e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

PATIENT'S HEALTHCARE RECORDS DATA SHARE WITH PRIVACY IN A DATABASE

Ms. G. Sirisha[*1], Md Motibul Raeen[*2], Santosh Yadav[*3], Kaushal Babu Yadav[*4]

[*1]Assistant Professor, Department Of Computer Science & Engineering, Guru Nanak Institute Of Technology, Ibrahimpatnam, RR District, Telangana, India.

[*2,3,4]Student, Department Of Computer Science & Engineering, Guru Nanak Institute Of Technology, Ibrahimpatnam, RR District, Telangana, India.

DOI: https://www.doi.org/10.56726/IRJMETS64736

ABSTRACT

In the current digital era, personal data storage on public platform is a major cause of concern with severe security and privacy. This is true especially in e-health data management since patient's health data must be managed following a slew of established standards. The Cloud Service Providers (CSPs) essentially provide computing and storage resource. However, data security in the cloud is still a utmost concern. In several instances, Block chain technology rescue the CSPs by providing the robust security to the underlying data by encrypting data using the unique and secret keys. Each network user in Block chain has its own unique and secrets keys to protect the data. However, Block chain technology suffers in high workload scenarios.

To overcome e-healthcare records privacy issues in a third-party cloud, we designed a Patient's Healthcare Records Management System (PRMS) that focuses. A PRMS is compared to the Secure and Robust Health-Based Block Chain (SRHB) approach using a database.

Keywords: Hospital, Database, Cloud Service Providers, Block Chain, Robust Security, E-Healthcare, Patient's Healthcare Records Management System.

I. INTRODUCTION

In the current era of digital communications, data are preferred to be stored in the cloud data centers over the local systems. Data generated from state-of-the-art applications such as smart city, Internet of Medical Things (IoMT), E-healthcare are stored and process on the cloud platforms owned by Cloud Service Providers (CSPs). However, CSPs merely provide the storage, and data processing infrastructure and do not provide comprehensive data security framework. In several instances, CSPs integrate the third-party security framework for privacy preservation and data protection. However, third-party security frameworks are subjects to integration issues and expensive. On the contrary, Blockchain technology provides condense and transparency by delivering immutable blocks of chain. However, Blockchain enabled security has shortcomings while processing multiple transactions such as latency and throughput. In the proposed work, we have exclusively focused to improvise the latency and throughput during the multiple transactions scenarios arise during the access of E-healthcare Records (EHRs).

Electrons records can integrate information from many registered resources and provide a more comprehensive picture of exact patient details, even though this has proven to be a challenging task [1]. Healthcare data is at great risk due to the cloud, despite all of its advantages over on-premises storage. The healthcare sector is undergoing a change as paper-based records are being phased out and replaced by computerized ones [2]. Personal Health Records (PHR), Electronic Health Records (HER), Electronic Medical Records (EMR), and Electronic Health Data (EHD) are examples of digitalized electronic medical records that have evolved from paper-based records. HER and EMR refer to patient health records maintained by healthcare professionals, where PHR refers to regularly maintaining and monitoring personal information by the patient or their relatives. EHD, also known as electronic health records or computerized patient records, is a type of smart health records that is delivered to patients [3]. Medication, medical histories, demographics, immunization records, laboratory test results, and other confidential patient information are all contained in these records. Traditional paper-based records have considerable disadvantages when compared to EHD systems. Compared to paper-based records, EHR involves fewer human resources, time, and physical storage [4]. Due to data centralization on the cloud, consumers and healthcare providers have several security and privacy issues. (1) provides and all-in-one honeypot for attackers to steal information and exploit transmitted data, and (2) transfers ownership rights to cloud service providers, allowing individuals and healthcare professionals to lose control of confidential data [5]. Furthermore, the current tendency is to use a cloud environment to share and manage massive amounts of distributed medical data, including EHR and lab test results, throughout the e-health system. Cloud storage services offer a viable and scalable solutions to such massive data management challenges.

II. LITERATURE SURVEY

1. TITLE: MUVINE: Multi-stage virtual network embedding in cloud data centers using reinforcement learning-based predictions.

AUTHOR: H. K. Thakkar, C. K. Demur, and P. K. Sahoo

YEAR: 2021

DESCRIPTION: The recent advances in virtualization technology have enabled the sharing of computing and networking resources of cloud data centers among multiple users. Virtual Network Embedding (VNE) is highly important and is an integral part of the cloud resources management. The lack of historical knowledge on cloud functioning and inability to foresee the future resource demand are two fundamental shortcomings of the traditional VNE approaches. The consequence of those shortcomings is the inefficient embedding of virtual resource on Substrate Node (SNs). On the contrary, application of Artificial Intelligence (AI) in VNE is still in the premature stage and needs further investigation. Considering the underlying complexity of VNE that includes numerous parameters, intelligent solutions are required to utilize the cloud resources efficiently via careful selection of appropriate SNs for the VNE. In this paper, Reinforcement Learning based prediction model is designed for the efficient multi-stage Virtual Network Embedding (MUVINE) among the cloud data centers. The proposed MUVINE scheme is extensively simulated and evaluated against the recent state-of-the-art schemes.

2. TITLE: Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review

AUTHOR: O. Ali, A. Shrestha, J. Soar, and S. F. Wamba

YEAR: 2019

DESCRIPTION: Cloud computing offers an innovative method of delivering IT services efficiently. Extant literature suggests that clouds technology can enhance the level of services in various industries, including healthcare service. As with any technological innovation, cloud computing should be rigorously evaluated before its widespread adoption. This research study presents a systematic review of scholarly articles of cloud computing in the healthcare sector. We considered 316 articles and filtered down to 88 articles to presents a classification framework that has three dimensions: cloud computing-enabled healthcare opportunities, issues, and applications. Implications to future research and practice are highlighted in the areas of value-added healthcare services towards medical decision-making, data security & privacy obligations of cloud services providers, health monitoring features and innovative IT service delivery models using cloud computing.

3. TITLE: cyber syndrome and its formation, classification, recovery and prevention

AUTHOR: H. Ning, S. Dhelim, M. A. Bouras, A. Khellou_, and A. Ullah

YEAR: 2020

DESCRIPTION: There evolutionary change in information and communication technology has made the people's lives much convenient more than ever before. But it has affected the human's physical and mental health as well as community's social connectivity. Cyber syndrome is the physical, social, and mental disorders that affect the human being due to the excessive interaction with the cyberspace. Many previous works have discussed the role that the technology plays in the development of specific disorders, such as Internet addiction disorder or gaming addiction disorder. However, none of these works have explored the effects of excessive interaction with the cyberspace on the people's lives as a whole and its impact on the social connectivity of the community. Therefore, in this paper, we have presented the formation stages, classification, recovery, and prevention methods of cyber syndrome. We have explored the impact of cyber Syndrome in physical, social, and thinking spaces and its future implication and complications.

III. SYSTEM ARCHITECTURE

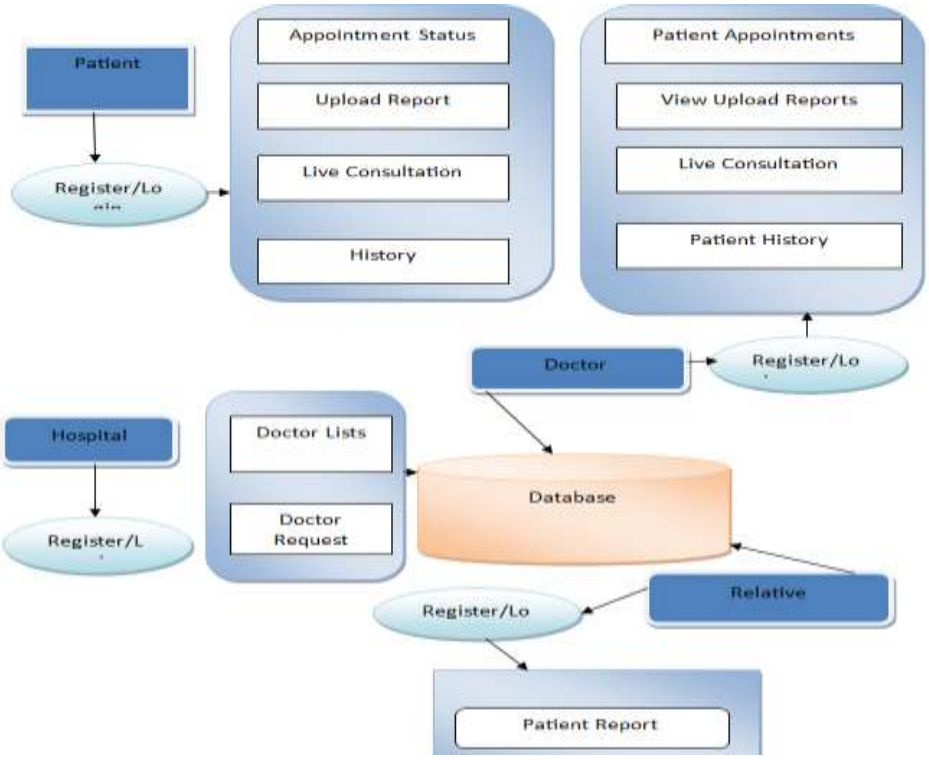


Fig 1: System Architecture

3.1 Methodologies

3.1.1 Module Overview

The system is organized into key modules, each designed to handle distinct aspect of patient's healthcare records in network information. The modules are as follows:

- User Interface
- Doctor
- Patient
- Hospital
- Relative

3.1.2 Module Descriptions

1. User Interface

In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly user can login into the server else user must register their details such as username, password and email id, into the server.

2. Doctor

First doctor has to register with all detail. Doctor has to takes permission from the hospital. Patients also takes permission from a doctor. Doctor have a patient appointment. Doctor has a view uploaded report. Doctor has a live consultation with the patient. Doctor has a patient history.

3. Patient

The patient has to register with all details. Patient has to login into the server. Patient has takes permission form a doctor. Doctor has approved. Then patient has an appointment status of a doctor. Patient has uploaded a diseases report. Patient has a history of record stores in a database.

4. Hospital

The hospital has a register with an id and password. Hospital has all doctor lists. Hospital has a doctor requests.

5. Relative

The relative has a register with a user id and login. Relative has a third party to see a patient lists. Relative has a patient record.

3.2 Technique

This paper is to improve the security of e-healthcare records in cloud computing environments and keep their privacy by reducing the number of security and privacy problems in cloud computing, such as information loss, data modification, and data leaks.

3.3 Design and Workflow modeling

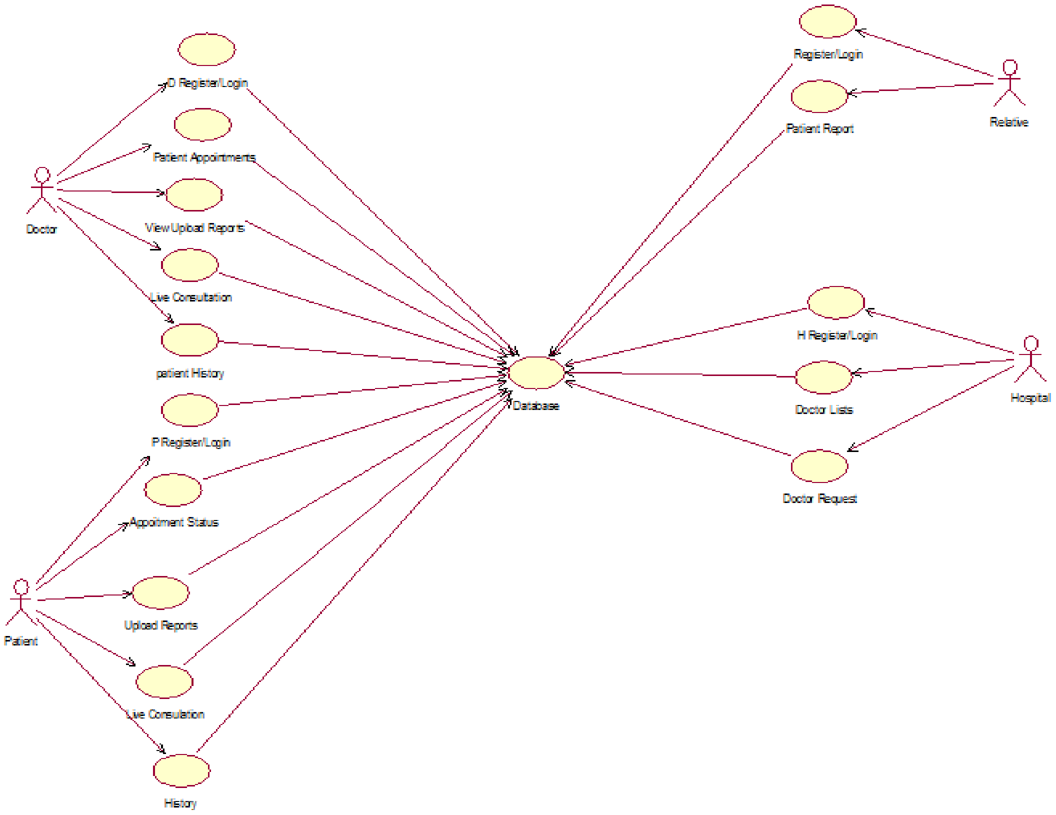


Fig 2: Use Case Diagram

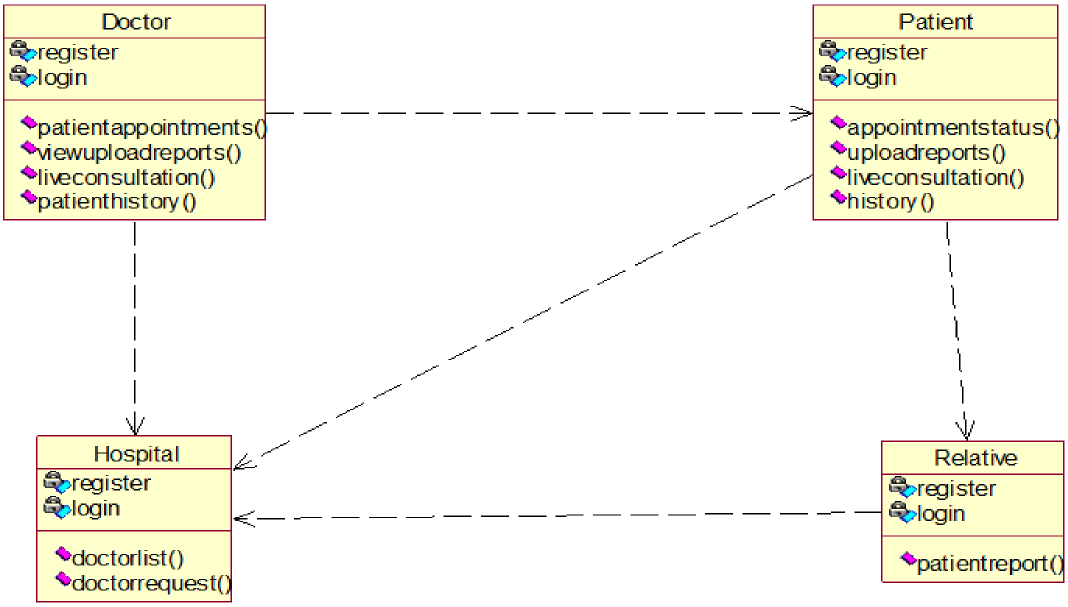


Fig 3: Class Diagram

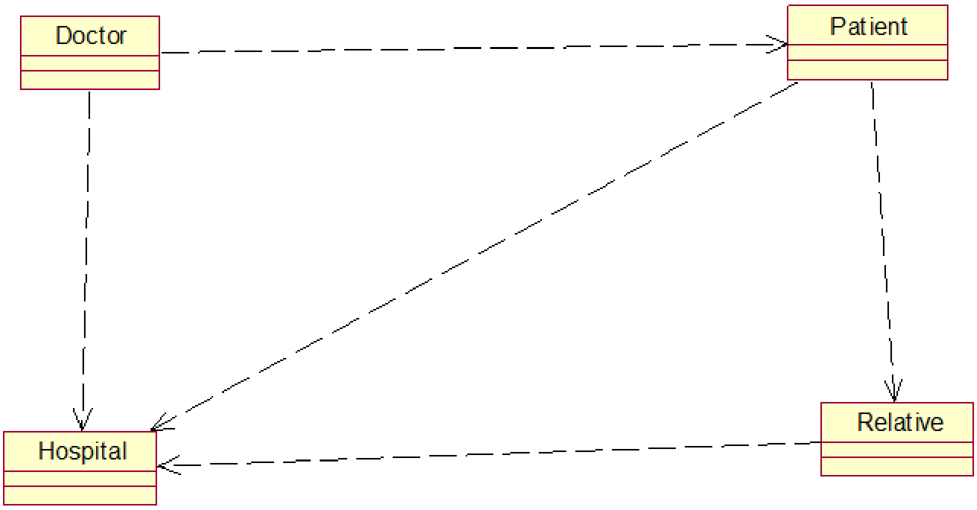


Fig 4: Object Diagram

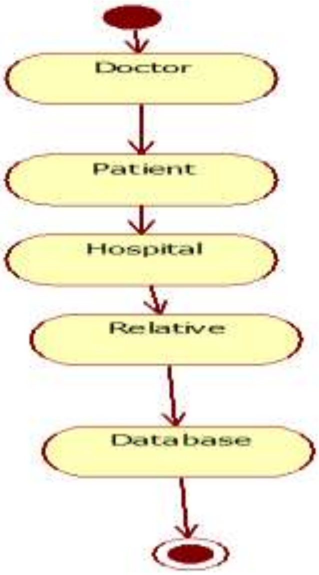


Fig 5: Activity Diagram

Design Engineering deals with the various UML (Unified Modeling Language) diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software.

In the USE CASE DIAGRAM, it captures the interactions between the various actors (doctor, patient, hospital, and relative) and the system. Each actor has specific responsibilities and interactions that contribute to the overall functionality of the healthcare management system. To create a visual representation, you can use diagramming tools as mentioned earlier.

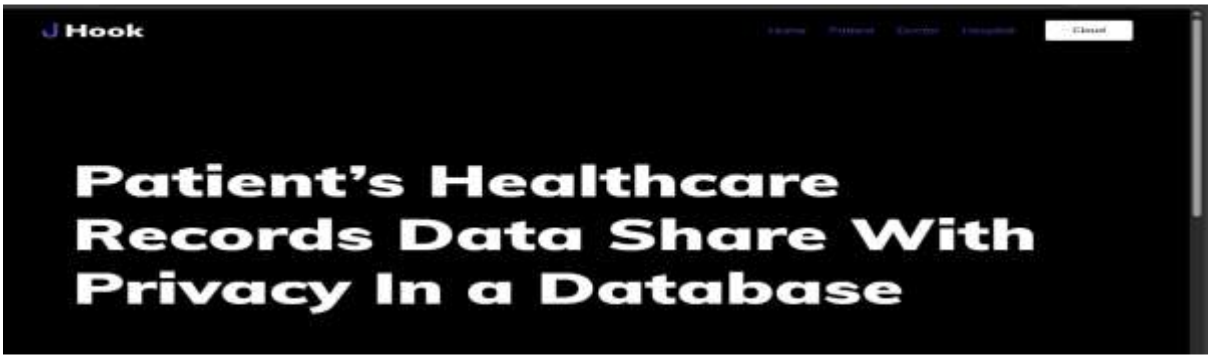
In CLASS DIAGRAM, here are the identified classes along with their attributes and methods has formed a relationship between each other by one-to-many like doctor to patient, patient to hospital.

In OBJECT DIAGRAM, it is a visual representation of a system at a specific point in time, showing instances of classes (objects) and their relationships. It is a snapshot of the system, illustrating how object interact with one another.

In ACTIVITY DIAGRAM, it starts with the patient initiating the consultation process. The patient logs in, views available doctors, selects one, and requests an appointment. After receiving confirmation, the patient prepares and joins the live consultation. Following the consultation, the patient receives a summary and has the option to upload any relevant reports. Finally, the patients log out, concluding the process.

IV. RESULTS AND DISCUSSION

This project is implements like web application using COREJAVA and the server process is maintained using the SOCKET & SERVERSOCKER and the design part is played by cascading style sheet.

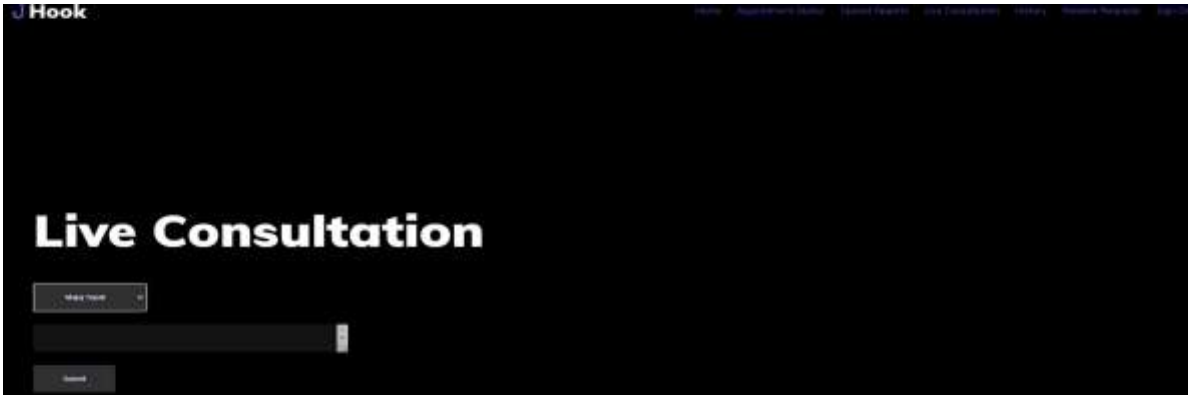


Patient's Healthcare Records Data Share With Privacy In a Database

Fig 6: Home Page

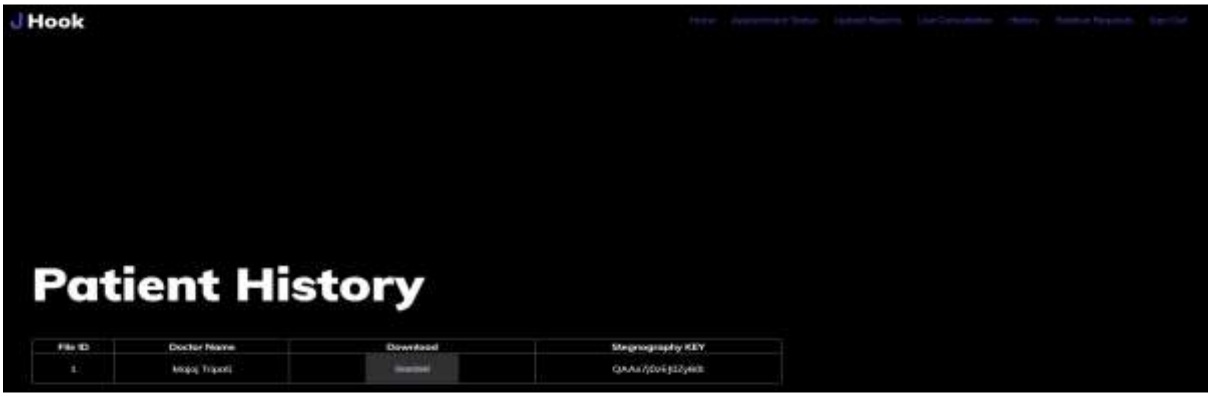
Patient Home

Fig 7: Patient Home Page



Live Consultation

Fig 8: Patient Live Consultation



Patient History

File ID	Doctor Name	Download	Stegnography KEY
1	Manoj Tripati	Download	QAAa7jDo4jt2yk8

Fig 9: Patient History Page

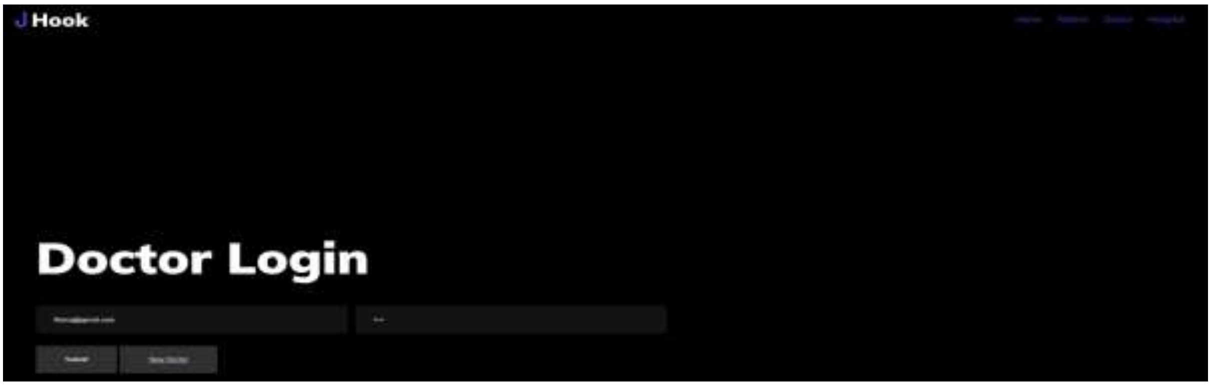
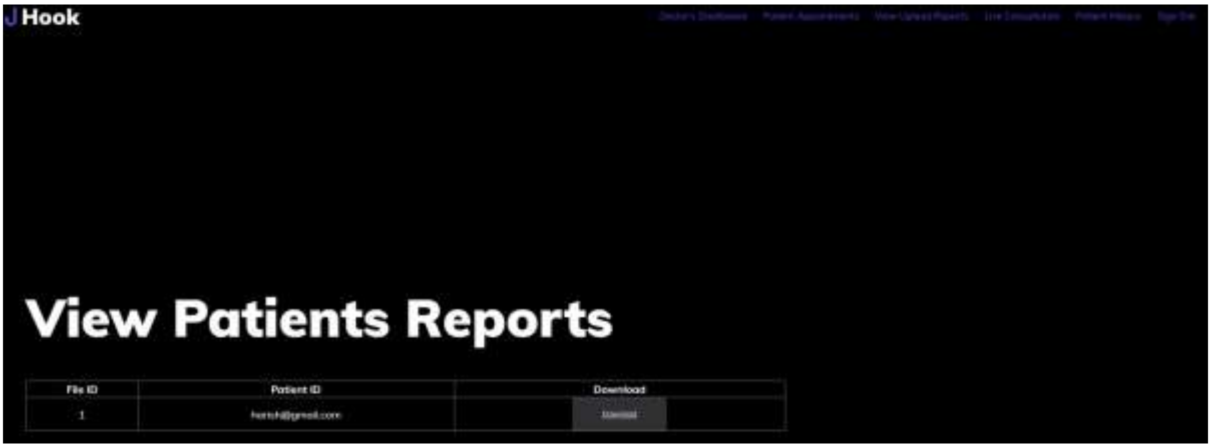


Fig 10: Doctor Login

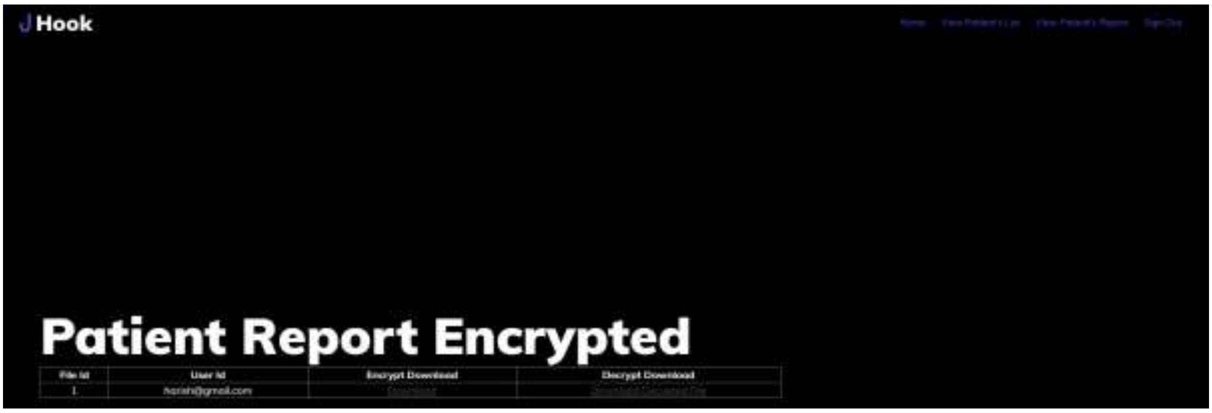


File ID	Patient ID	Download
1	harish@gmail.com	Download

Fig 11: Doctor View Patient Report

Fig 12: Cloud Login Page

Fig 13: Relative Login



Patient Report Encrypted

File Id	User Id	Encrypt Download	Decrypt Download
1	harish@gmail.com	Download	Download Decrypted File

Fig 14: Relative Patient Report

V. CONCLUSION

This paper examines the effectiveness of steganography encryption in a cloud environment by comparing latency and throughput with Ethereum and Hyperledger fabric platforms with varying transaction numbers. It is a significant challenge to ensure the security of patient's e-health records in the cloud. Additionally, the proposed PRMS (Patient Medical Records Management System) is compared to the secure and robust healthcare-based block chain method (SRHB) in terms of System Execution Time (SET) and Average Delay. The efficiency of the proposed PRMS architecture has many quality matrices like maintaining user privacy, effectively medical data sharing, and information hiding. PRMS is a security architecture that uses cryptography and steganography to protect patient health records in the third-party cloud from unauthorized access while also allowing patients to control their health records. The entire system was constructed, and some of the system design of the PRMS cloud-based e-health application was described in the paper.

VI. FUTURE SCOPE

Future work will include the addition of data encryption and cloud storage security algorithms to the PRMS system in order to further enhance the cloud security of patient data. External access to e-healthcare data transferred across multiple networks will be the subject of additional data security and privacy analyses in the near future.

VII. REFERENCES

[1] M. Azhagiri, R. Amrita, R. Aparna, and B. Jashmitha, "Secured electronic health record management system," in Proc. 3rd Int. Conf. Commun. Electron. Syst. (ICCES), Oct. 2018, pp. 915_919.

[2] N. Dong, H. Jonker, and J. Pang, "Challenges in e-health: From enabling to enforcing privacy," in Proc. Int. Symp. Found. Health Informat. Eng. Syst. Cham, Switzerland: Springer, 2011, pp. 195_206.

[3] X. Yi, Y. Miao, E. Bertino, and J. Willemson, "Multiparty privacy protection for electronic health records," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2013, pp. 2730_2735.

[4] C. S. Kruse, M. Mileski, A. G. Vijaykumar, S. V. Viswanathan, U. Suskandla, and Y. Chidambaram," Impact of electronic health records on long-term care facilities: Systematic review, "JMIR Med. Informat., vol. 5, no. 3, p. e35, Sep. 2017.

[5] Y. Al-Issa , M. A. Ottom, and A. Tamrawi, "E-Health cloud security challenges: A survey," J. Healthcare Eng., vol. 2019, pp. 1_15, Sep. 2019.

[6] H. K. Thakkar, C. K. Dehury, and P. K. Sahoo, "MUVINE: Multi-stage virtual network embedding in cloud data centers using reinforcement learning based predictions," IEEE J. Sel. Areas Commun., vol. 38, no. 6, pp. 1058_1074, Jun. 2020.

[7] H. K. Thakkar, P. K. Sahoo, and B. Veeravalli, "RENDA: Resource and network aware data placement algorithm for periodic workloads in cloud," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 12, pp. 2906_2920, Dec. 2021.