Protected Admittance E-Health Record System Using Blockchain Technology

Sharyu Kadam and Dilip Motwani

Abstract E-health record is considered as an individual's health document, which gets shared among several amenities. The EHR system is becoming a popular protagonist as it has the potential to transform the paper-based industry into the digital system for maintaining the patient's health records. Nevertheless, the E-health record system needs renovation in terms of confidentiality and access to records since the hospital authority is treated as a central holder for the records. The proposed system comes up with a novel solution to modernize the traditional centralized system by the erection of a decentralized framework, whereas the patient is the sole owner of the health document. Implementation of blockchain technology with a decentralized patient-centered structure promotes a secure healthcare system. Blockchain's open admittance would permit changes to an individual's her, which needs to be restructured in real-time and makes it instantly available to parties involved for the same. The use of shrewd agreements and dispersed stockpiling improves the therapeutic administrations, including clinical records comparably persistent related proof. This high-level model gives high security and ease of utilizing the highlights through disseminated record where information can't be held for payment, where every client has a refreshed duplicate of the blockchain.

Keywords Block chain · Distributed ledger · Electronic health record (EHR) · IPFS · Security

1 Introduction

The present digital era is moving away from the long-standing system and believes in modern practices. This modernization has facilitated the convenience to different sectors so that the health sector also remains as one of the consumers, which discover novel ways for improvement. An electronic health record provides a great feature, where patient acquires clinical records in purely digital form in spite of paper [1].

S. Kadam · D. Motwani (✉)
Computer Engineering Department, Vidyalankar Institute of Technology, Mumbai, India
e-mail: dilip.motwani@vit.edu.in

The move towards patient control collaboration has the potential to introduce a new platform for data sharing in healthcare and hence brings new challenges and requirements related to privacy and technology. E-Health record systems are real-time and patient-focus records that offer records immediately and securely to authorized users. This structure facilitates the ownership of the records to patients in order to achieve confidentiality and ease of access. This structure remains helpful to deliver secure data access and exchange with valid approval. This protected admittance of EHR structure will offer cavernous shared faith between each associated with the help of blockchain technology [2]. Furthermore, this system provides the distributed storage to maintain EHRs in a secure and steady form, hence the patient become a sole owner and creates a patient-centred environment to provide interoperability among the specialist [3].

2   Literature Review

[1]**"Securing Blockchain based Electronic Health Record using Multilevel Authentication Radhakrishnan, A Sam Joseph, S. Sudhakar, International Conference on Advanced Computing & Communication Systems (ICACCS), 2019**.

E-medical system has various shades of patient's medical information and their medical antiquity. Damage to electronic health record stimulates a confusing prescription. Societal insurance frameworks serve fewer safety attempts to guarantee about fitness histories. Blockchain is a flowed and distributed data that acknowledges an essential action in guaranteeing the information and exchange. Presentation of blockchain with respect to the social organization framework guards the fitness information against the provokers. This paper suggests an astounding insistence and grounded course of action to guard the blockchain against the assaults referred currently.

[2]**"Using Blockchain for Electronic Health Records", Ayesha Shahnaz1, Usman Qamar1, (Member, IEEE), Ayesha Khalid, (Member, IEEE), IEEE, 2019**.

In time, this effort will revolutionize the world of technology. This change has made it much easier for the patient to handle data in digital form but there are also some problems with its convenience. Safety and confidentiality are the two most important apprehensions for patients and it is equally important to verify the unauthorized access to such vital information. Of course, adaptability and interoperability are also remaining critical issues that require significant research focus. Proposed work addresses the special issues and spotlights the profits of the blockchain development for the association of an ensured and flexible response for clinical data exchange in order to have the best introduction.

[3]**G. Jetley and H. Zhang, "Electronic health records in IS research: Quality issues, essential thresholds and remedial actions," Decis. Support Syst., vol. 126, pp. 113–137, Nov. 2019**.

E-clinical records are serious, extremely delicate isolated data in the medical sector, which is must commonly share with other parties. Blockchain delivers a communal, absolute and secure structure to established accountability and transparency. This research offers an exclusive prospect to develop a confidential and distributed EMR system using blockchain. The perspectives of this paper are to provide a decentralized E-clinical system, for data sharing among the healthcare providers. In association with Stony Brook University Hospital, the executed structure ensures security, availability, and accessibility over E-medical records. Offered effort can expressively shrink the turnaround time for EHR distribution and progress judgment ability for health care.

[4]**"Health Record Management through Blockchain Technology", Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte, IEEE, 2019**.

The exchange of E-records on the clinical background has unimaginable progressive importance for the exploration of infirmity and experts' decision. Lately, cloud-based E-clinical data exchange arrangement has transported enormous measures of convenience, yet the monopolization for cloud system opens risks unavoidably to data safety. Blockchain advancement is oftentimes seen as a promising response to deal with these issues by ideals of its amazing assets of decentralization, mystery, and proof. Here, the blockchain-based structure offers safe and shielded exchange of E-health records. Data demander demands for specific e-health record which is retrieved from the blockchain-based cloud server in the encrypted form after the owner's permission. The use of blockchain methodology achieves security and confidentiality aspects for the system.

[5]**"BlocHIE: a BLOCkchain-based platform for Healthcare Information Exchange", Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. 2018 IEEE International Conference on Smart Computing (SMARTCOMP)**.

HIE submitted remarkable achievements for the clinical sector. Uploading and sharing copious clinical information is a chief requirement as well as a great challenge. In this paper, BlocHIE is a platform that provides interoperability for healthcare information. The initial step as per this paper was to perform an investigation of the different requirements which need to be shared and their different sources. Based on this investigation, the system will hire Blockchain to operate on miscellaneous e-health records. Furthermore, to achieve confidentiality and authenticity combination of on-chain and off-chain verification was used.

3   Problem Statement

Traditional framework believes in centralized storage method and as per this traditional methodology clinical centers are responsible to hold the entire information of a patient into to the central database as well as the access of this data is also done through a central authority [3, 4]. According to the investigation of the current system, one of the problems has been noticed that various types of vital as well as
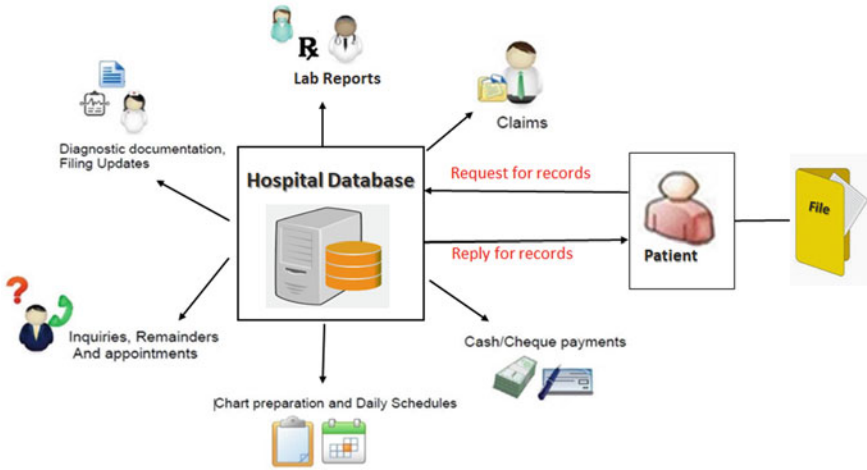
Fig. 1 Existing centralized EHR system

personal information take place into the EHR system like appointment documents, different format of reports and personal information which is in steady form and not available all the time with the patient [5]. Access to past clinical records for a patient is a struggling task as they need to approach hospital authority every time. Provision of secure medical data is another toughest task as this data handle by various clinicians/doctors.

Figure 1 illustrate the traditional framework of data where hospital management is the owner of the data process and data exchange. In this centralized structure, After the patient is examined or treated for his illness, the hospital office authority is responsible to take care of all the relevant documents. Data access is one of the irritating and waiting processes from the patient site as they require the permission of hospital authority every time. By reason of the consolidated storage system faces information damage.

3.1 Objectives

The approach behind the proposed system is to come up with a polished framework to whelm the issues related to the existing system and Provides secured and classified records by exploring "Blockchain Technology" [4]. The main objective of this system is to eliminate centralized authority and avail easy access facility to the patients for their steady form records anytime. Utilization of blockchain technology helps in order to provide secured and unchanged data which reduce the data loss or data modification [6]. Our examination contributes innovative information for the interconnection between the performances of an E-Health Record structure and as

needs be the idea of social administrations passed on inside the inpatient setting. The goal of the system is to divert patient from paper-based industry to digitalization hence no need to transport records in the form of papers by patient. Digital gadgets becomes one of the finest media for storing the data in order to improve the usability of the system.

4 Related Work

Until now, most of the hospitals were operating according to the existing system which is based on centralization and due to such a central system records handling is not an easy task for patients [7]. The necessary situation according to that patient always handles records in the paper arrangement. Storage of large volume records and to access those records is another challenge for the existing system [8]. Adoption of the decentralized method provides handy use of records to the patients. Another major concern of this historical structure is security provision for vital information of the patient. According to the centralized approach, all the records handled by hospital management [9]. Hospital is blamed for carelessly supervision the clinical data, changing it or breaking the privacy of the histories. Blockchain-Based EHR along with decentralization delivers a locking system to the patients due to which patient has the facility to restrict the admittance of records for health specialist [10, 11].

5 Proposed System

With most advanced stage of development in computers, an existing structure provides approach for storage of patient's health records. This system provides an excellent type of technique that allows the patient's record, reports and specialist's solution to be handled very well. Due to centralized mechanism there is chances of data leakage and unauthorized access of patient's records. In centralized framework patients are unable to hide and secure their own data. There is always a lobby and patient need to wait outside the lobby when they want to access their data. By considering these issues, the system is come up with a new concept of decentralization by using Blockchain technology. System is able to gain security of records by implementing unique ID and hashing concept of blockchain. Unauthorized access restricted by adoption of decentralized method.

Figure 2 overviewed the decentralized concept for secured information exchange by using latest technology i.e. Blockchain where patient is a decision maker for his/her records by granting and denying the permissions. Uploading records with the unique id is the main task of the patient. Further, these records transferred on Blockchain with secured hash value.
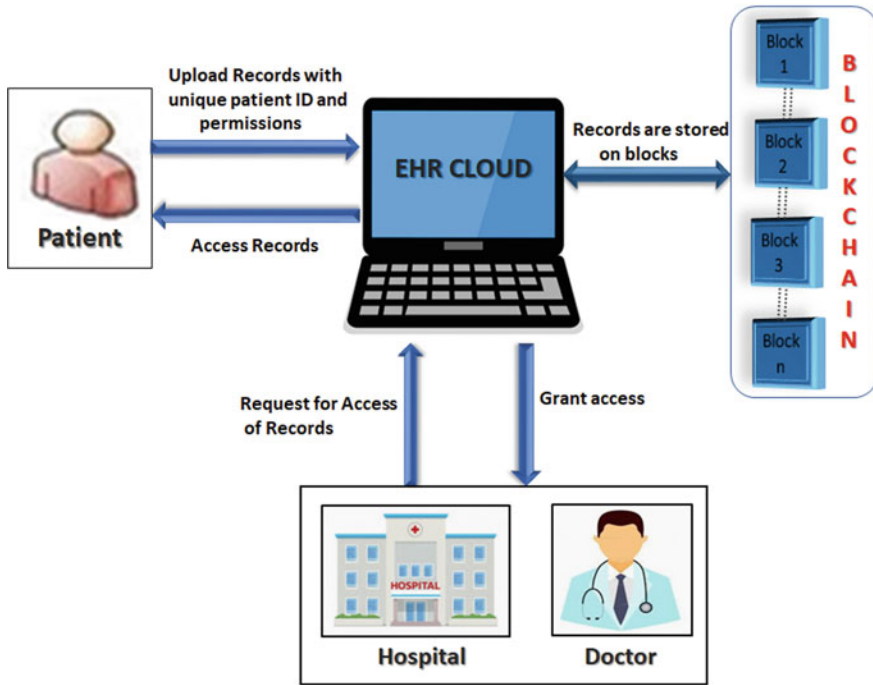
Fig. 2 Blockchain-based decentralized EHR system

5.1 Blockchain Background

The inauguration of Digital currency was introduced by Satoshi Nakamoto in 2007 [12]. Blockchain technology has a great contribution to every sector as well as many aspects of our lives [13]. This technology provides a large platform for constantly growing ledger which keeps a permanent record of all the transaction in a secure, consecutive and static [13]. This juncture uses a distributed system that allows the information to be spread and that every cycle of particular data or usually identified data have shared belonging. Blockchain innovation breaks the twofold go through the issue with the assistance of public-key cryptography, where every client has relegated a private key and a public key is imparted to any remaining clients [14]. This benefit provides a reasonable substitute for the patient's clinical storage subsequently, on the grounds that the advanced expansion of social administration's commerce focused the safety for the patient's clinical data on a prior basis.

Figure 3 clarifies the universal blockchain measure for exchange in which the sender can make an exchange of a square. This square of exchange is approved through cryptographic hashing. Additional, this conveyed diced exchange is submitted and remunerated by excavators and moved to the recipient.
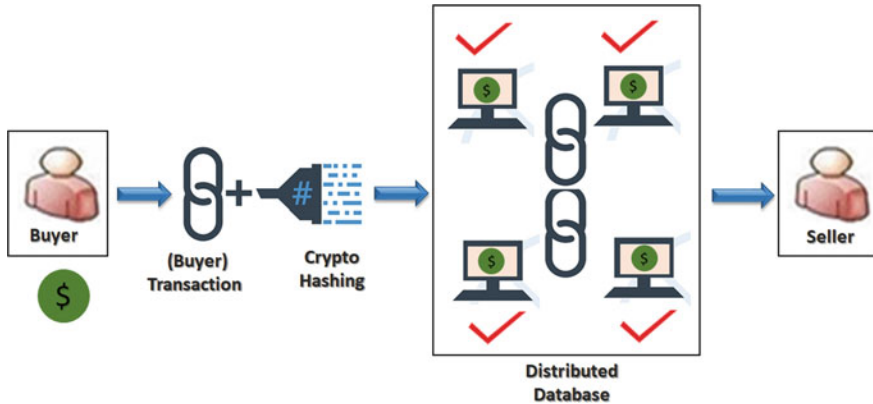
Fig. 3 Blockchain process

5.2　Flow of the System

Figure 4 characterizes the progression of the framework which has three principal sections are Patient, Admin, Doctor and Hospital. The operational progression of the proposed framework alongside these sections is as per the following:

1. Creating a clinical specialist's profile is the first task of the admin and for that, the admin needs to login into the system himself.
2. In the beginning, patient must register to the system and then proceed to login.
3. After entering the system, the patient generates his / her identification through a unique medical ID.
4. At this moment data uploading takes place and the patient is ready to upload its clinical and personal information.
5. A special security facility is available to the patient and according to that patient restricts the record access.
6. Hospital staff and doctor can search patient by using their unique medical id and for this first, they have to enter into the system through login.
7. Patient's records can be accessed by the doctor and hospital once it is approved by the patient.
8. Once permission is granted by the patient for accessing records, then only documents can be viewed by a doctor and hospital.

5.3　System Architecture

A protected admittance EHR system is a storage platform where vital information of the patient is uploaded to the cloud. Data Uploading and data sharing are important processes executed by this system. E-medical care records may consolidate singular information along with therapeutic data of patients provided by them. A patient able
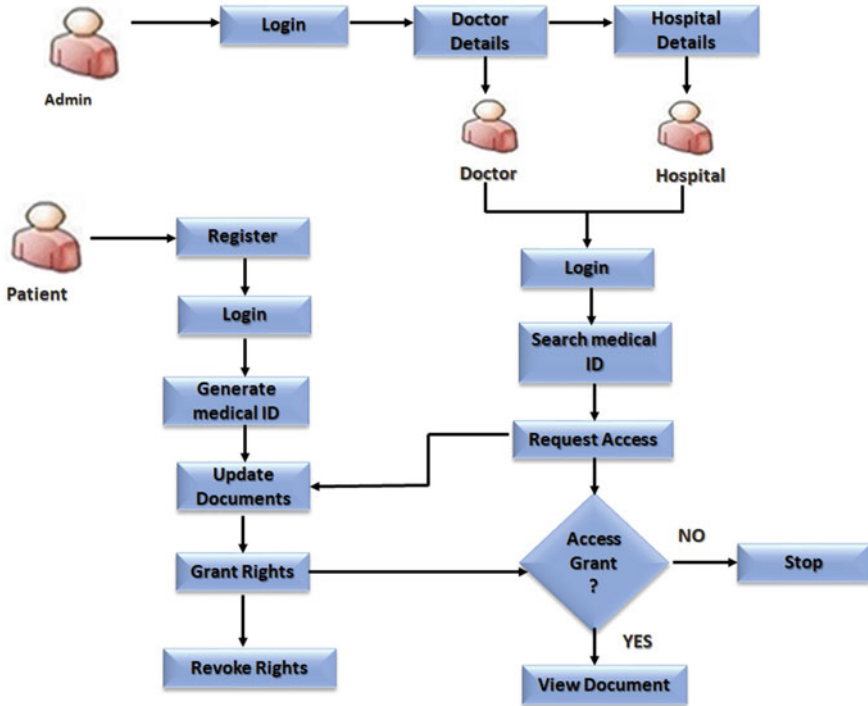
Fig. 4 System Flow

to create their own remarkable clinical ID also they have a special facility to restrict admittance of their histories for health sectors.

As shown in Fig. 5. The entire system is divided into two major parts are data uploading and data sharing.

Data Uploading

In this blockchain-based decentralized system, patients play the chief role in uploading their own vital information on the cloud as well as they can generate a unique medical ID as their identity [15]. Separate blocks are created for an individual patient and generated unique id is linked with the blockchain [16]. Each block of blockchain enclosed with its own Block hash value, previous block hash value, patient ID, and time stamp.

Data Sharing

Data exchange is a crucial part of this system, which facilitates easy access for patients to their own data. Data sharing is done by the following important modules:

Admin: Admin is a mastermind behind exchanges and procedures on the cloud. An administrator is careful to send adroit agreements and the primary component with the ability to invigorate or change game plans in sharp agreements [16].
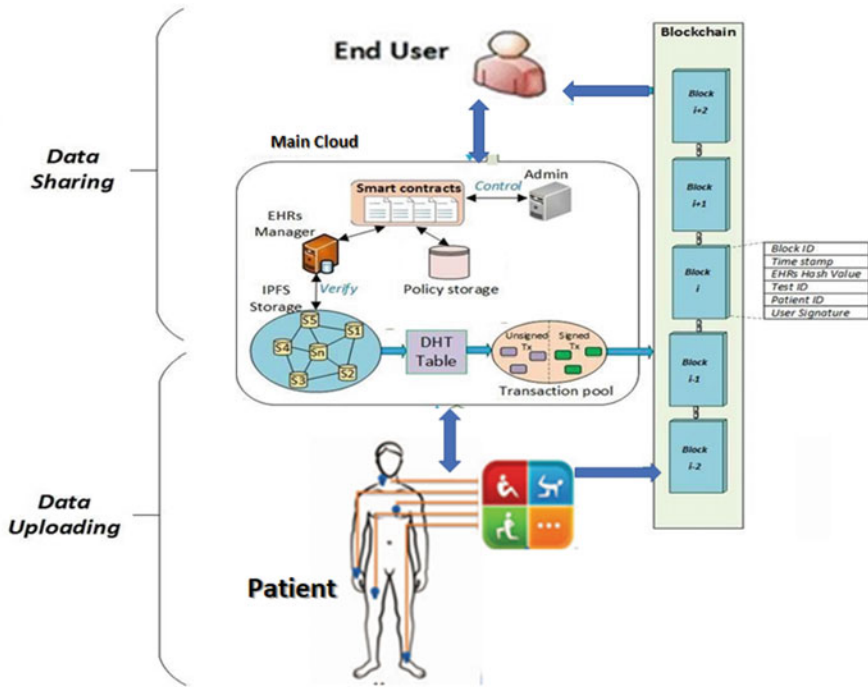
Fig. 5 System structure

EHRs manager: In this system information sharing is a chief constituent. The EHR manager contributes major efforts to control all customer trades on the blockchain [16]. The organization of EHRs overseer is engaged by quick agreements through demanding customer systems.

Smart contracts: They indicate all exercises acceptable in the passage regulator structure. Customers can interface with sharp arrangements by understanding location [17]. A canny arrangement can perceive, affirm sales and grant get to approvals for medical customers by enacting trades [17]. The quick arrangement and its exercises are available to all blockchain components (Fig. 6).

SHA 256 Algorithm
To avail secure hash bits, National Institute of Standards & Technology invented uniques algorithm called as SHA—Secure Hash Algorithm, and now a days hashing done with their latest version SHA-256 The key procedure is given in the name of this algorithm, and accordingly this algorithm calculates the hash length of 256 bits which is very remarkable [18]. The principle behind this is the input value is at the end added to the output and that it transforms an encryption algorithm into a "hashing" algorithm, a building piece of a standard hash function. The underlying block cipher has 64 rounds and thus a 2048-bit expanded internal key (64×32 bits).
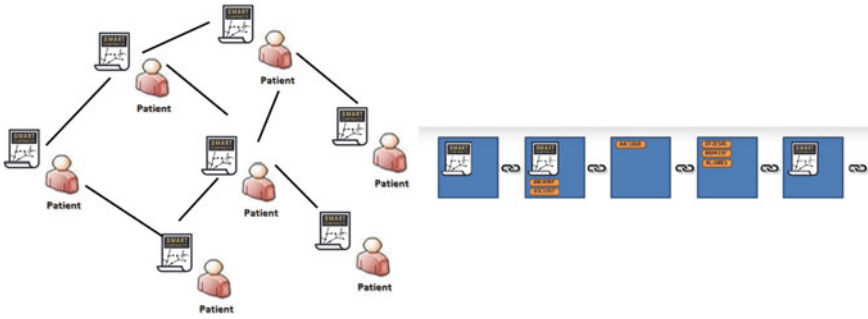
Fig. 6 Smart contracts

This key is obtained from the message block to be compressed, which has 512 bits at the input and is expanded four times to form this 2048-bit internal key for our block cipher. The SHA-256 algorithm is divided into two stages: pre-processing and hash computation [18]. Pre-processing involves padding a message and parsing the padded message into m-blocks. Initialization values are set which is to be used in the hash computation. Hash computation produces a message plan from the cushioned message. The yield hash esteem produced by hash computation is used to decide the message digest. Hash computation includes message plan, functions, capacities, and word activities that are created iteratively to get hash esteem. Security of SHA-256 hash calculation based on the amount of the hash value.

Interplanetary File System
An interplanetary file system is a show which usages conveyed framework for data amassing. It gives secure data storing as data set aside on this file system is shielded from every variation [19]. It uses a cryptographic identifier that protects the data from the change as any undertaking to make a change on the data set aside on IPFS should be done by altering the identifier.

Figure 7 represents the part of the interplanetary file system stockpiling for the blockchain-based system. As this file system is a distributed convention any place each data stores a bunch of diced documents checked by EHR director through shrewd agreement strategy [19]. IPFS is a non-centralized convention that monitors the substance-based tending. When hash esteem produced for the explicit data, that confused data alongside novel key is moved to the conveyed hash table (Fig. 8).

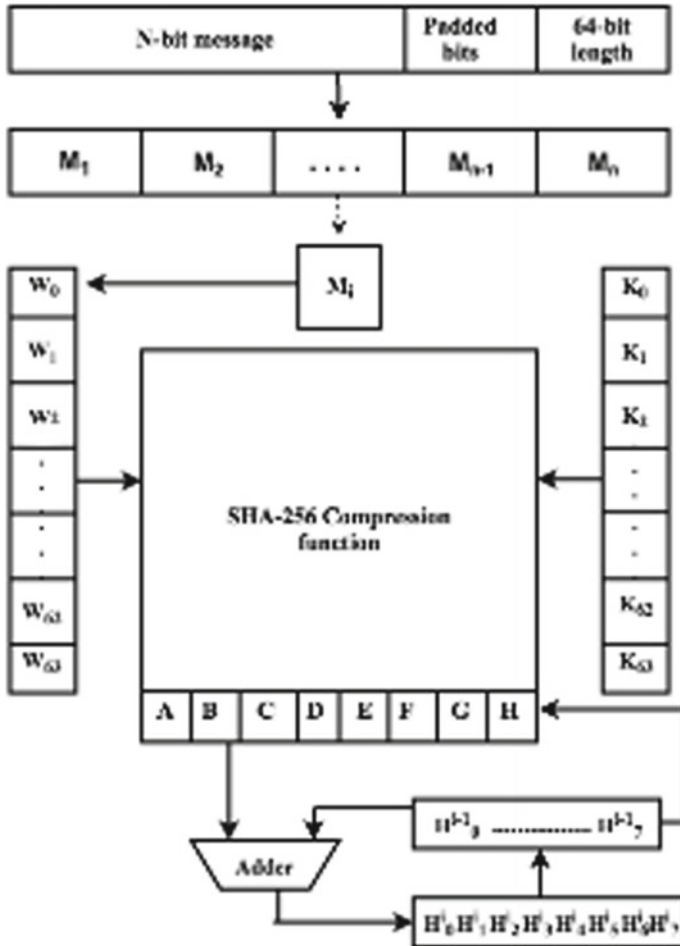**System Screenshots**
See Figs. 9, 10, 11, 12 and 13.

Fig. 7 Processing of SHA 256

6 Result Analysis

Due to its idiosyncratic properties, it has been proven that a decentralized EHR system gives much better performance than a centralized system. According to decentralization, patients have become free birds. They can handle their records anytime and most importantly easily. The security of a patient's vital and personal information with the help of blockchain technology is inevitable but this ease has created a puzzle and that is scalability. These systems got successes to solve generate code by using the off-chain database with the help of IPFS. According to this methodology, all the documents related to the patient's medical history are stored in off-chain databases

Fig. 8 IPFS process

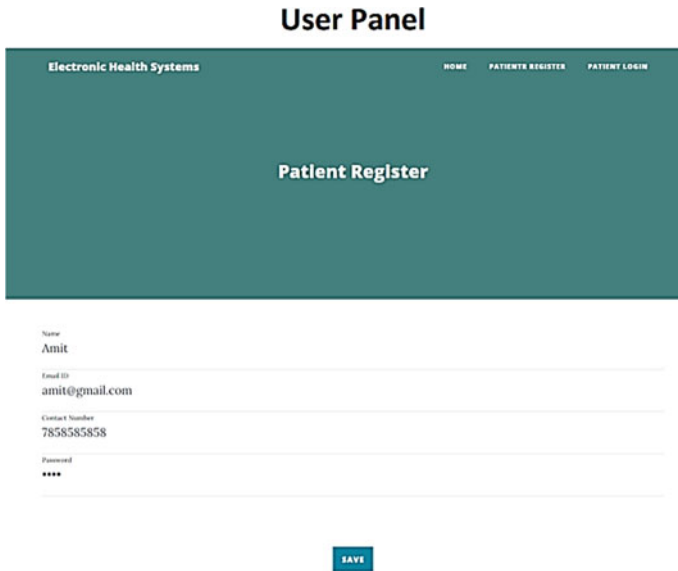**Fig. 9** Doctor/Hospital registration panel

Fig. 10 Patient registration panel

instead of blockchain so that the scalability of the system is enlarged by the attractive number of Percentage. Figure 14 clarifies the comparison between centralized health record system and decentralized health record system on the basis of various characteristics (Table 1).

7 Conclusion

This age in the field of technology is evolving day by day so much that a new invention is becoming very popular where patients became landlord of their record process. For given system, the patient holds decision-maker degree who took all decisions related to data sharing and processing. Provision of high-level security for patients records and avert data leakage is the highest attainment of the system. This milestone achieved by using blockchain technology which fulfils the security aspects. Storing all the vital information of patients in distributed ledger is a very crucial function that blockchain methodology contributes completely to the performance. The system provides fully protected data for the authorized user. In any event, when the patient visits any clinical foundation like an emergency clinic, the patient should throw the clinical id, entire evidence that hospital on the patient's clinical id which can be gotten to anyplace. SHA 256 has an important contribution to this system in order to supply a secure hash value. A 256-bit hash value is the key point of this system. Furthermore, the construction offers procedures to ensure the system can take care

Fig. 11 Data uploading

Fig. 12 Data sharing (Grant Access)
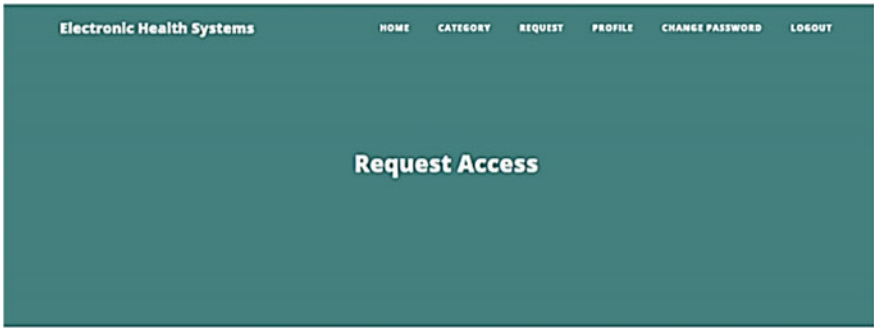
SR.NO	Category Name	Description	Access	Cancel Access
1	Medical	demo M	Access	Cancel Access
2	Pharma	Demo	Access	Cancel Access

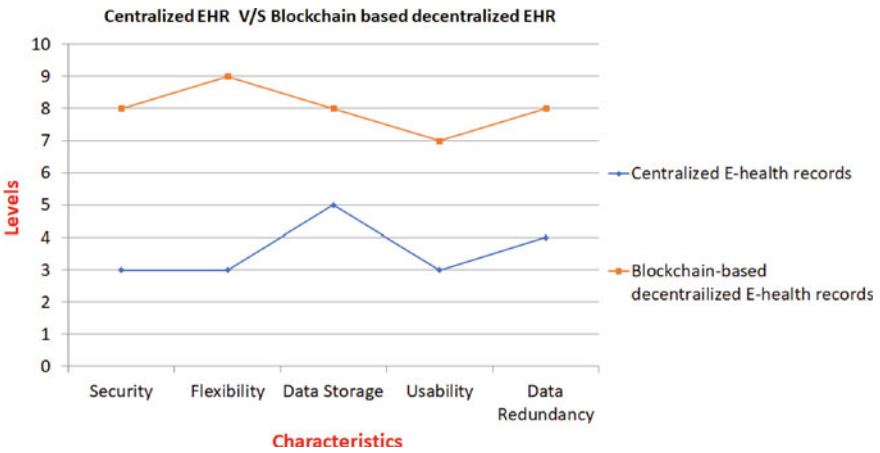**Fig. 13** Data sharing (Cancle Access)

Fig. 14 Centralized EHRs versus blockchain-based decentralized EHRs

Table 1 Performance characteristics of centralized EHRs and decentralized EHRs

Characteristics	Centralized E-health records	Blockchain-based decentralized E-health records
Security	3	8
Flexibility	3	9
Data storage	5	8
Usability	3	7
Data redundancy	4	8

of the concern of data storing as it utilizes the off-chain accumulating part of IPFS. This outlook also passes on a clever arrangement, like a puzzle, which executes on its own when both the social events agree on the course of action of shows. Patients are able to upload insurance-related documents along with medical documents but the insurance claim settlement process is still pending. Given structure is a purely web-oriented system and due to this sometimes causes a delay in permission granting process. A mobile-based application would be a great way to avoid this delay.

References

1. Radhakrishnan, B.L., Joseph, A.S., Sudhakar, S.: Securing blockchain based electronic health record using multilevel authentication. In: International Conference on Advanced Computing & Communication Systems (ICACCS), 2019
2. Shahnaz, A., Qamar, U., Member, IEEE, Khalid, A., Member, IEEE: Using Blockchain for Electronic Health Records. IEEE, 2019
3. Jetley, G., Zhang, H.: Electronic health records in IS research: quality issues, essential thresholds and remedial actions. Decis. Support Syst. **126**, 113–137 (2019)
4. Harshini, V.M., Danai, S., Usha, H.R., Kounte, M.R.: Health Record Management through Blockchain Technology. IEEE (2019)
5. Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., He, J.: BlocHIE: a BLOCkchain-based platform for Healthcare Information Exchange. In: 2018 IEEE International Conference on Smart Computing (SMARTCOMP)
6. Wisner, K., Lyndon, A., Chesla, C.A.: The electronic health record's impact on nurses' cognitive work: an integrative review. Int. J. Nursing Stud. **94**, 74–84 (2019)
7. Akbari, E., Zhao, W.: The impact of block parameters on the throughput and security of blockchains. In: ICBCT'20: Proceedings of the 2020 the 2nd International Conference on Blockchain Technology, Mar 2020
8. Bardhan, I.R., Thouin, M.F.: Health information technology and its impact on the quality and cost of healthcare delivery. Decis. Support Syst. **55**(2), 438–449 (2013)
9. Mikula, T., Jacobsen, R.H.: Identity and Access Management with Blockchain in Electronic Healthcare Records. IEEE (2018)
10. Cirstea, A., Enescu, F.M., Bizon, N., Stirbu, C., Ionescu, V.M.: Blockchain technology applied in health. In: ECAI 2018—International Conference—10th Edition Electronics, Computers and Artificial Intelligence, 2018
11. Pramod, P., Tripathy, P.K., Bajpai, H., Kounte, M.R.: Role of natural language processing and deep learning in intelligent machines. In: IEEE International Conference on Electrical, Communication, Electronics, Instrumentation and Computing (ICECEIC), Kanchipuram, India, 30–31 Jan 2019
12. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electrnic Cash System (2008)
13. Vivekanadam, B.: Analysis of recent trend and applications in block chain technology. J. ISMAC **2**(04), 200–206 (2020)
14. Koczkodaj, W.W., Mazurek, M., Strzałka, D., Wolny-Dominiak, A., Woodbury-Smith, M.: Electronic health record breaches as social indicators. Soc. Ind. Res. **141**(2), 861–871 (2019)

15. Spatar, D., Kok, O., Basoglu, N., Daim, T.: Adoption factors of electronic health record systems. Technol. Soc. **58** (2019)
16. Nguyen, D.C., Pathirana, P.N., Senior Member, IEEE, Ding, M., Senior Member, IEEE, Seneviratne, A., Senior Member, IEEE: Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems (2019)
17. Novikov, S.P., Kazakov, O.D., Kulagina, N.A., Azarenko, N.Y.: Blockchain and smart contracts in a decentralized health infrastructure. In: 2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (ITQMIS), pp. 697–703. IEEE (2018)
18. Gilbert, H., Handschuh, H.: Security Analysis of SHA-256 and Sisters. France Telecom R&D, FTRD/DTL/SSR 38–40 Rue du General Leclerc, F-92131
19. Zheng, Q., Li, Y., Chen, P., Dong, X.: An innovative IPFS-based storage model for blockchain. In: An Innovative IPFS-Based Storage Model for Blockchain. 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI) (2018). https://doi.org/10.1109/wi.2018.000-8