryptography,&#39;&#39; in Advances in Cryptology-EUROCRYPT. Berlin, Germany: Springer, 1998, pp. 127144.