IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204263 |

Blockchain Framework for Securing and Managing Electronic Healthcare Records

Nidhi G T[1], Priyanka S [2], Sneha G M[3], Yashaswini S P[4], Dr. Pardeep N [5]

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[1]

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[2]

U.G. Student Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[3]

U.G. Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[4]

Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davanagere, Karnataka, India[5]

ABSTRACT: In the era of smart cities and smart homes, the patient's information like name, personal details and disease description are highly insecure and tampered most often. These details are stored digitally in a network called Electronic Health Record (EHR). The EHR can be useful for future medical researches to improve patients' healthcare and the performance of clinical practices. These data is not accessible for the patients and their caretakers, but they are easily available for unauthorized external agencies and are readily breached by hackers. This creates an imbalance in data accessibility and security. This can be resolved by using blockchain technology. The blockchain creates an immutable ledger and makes the transaction to be decentralized. The blockchain has three main key features namely Security, Transparency, and Decentralization. These key features make the system to be highly secured, they prevent data manipulation, and can only be accessed by authorized persons. In this paper, a blockchain-based security framework has been proposed to secure the EHR and provide a safe way of accessing the clinical data of the patients for the patients and their caretakers, doctors, and insurance agents using cryptography and decentralization. The proposed system ismainly responsible for maintaining the balance between data accessibility and security. This paper also directs how the proposed framework helps doctors, patients, caretakers, and external authorities to securely store and access patients' medical data in EHR.

KEYWORDS:Blockchain; electronic healthcare record (EHR); cryptography; decentralization;storage; security; accessibility

I. INTRODUCTION

The advancement in technology in the past few decades has affected several parts of human life. It has benefitted us inmany living sectorsespecially healthcare. There has been significant progress in the healthcare industry in pastfew years. We can now store our medical records electronically. Clinical technicians can perform better diagnoses of patients,the communication between doctors and patients became effortlessly advanced and doctors are instantly available to the patients at the time of emergency[1]. Through electronic records, the patients can contact their doctors even from remote places. But along with the pros of modern technology, the drawbacks of this advancement also existed. Theincreased advancement in information technology helped hackers by providing them better hacking tools for accessing therecords and altering them. Thus, increasing the threat to the security of medical records and privacy of patients. Inthis paper, we propose a system to secure these medical records(EHRs) and protect the privacy of the patient from such acts[1].

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204263 |

Decentralization, security, privacy, and resilience through cryptographic algorithms are all elements of blockchain that have the potential to tackle the present difficulties in the healthcare industry. The digital healthcare service plays a critical role in keeping and storing data. However, it has a big issue with patient information leaking out. The existing healthcare system is insecure among several medical services because of data availability delays and the danger of data theft. Hospital records can be archived without the patient's knowledge. Due to several challenges, such as security and accessibility of data, there has been no exploration or experimentation in the healthcare industry.

In today's healthcare sector, securely accessing data within the network is a top focus of the proposed system. The blockchain-based system can generate excellent outcomes in many ways if used appropriately. It is an efficient and effective way to secure authentic information. The information is maintained as a ledger feature in blockchain technology with the smart contract, controlling the patient's access to medical records. It guarantees security, ease of access, and other manufacturing aspects of administration, as well as privacy, validity, and authentication for this system.

II. RELATED WORK

Cybersecurity is a set of technologies and processes designed to protect computers, networks, programs and data from attacks and unauthorized access, alteration, or destruction. A network security system consists of a network security system and a computer security system. Each of these systems includes firewalls, antivirus software, and intrusion detection systems (IDS). IDSs help discover, determine and identify unauthorized system behaviour such as use, copying, modification and destruction. The purpose of this paper is for those who want to study network intrusion detection in ML/DL. Thus, great emphasis is placed on a thorough description of the ML/DL methods, and references to seminal works for each ML and DL method are provided. Examples are provided concerning how the techniques were used in cyber security. Similarly to ML methods, DL methods also have supervised learning and unsupervised learning. Learning models built under different learning frameworks are quite different. The benefit of DL is the use of unsupervised or semi-supervised feature learning and hierarchical feature extraction to efficiently replace features manually. With the increasingly in-depth integration of the Internet and social life, the Internet is changing how people learn and work, but it also exposes us to increasingly serious security threats. How to identify various network attacks, particularly not previously seen attacks, is a key issue to be solved urgently.

III. METHODOLOGY

The Electronic health records(EHR)are regulated by health centres instead of patients, making it difficult to obtain medical advice from various health centres. Thus, patients need to concentrate on restoring the management of their health details and their medical information [4,5]. The quick evolution of blockchain technology encourages population healthcare, including access to patient information and medical data. The technology offers patients access to extensive, consistent reports with free access to EHRs from treatment websites and providers. In this section, we describe the development of a blockchain security framework for EHR with multiple authorities to meet the need for blockchain in shared EHR systems. This framework protects the privacy of patients and maintains the consistency of EHRs.Using Blockchain framework for EHR, the patient is able to manage, download and share his/her EHRs independently.There are six entities consisting in our framework , such as attribute authority organization (AAO), patients, hospitals, blockchain system, EHR servers, and medical data users (such as medical institutions and insurance companies)[10].

The AAO is mainly responsible for distributing the corresponding attribute signature key SIKi,GID, transformed key tk and private key d to the patient, medical data users and hospitals respectively. The patient formulates the access control policy 3 and sends 3 to the hospitals. Then, the patient generates the signature key of medical-related information according to the LSSS[9]. Finally, the patient sends signature key and medical related information to the data pool. The hospital encrypts the medical data according to the access structure 3 specified by the patient and sends the ciphertext CT to the data pool. The blockchain system consists of a data pool, blockchain and consensus network. The data pool stores medical data ciphertext, medical-related information and its signature. To improve the security of the medical data, the consortium blockchain is constructed in the system[6].

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204263 |

The EHR system server is one of the nodes in a blockchain network. It acts as a miner that collects transactions (EHRs) and organizes them into blocks. Whenever EHRs are created after treatment, all network nodes receive them and verify their validity.Then, the miner node gathers these transactions from the data pool and begins assembling them into a block. The data pool is a "waiting area" for transactions that each node maintains for itself. After a transaction is verified by a node, it waits inside the data pool until it is picked up by a miner and inserted into a block. This new block will then be added to the blockchain.This happens by creating a so-called "hash". A hash is a 256-bit number that uniquely identifies the data in the block.In the consensus network, the proofof-stake (PoS) mechanism is used in the process to ensure the security of the blockchain ledger. The consensus nodes first implement the PoS mechanism to select the accounting nodes, which can realize the distributed consensus of the blockchain.Compared with the distributed server, blockchain has the characteristics of decentralization, verifiability and immutability, which are essential in our system[8]. Next, the accounting nodes sends the storage address of cloud medical data ciphertext and medical-related information to the blockchain.And the EHR is also authorized by the data users to complete a partial decryption of the encrypted medical data[7].

IV. EXPERIMENTAL RESULTS

Figures shows the results of managing and securing electronic healthcare records based on blockchain technology using secure hash 256 algorithm. Fig(a) shows the interfaces of EHR website(b) is the image obtained when a new patientregisters(c)is the image showing confidential patient information (d)shows the hospital login details of a already registered hospital (e)shows the interface of login credentials of a medical data user (f)shows the interface of attributeauthority login (g) shows the interface of a local cloud server (h) shows the encryption and decryption time graph.

Fig (a) shows the interfaces of EHR website

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204263 |

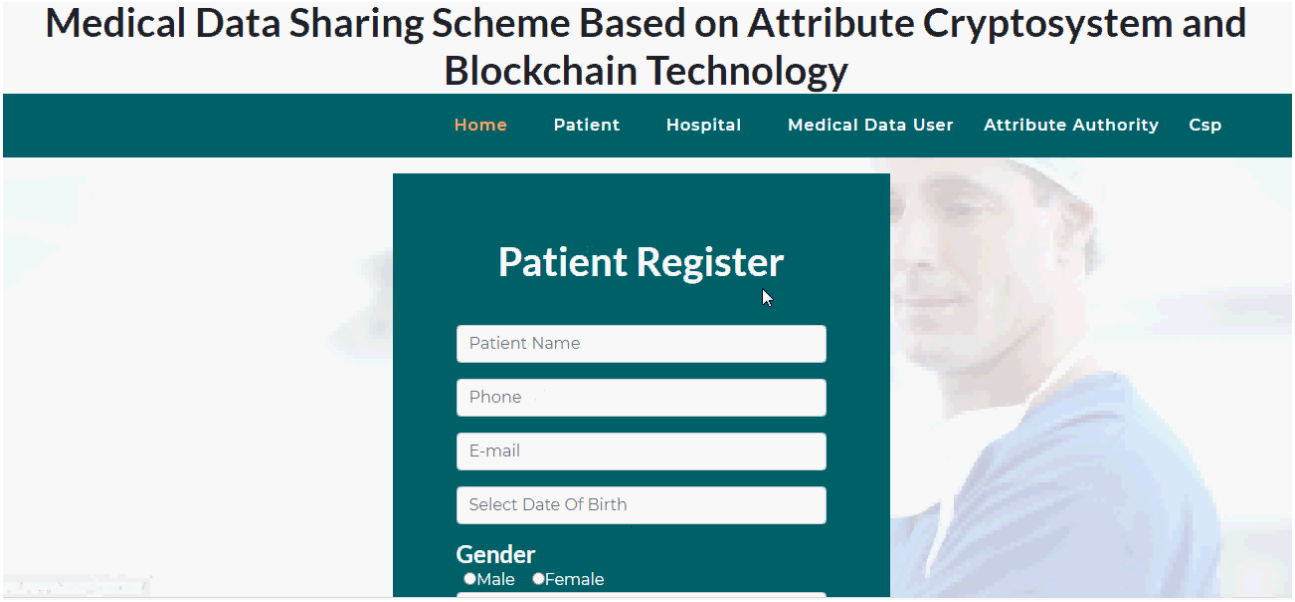

Fig (b) display the image of a new patientregistration

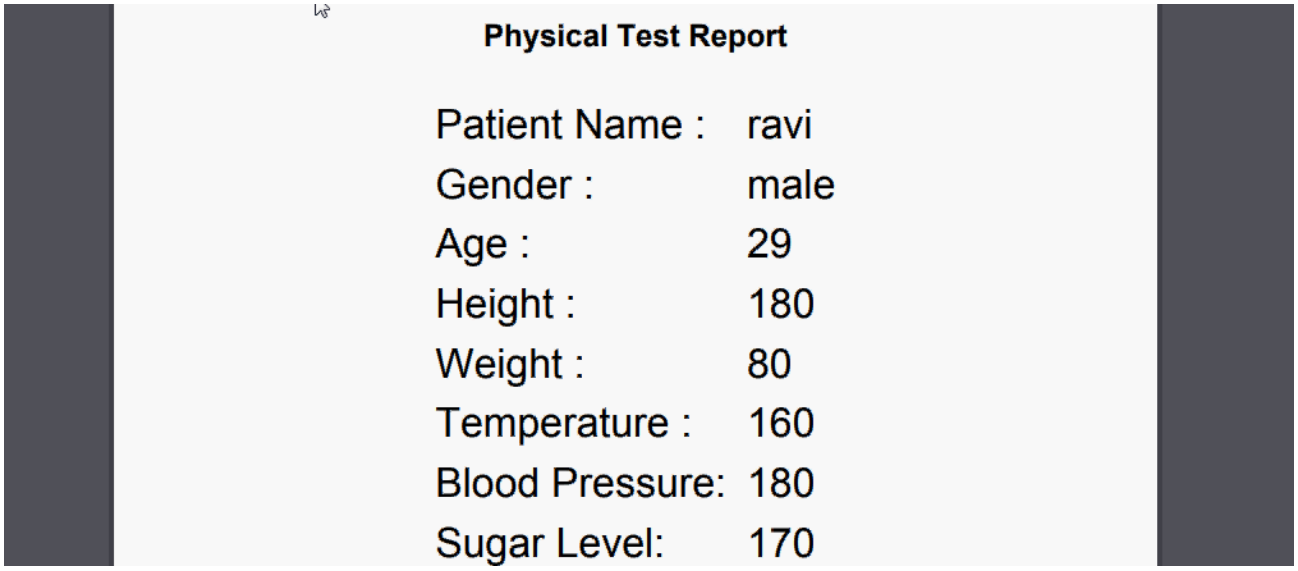

Fig (c) shows the confidentialpatient information

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204263 |

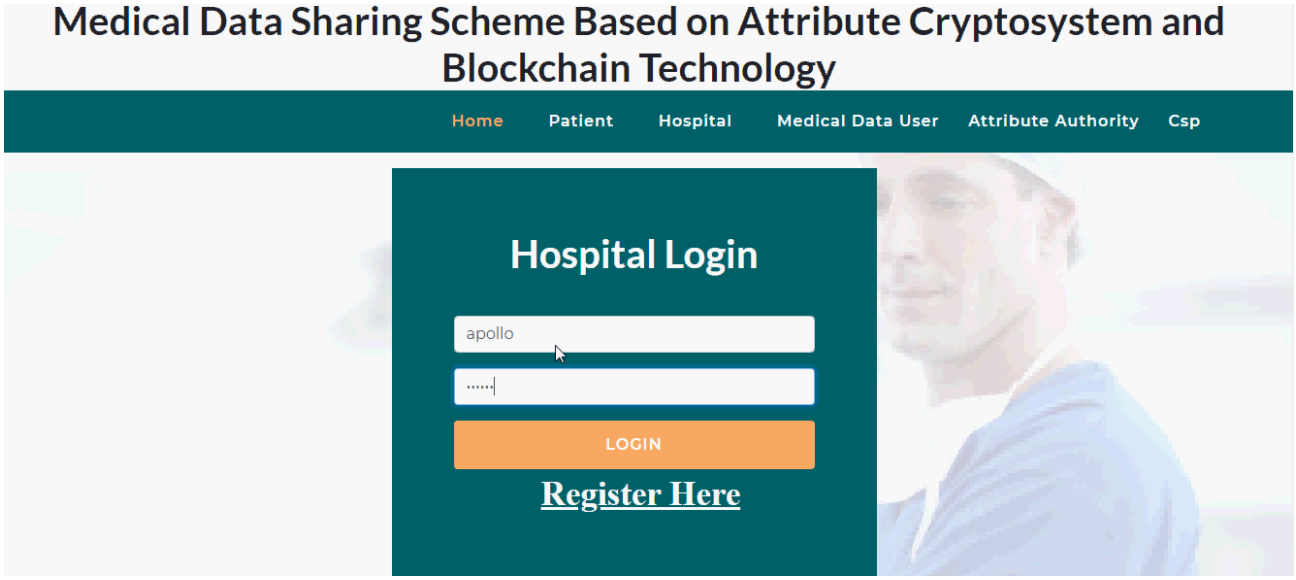

Fig (d) shows the hospital login details

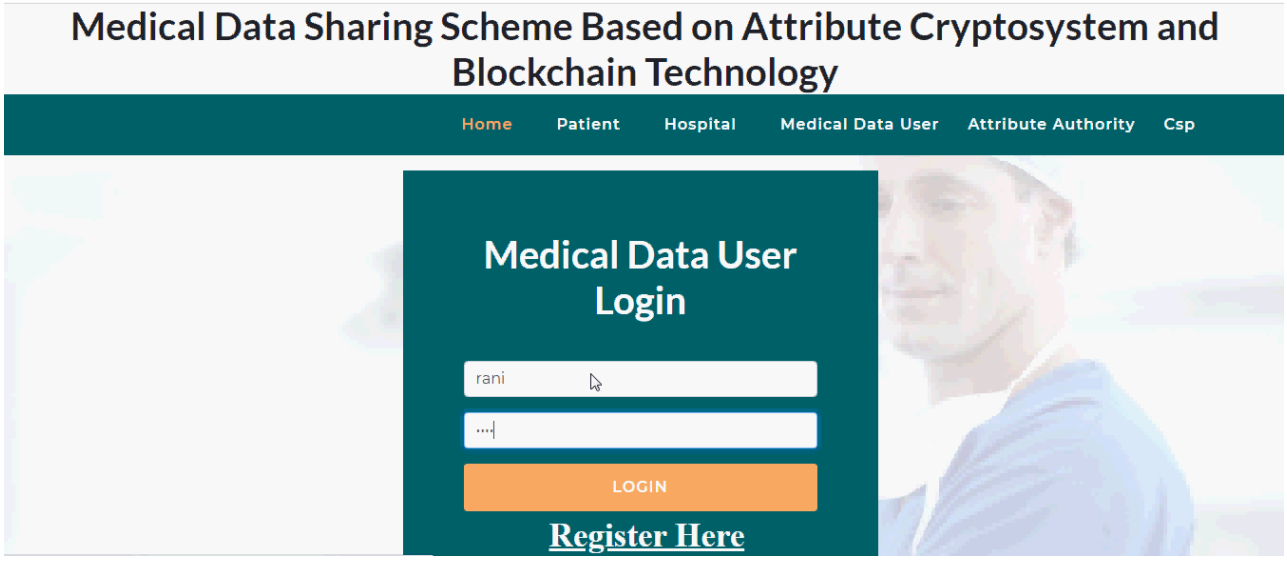

Fig (e) shows login credentials of a medical data user

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204263 |

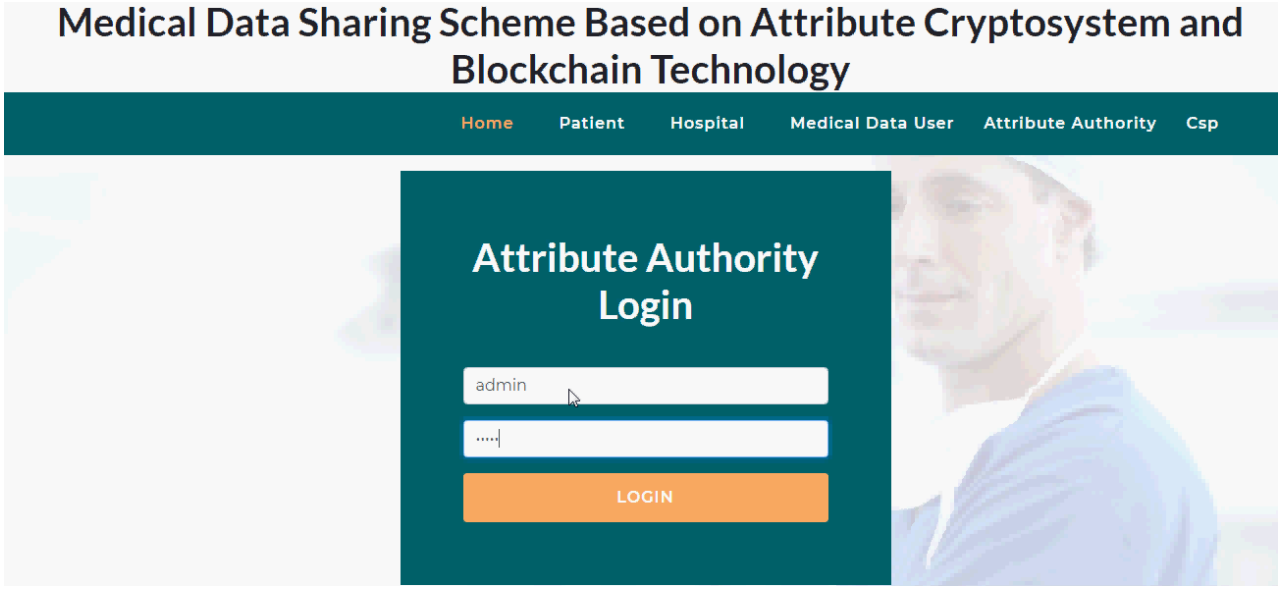

Fig (f) shows the interface of attribute authority login

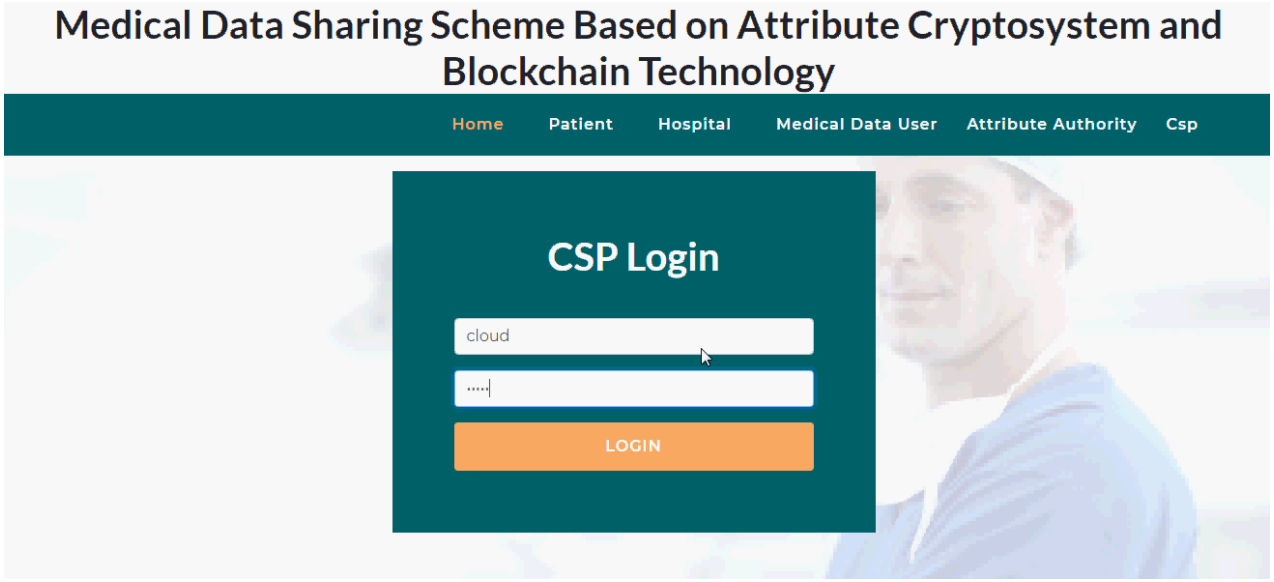

Fig (g) shows the interface of a local cloud server

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204263 |

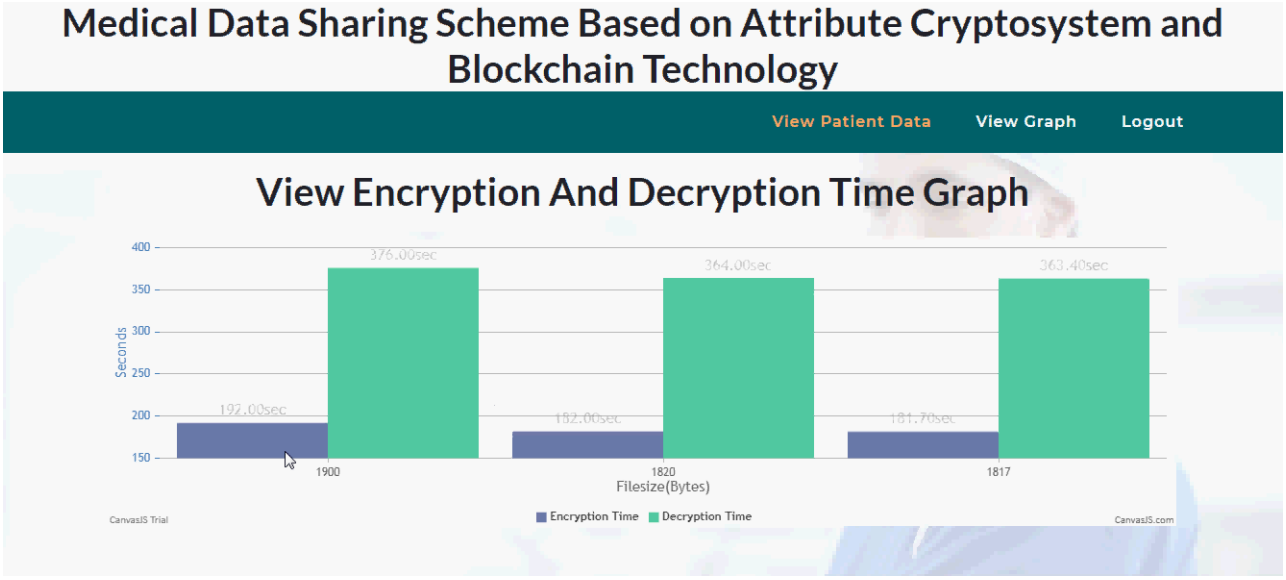

Fig (h) shows the encryption and decryption time graph

V.CONCLUSION

The proposed framework in our paper describes the various features of blockchain in the field of healthcare for data storage in EHR and sharing them between the users. This framework overcame the limitations of current data models and supply chains. The access control, time consumption for requesting and searching data in EHR in a blockchain, and the feature comparison were also discussed in this paper and the results show that the proposed system outperforms the existing approaches in all possible ways. From the proposed approach, it is clear that the use of blockchain in healthcare data management prevents data breaches and fraudulent billing and enhances privacy, security, and transparency. Also, data sharing via blockchain facilitates safe and secure sharing among authorized third parties. This approach guarantees
secure healthcare management among all the levels which include patients, doctors, hospitals, insurance companies, Pharmaceuticals.

REFERENCES

1. R. Klitzman, "“Patient-time”, “doctor-time”, and “institution-time”: Perceptions and definitions of timeamongdoctors who become patients", Patient Education and Counseling, vol. 66, no. 2, pp. 147-155, 2007.Available:10.1016/j.pec.2006.10.005.
2. E. Bertino, R. Deng, X. Huang and J. Zhou, "Security and privacy of electronic health information systems", International Journal of Information Security, vol. 14, no. 6, pp. 485-486, 2015. Available: 10.1007/s10207-0150303-z.
3. J. Fernández-Alemán, I. Señor, P. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review", Journal of Biomedical Informatics, vol. 46, no. 3, pp. 541-562, 2013. Available:10.1016/j.jbi.2012.12.003.
4. Cilliers, L. Wearable devices in healthcare: Privacy and information security issues. *Health Inf. Manag. J.* **2020**, *49*, 150–156.
5. Bach, L.M.; Mihaljevic, B.; Zagar, M. Comparative analysis of blockchain consensus algorithms. In Proceedings of the 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 21–25 May 2018; pp. 1545–1550.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204263 |

6. V. Goyal, A. Jain, O. Pandey, and A. Sahai, ‘‘Bounded ciphertext policy attribute based encryption,’’ in Proc. ICALP, 2008, pp. 579–591.
7. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, ‘‘Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,’’ in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., vol. 2010, pp. 62–91.
8. A. Lewko and B. Waters, ‘‘Decentralizing attribute-based encryption,’’ in Proc. 30th Annu. Int. Conf. Adv. Cryptol. (EUROCRYPT), vol. 2011, pp. 568–588.
9. A. Beimel, O. Farràs, Y. Mintz, and N. Peter, ‘‘Linear secret-sharing schemes for forbidden graph access structures,’’ in Proc. Theory Cryptogr. Conf. Cham, Switzerland: Springer, 2017, pp. 394–423.
10. M. Abomhara and H. Yang, ‘‘Attribute-based authenticated access for secure sharing of healthcare records in collaborative environments,’’ Hospital, vol. 3, no. 6, pp. 3–20, 2016.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details