Secure Medical Records System using Block Chain Technology

Nirmal M. Chhodvadiya[1], Kaushik M. Rakholiya[2], Vaman B. Bhuvani[3], Mr. Hemang. J. Shah[4]

[1, 2, 3]Student, Dept of Computer Engineering, R. N. G. Patel Institute of Technology, Gujrat, India
[4]Professor, Dept. of Computer Engineering, R. N. G. Patel Institute of Technology, Gujrat, India
---***---

ABSTRACT:- *The healthcare industry has been at the cutting edge of technology since time immemorial. Hardware, software, medication, surgical procedures; As with respect to present scenario in the real world in Medical Domain, advancement in terms of treatments given to patient has reached to a high level. For a maintaining record of patients Electronics Health Records (EHR) systems are widely used in hospitals and primary care centres but it is usually difficult to share information and to collect patient data for clinical research. This is partly due to the different proprietary information models and inconsistent data quality. The main goal is to empower patients to be the center of their own health record so that, the patient doesn't have to rely on different institutions or hospitals they might visit. Blockchain technology and smart contracts provide an interesting and innovative way to keep track of Electronic Health Records (EHRs). This technology could help the patients to have better control of their own data. In the present article, we discuss how blockchain technologies can be used to handle EHR while improving the efficiency of operations through streamlining processes and transparency. We propose an architecture to manage and share healthcare data among different organizations. The proposed work could significantly reduce the time needed to share patient data among different health organizations and reduce the overall cost.*

KEYWORDS: Blockchain, Healthcare, EHR

1.INTRODUCTION

Healthcare processes are highly collaborative and various people from different disciplines must work together to enhance the quality of care. Achievement of this goal has been revolutionized through the use of computer-based methods. For instance, electronic health record (EHR) is commonly used, replacing paper health record with digital one. EHR can improve the quality of care and also reduce costs [1].

Electronic health record (EHR) systems are a type of health information technology (HIT) that has been widely proposed as a mechanism for improving the quality and positive impact of health care services [2]. Research suggests that well-implemented and fully-integrated EHR systems can promote complete record-keeping and more efficient access to documentation, facilitating information sharing and better coordination of care [3].

EHR systems are widely used in hospitals and primary care centres but it is usually difficult to share information and to collect patient data for clinical research. This is partly due to the different proprietary information models and inconsistent data quality [4].

An EHR system includes (1) longitudinal collection of electronic health information for and about persons, where health information is defined as information pertaining to the health of an individual or health care provided to an individual; (2) immediate electronic access to person- and population-level information by authorized, and only authorized, users; (3) provision of knowledge and decision-support that enhance the quality, safety, and efficiency of patient care; and (4) support of efficient processes for health care delivery. Critical building blocks of an EHR system are the electronic health records (EHR) maintained by providers...and by individuals (also called personal health records) [5].

An EHR with Blockchain that allows patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship [6].

This paper includes implementation methods for Electronic health record (EHR) systems using Blockchain technology, and smart contracts, could help in some typical scenarios related to data access, data management and data interoperability for the specific healthcare domain.

2. BLOCKCHAIN METHODOLOGIES FOR ELECTRONIC HEALTH RECORD

This section first discusses some nontechnical aspects that make health data sensible and how blockchain can enable data interoperability and privacy. Then, describes the process flow used by blockchain to handle medical data, discuss and analyse the usability of our software implementation and finally discuss some implementations challenges.

2.1 Limitation of current EHR and Blockchain Solutions

The state of health care records is currently unconnected due to lack of common architectures and standards that would allow the safe transfer of sensitive information among stakeholders [6]. Patient access permissions to the current EHRs are very limited, and patients are typically unable to easily share their data with researchers or providers. Despite all the advances in medicine, different EHR systems do not communicate effectively. The primary means of transferring healthcare data from one health institution to another are still through fax machines and snail mail. Each health care institution provides services, tracks, and updates the patient's clinical information set each time a medical service is provided. This information includes personal data, such as the patient's gender and date of birth, as well as information on the specific service provided, such as the procedure performed, the care plan. Those information's are usually stored in a database within the organization or within a defined network of health care stakeholders. This flow of information originating from the patient through the health care organization each time a service is performed should not stop at the individual organizational level or at the health care network only. Instead, that information representing each patient interaction should be directed into a nationwide blockchain transaction layer. Thus, information stored on the blockchain could be universally available to a specific individual through the blockchain private key. The private key enables patients to share their information with different health care organizations more seamlessly. Health care information's are sensible data that must be kept in secret. Thus, each health organization's EHR system must implement privacy policies in order to ensure that only the patient and the healthcare Blockchain. Agents, who have explicitly granted permission by the patient, can have access to personal health records.

2.2 Process Flow

The process flow of a blockchain transaction can be summarized in four main steps as shown in figure 1.

Step-1 Patient and doctor register by providing name and age on interface

Step-2 Patient uploads files and provides random nounce to encrypt the file, file will be uploaded to IPFS and secret is stored in ethereum

Step-3 Patient provides access to particular doctor Once doctor is given access by patient, he will be able to see patient's address in his home page.

Step-4 Doctor can get all files ipfs hash of patient and send request to node app for file view.

Step-5 Node app will fetch file from ipfs and get secret from blockchain, decrypt file and send it to doctor Thus, data remains non-identifiable to those without the key.
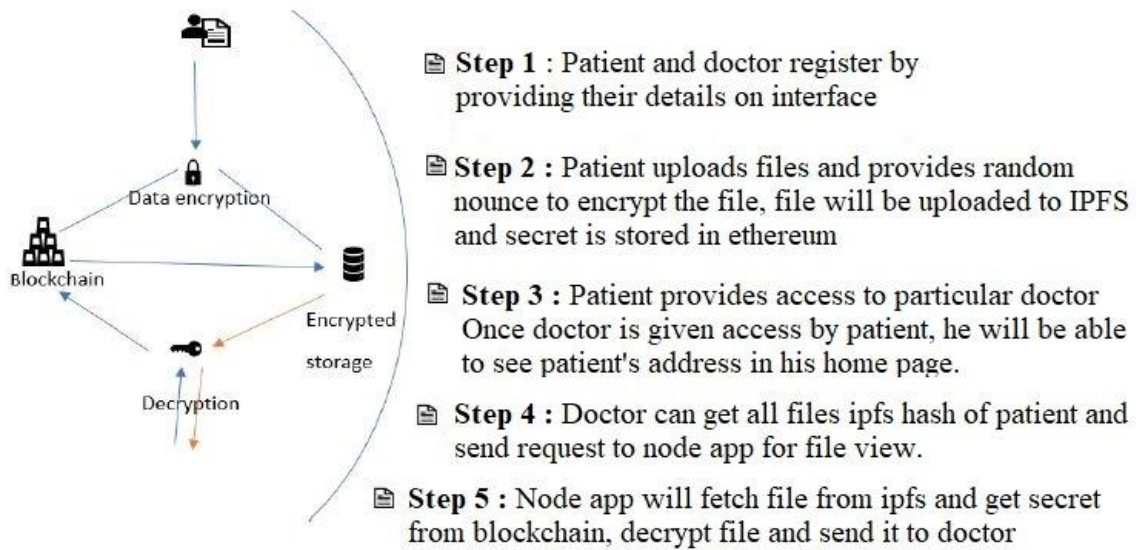
Step 1 : Patient and doctor register by providing their details on interface

Step 2 : Patient uploads files and provides random nounce to encrypt the file, file will be uploaded to IPFS and secret is stored in ethereum

Step 3 : Patient provides access to particular doctor Once doctor is given access by patient, he will be able to see patient's address in his home page.

Step 4 : Doctor can get all files ipfs hash of patient and send request to node app for file view.

Step 5 : Node app will fetch file from ipfs and get secret from blockchain, decrypt file and send it to doctor

Figure 1: Basic Blockchain's process flow

2.3 System Implementation

2.3.1 Background

At its core, a blockchain is a distributed system that record and stores transaction. More specifically, it is a shared and immutable record of peer-to-peer transactions built from linked transaction blocks and stored in a block. Record are linked together and can provide the entire history or provenance of an asset. Each record is also encrypted to provide an extra layer of security.

Blockchain was originally intended to timestamp digital document so it is not possible to backdate them. In a healthcare context, transactions would consist of the documentation of specific healthcare services provided. The patients would encrypt the data, which would reference a patient ID, to a hybrid blockchain.

Blockchain uses an established cryptographic technique to allow each participant in a network to interact (e.g. store, exchange, and view information), without existing trust between the parties. Blockchain system does not provide central authority; instead, transaction records are saved and distributed across all network participants.

2.3.2 System Architecture

Blockchain technology utilizes computer science technique such as (linked lists, distributed networking) as well as cryptographic primitives such as (hashing, digital signatures, public/private keys) mixed with financial concepts such as ledgers [7]. In the blockchain technology, the centralized infrastructure is replaced with a distributed one. Blockchain software runs on thousands of nodes distributed across the entire network. When a new transaction arrives, it is distributed to all the network nodes, when all the nodes have reached a consensus to accept the new transaction into the common ledger, the transaction is added to the ledger. As the name indicates, a blockchain is a chain of blocks that contain information. It contains:

 A hash: used to uniquely identify a block. Even the smallest change of input (e.g., a single bit) will result in a completely different output [7]. The blockchain technology takes a list of transactions and creates a hash "fingerprint" for the list. Anyone with the same list of transactions will generate the exact same fingerprint. If a single value in a transaction within the list changes, the fingerprint for that block changes. A block also contains the hash of the previous block.

A transaction: It is a recording of an assets (consist of documentation of specific healthcare services provided) [8]. An ID or a hash is generated for that specific transaction as a unique identifier. To validate the transaction, it is signed with a public/private key pair. Each transaction is assigned a block that cannot be altered unless the other blocks in the chain are altered. The transaction should include a digital signature of the contributor to trace the provenance of data. After the documents are stored in the blockchain, the patient would use a web-based or mobile application to view their blockchain contents and to grant or revoke access to specific parties.

Address: It is a short, alphanumeric string derived from the user's public key. It uses a hash function, along with some additional data. Addresses are not secret and are shorter than the public keys. They are used to send and receive digital assets [7]. They are generated by taking a public key, hashing it, and

converting the hash to text. Addresses represent the public-facing "identity" on a blockchain for a user. When a transaction is added to the blockchain, it is assigned an address. The wallet software can also calculate the total number of transactions a user may have. It contains the patient's identification to a blockchain. It could be a web-based or mobile application used by the patient to view their blockchain contents and to grant or revoke access to specific stakeholder [8].

2.4 Implementation Analysis and Usability

Blockchain technology is a distributed system and should, therefore, involve many participants. To use blockchain technology in healthcare industry, the health organization and other record keeping systems would encrypt the data and send them into the public healthcare blockchain as one transaction (containing patient care data, encounter notes, prescriptions, family histories, etc.). After the documents are stored on the blockchain, the patients would use a web-based or mobile application generally call wallets to view their blockchain contents and to grant or revoke access to specific parties. this technique will facilitate the process of collecting old patient data and reduce the cost of transactions.

To ensure security and trusted access to the patient's data, the ledger component could be implemented using the Ethereum platform. Ethereum uses the proof of work consensus algorithm and its peer-to-peer protocol to secure the state-machine and transition logic from tamping and to share information with all nodes participating in the system. Ethereum is a decentralized platform that runs smart contracts. Smart contracts are programs written in solidity and stored in the blockchain and can be executed in a virtual machine. They are responsible to store a new transaction in the block, to receive and process requests to access, and to grant. Its development should minimize the possibilities of exposure of sensitive data. The users must create or have an Ethereum account prior to any transaction. Our basic smart contract implementation will define the following types of methods New Record: Used to create and store a new record containing the patient's information including his address. This address will be used to retrieve the data Request access: Create by the institution to request the content owned by a patient Granted access: Create by a patient in response to the request access Modify record: Create by the institution to update a patient's record

Our implemented system currently running on the test Network, allows a doctor to store new patient's information on the blockchain, allow a doctor to see or update patient's information stored on the blockchain, give or revoke access to any doctor who wishes to access patients' information. Figure 4 shows a basic interface that can be used by a patient to grant access to a doctor with an Ethereum account. and figure 6 shows a basic interface that can be used by a doctor to retrieve the patient's data. the doctor must first check if he has access before doing any further action on a patient's record.
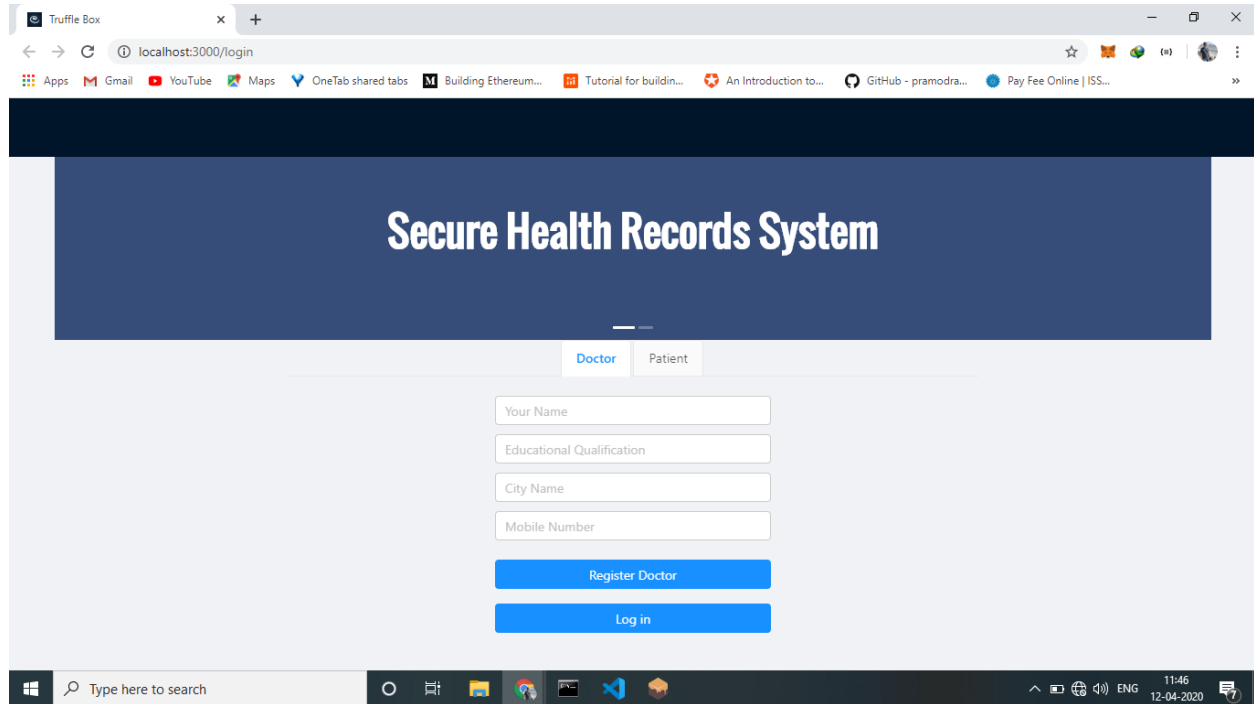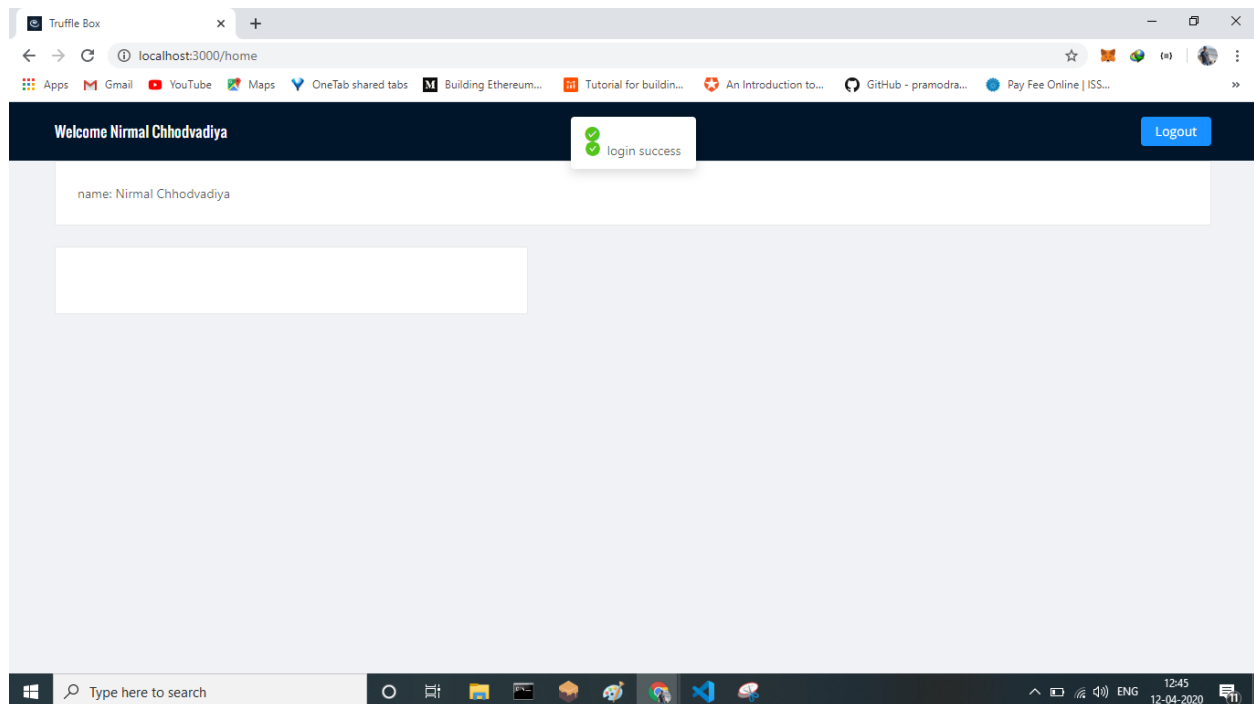
Figure 2: Doctor Registration

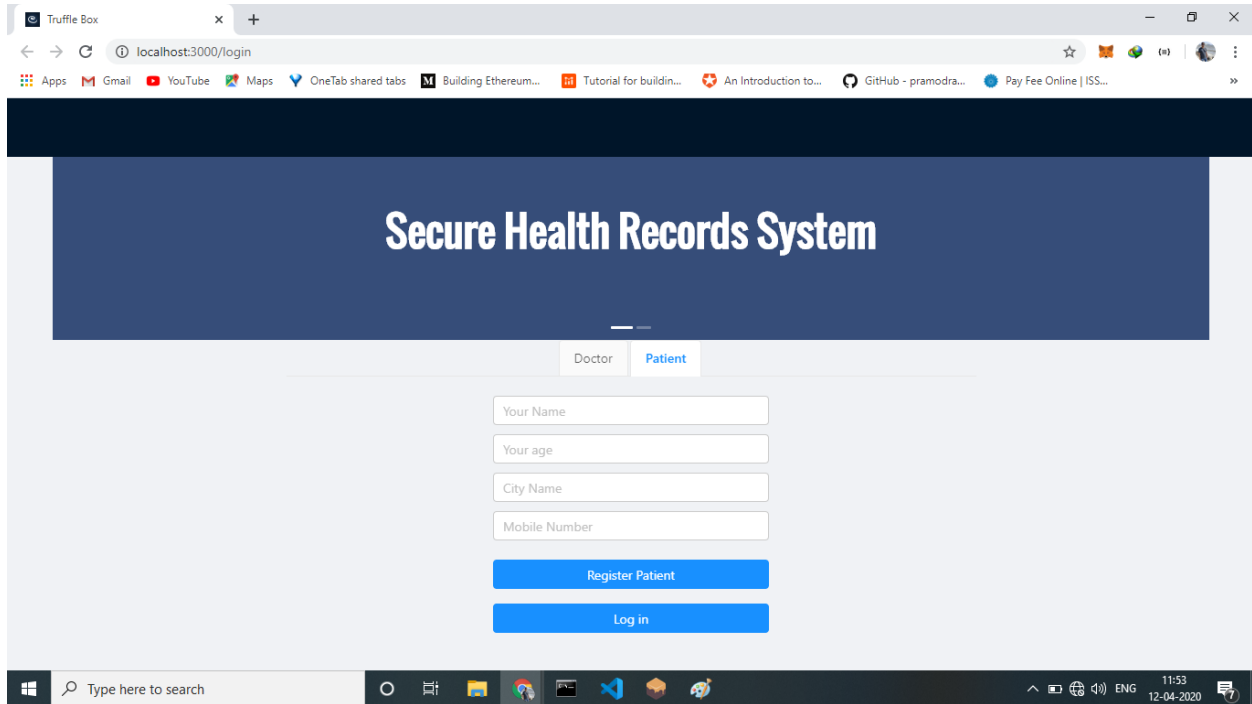**Figure 3: Doctor Login Successful (Doctor Profile)**

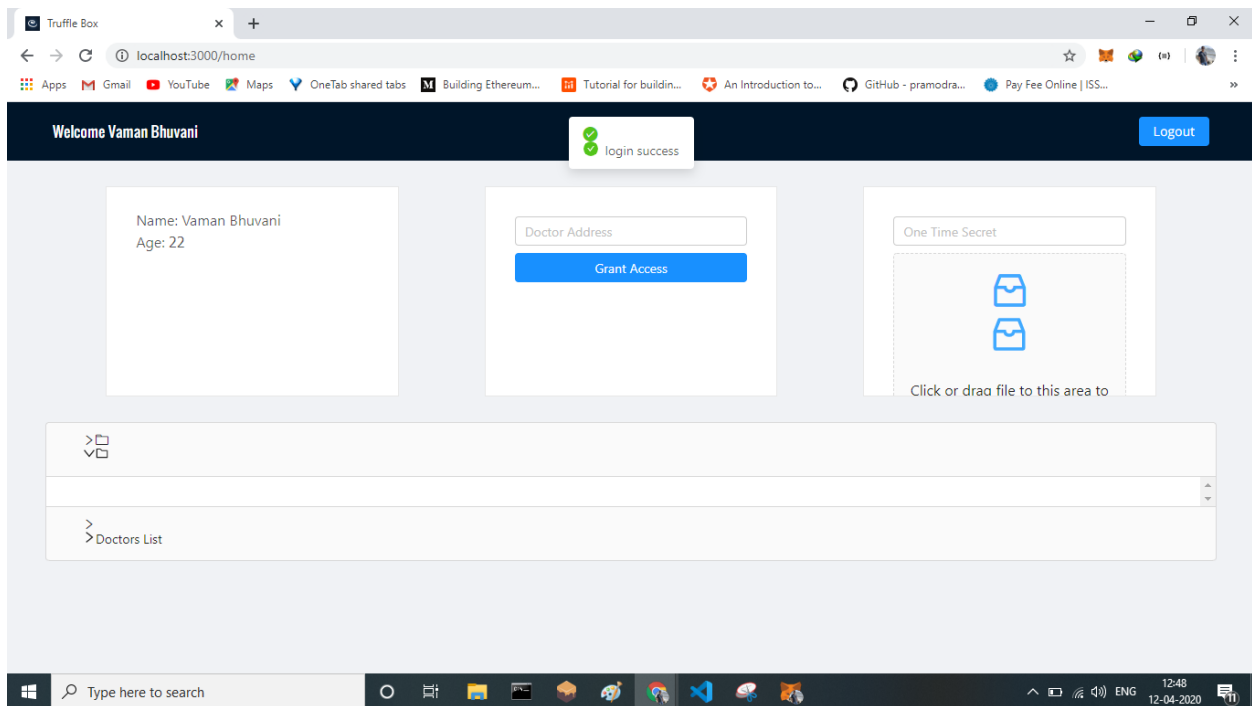**Figure 4: Patient Registration**

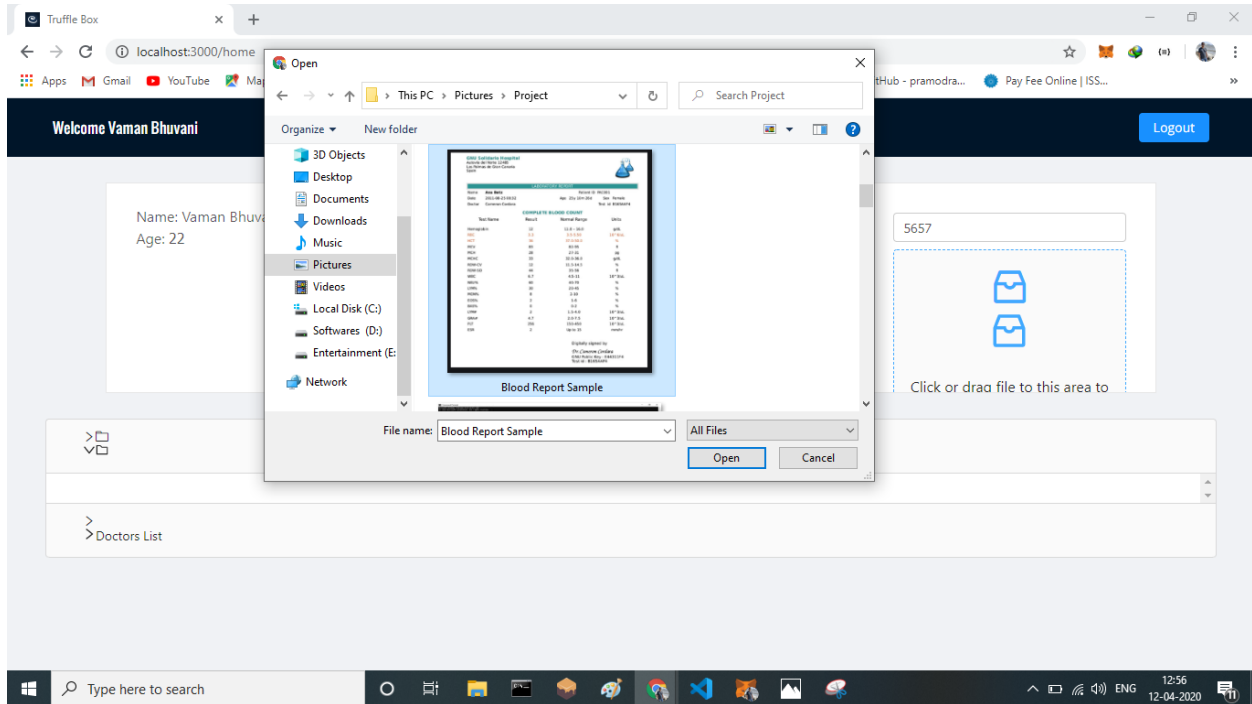**Figure 5: Patient Login Successful (Patient Profile)**

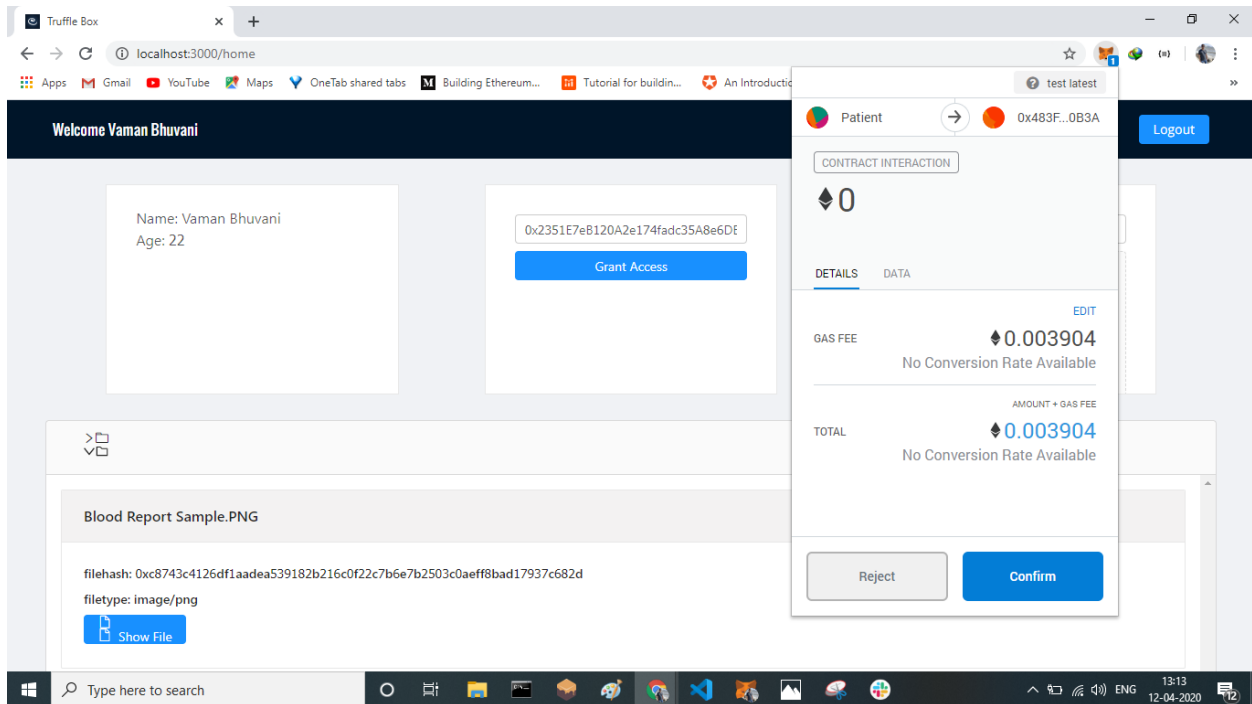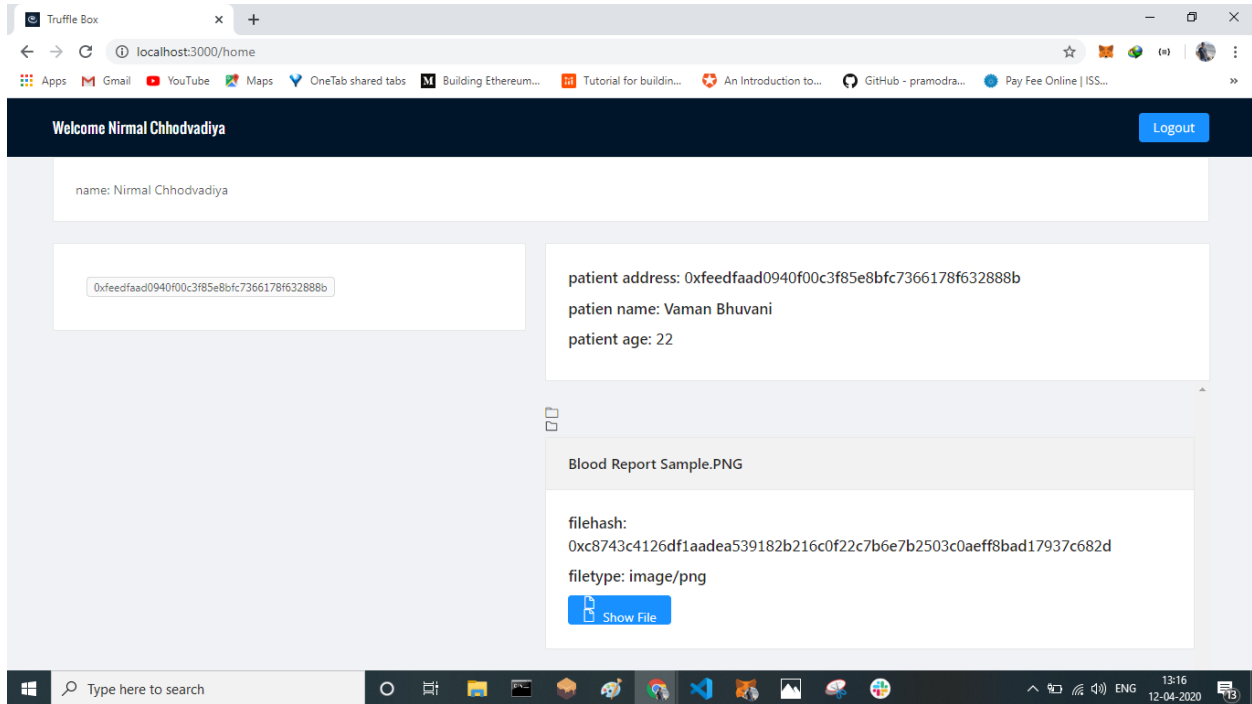**Figure 6: Patient Blood Report Upload Process**

Figure 7: Grant Access Process (transaction confirmation)

Figure 8: Patient Details with Health Record (Blood Report)

2.5 Implementation Challenges

Despite the numerous opportunities offered by blockchain to improve the current EHR system management, there are also concerns about it that are still preventing its widespread adoption. Several technics and organization challenges must be addressed before it can be adopted by health care organization nationwide.

Scalability constraints: Compromises between transaction volume and available computing power. In the case of Permissioned blockchains, they can expedite the transaction processing times, but they may face computing power constraints due to reduced participation in the network. For example, In the health care landscape where the United States Department of Health and Human Services (HHS) operates, The HHS could supply the computing power necessary to process all blockchain transactions on one permissioned network for select participants; however, this would result in HHS being the relative owner of the blockchain. A nationwide blockchain, with many health care participants, would make the system not only more interoperable, but it would also make it more secure.

Data standardization and scope: Organizations must consider what information is stored in or out of the blockchain. For health care blockchain, the most immediate concern is the size of information stored on the blockchain. A form submission of data to the blockchain, such as doctor notes, could create unnecessarily large transaction sizes that could adversely impact the performance of the blockchain. The blockchain can be efficiently operable with a specific and confined set of data, such as demographic information, medical history, and codes for services rendered. Thus, to standardize data stored on the blockchain, organizations should align on a framework for defining what data, size, and format can be submitted. Participants can also privatize the blockchain to restrict access.

Costs of operating blockchain technology: While blockchain technology enables faster, near-real-time transactions, the cost of operating such a system are still unclear. Health institutions spend a lot of time and money to set up and manage traditional information systems and data exchanges. This requires resources to continuously troubleshoot issues, update field parameters, perform backup and recovery measures. Blockchain's open-source technology and its distributed nature can help reduce the cost of these operations. Once the blockchain and its smart contracts are configured, the parameters become

absolute and reduce the need for frequent updates and troubleshooting. Moreover, the blockchain's transparent information structure could reduce many data exchange integration points and time-consuming reporting activities.

Integration with Legacy Systems: In order to make the move to a blockchain-based system, the organization must either completely overhaul their previous system or find a way to integrate their existing system with the blockchain solution. However, it may be difficult for blockchain solutions to handle all functions needed by organizations, making it difficult to completely eradicate legacy systems. Therefore, considerable changes must be made to the existing systems in order to facilitate a smooth transition. This process may take a significant amount of time, funds and human expertise.

3. ADVANTAGES

1. With an electronic health records initiative, many medical providers have created online portals. These portals allow patients to access their medical records whenever they wish, as long as they have a secure data or internet connection.

2. EHR allows every patient to reference a treatment plan or understand how their doctor sees their current state of health at any time.

3. When a patient portal is introduced with an EHR system, it can be setup so that patients can input their own data directly into their records. They can enter their data directly into their file days, if not weeks, before their scheduled visit. It saves them time and it saves time on the administrative work by the medical provider.

4. With an EHR system, doctors can immediately place orders for imaging or laboratory work.

5. An electronic order can be sent directly to the pharmacy of choice for a patient.

6. Medical providers have access to all patient data immediately with an electronic health record.

7. EHRs have eliminated the physical transporting, sifting and filing of charts, making data available at all times.

8. With an EHR system fewer storage costs and demands as compared to paper work and file system.

9. The electronic health record stores them all in a standardized format, it is much easier to skim through directly for the information more relevant to your queries at the time.

10. An electronic health record system often provides an online patients' portal that they can use to access their medical history and information wherever and whenever they wish.

11. Online EHR systems can be much safer, since they are stored on a database that you require the right login details to access.

12. Computerized notes are often easier to read than a physician's handwriting. This reduces the risk of errors and misinterpretations that can negatively impact the quality of patient care.

13. Medical and office staff no longer have to waste time sorting through cumbersome paper records. Users can access electronic health records quickly and efficiently with just a few strokes on a keyboard.

14. An effective EMR platform allows you to spend more meaningful time with your patients during a visit. In just a few clicks, you'll have a patient's medical history, lab results, current treatment plan, and previous medical notes at your fingertips.

15. Securely sharing electronic information with patients and other clinicians.

16. Enabling safer, more reliable prescribing.

4. DISADVANTAGES

1. Ransom ware attacks initiated through malware and other security access problems on electronic health record servers, cost numerous hospitals thousands of dollars per incident.

2. Like any software solution, an electronic health record platform must receive regular updates so that it can perform as needed.

3. EHR must be updated on a regular basis.

4. When the doctor forgets the electronic device, then gaps of information may begin to appear in the patient record.

5. Electronic health record systems are not cheap.

6. Lack of interoperability between electronic health records (EHRs).

7. Cost of set-up and maintenance of electronic health records (EHRs) is often a deterrent.

8. EHRs actually increase the physician workload. With written notes, documentation tended to be briefer and straight to the point. With EHRs, much more documentation is required of physicians before, during and after a patient visit.

9. With EHRs, there are no give-and-take conversations or question-and-answer scenarios.

10. For every task large or small — whether it's a basic wellness visit, a diagnosis, a procedure, a treatment or a prescription — the EHR system requires a corresponding update.

11. EHRs allow for easier access to sensitive information, there is an increased risk of privacy violations.

12. Many EHR systems allow for auto-population of data for new records. While these shortcuts save some time and effort on behalf of the physician, they can also result in inaccurate new records if the previous auto-populated record is not current.

13. It takes time due to factor in the preliminary research like determining budget and deciding which features need as well as the time spend doing product demos and negotiating with vendors to building electronic health records system (EHRs).

14. With EHR Cyber security issues like medical staff must be trained in basic digital security to ensure they do not leave their stations vulnerable to unauthorized access. Having patient's data fall into the wrong hands is not acceptable.

5.CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we discuss how blockchain technology can be used to handle EHR (Electronic Health Record) and we propose an architecture that could be used to improve the current EHR, as well as the challenges behind its widespread adoption. We chose the Ethereum framework to implement the proposed scenarios. It is clear from these analyses That, a medical record is the most comprehensive record about the identity of a person and must be handle in a secure manner. Because blockchain encrypted information cannot be modified or deleted, it ensures complete integrity and security of medical records from day one of its use. Thus, to enable trusted access to medical data, patients would be place at the centre of their healthcare data and could grant or revoke access to any other institution who needs to access their information. The blockchain and distributed infrastructure technology are exciting developments that show promise in the healthcare industry. It should be a part of the strategic design for the business process modernization of an institution who worried about issues of security, interoperability, and privacy. Therefore, as medical information is comprised of medical records, images, documents and lab reports which require a significant amount of storage space. Conceptually, every member included in the chain would have a complete copy of the full medical record of every individual and this volume could potentially exceed the storage capacity of current blockchain technology. In the future, we plan to further strengthen the design of the interface application with login access to allow easy and trusted user interaction, add pointer to get patient's data from the provider database, deploy on the main Ethereum and investigate on the storage capability of the blockchain.

6. REFERENCES

[1] Bleich, H.L. and W.V. Slack, Reflections on electronic medical records: When doctors will use them and when they will not. International Journal of Medical Informatics, 2010. 79(1): p. 1-4.

[2] Chase HS, Mitrani LR, Lu GG, Fulgieri DJ. Early recognition of multiple sclerosis using natural language processing of the electronic health record. BMC Med Inform Decis Mak 2017 Feb 28;17(1):24

[3] Elias B, Barginere M, Berry PA, Selleck CS. Implementation of an electronic health records system within an interprofessional model of care. J Interprof Care 2015;29(6):551-554.

[4] Chen, R., Enberg, G. & Klein, G.O. BMC Med Inform Decis Mak (2007) 7: 10. https://doi.org/10.1186/1472-6947-7-10

[5] National Institutes of Health, Committee on Data Standards for Patient Safety. Key Capabilities of an Electronic Health Record System: Letter Report. Washington, DC: National Academies Press; 2003

[6] RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai;, "Blockchain: Opportunities for Health Care," Deloitte, 2016.

[7] Dylan Yaga, Nik Roby, Karen Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology, 2018.

[8] Ariel Ekblaw, Asaph Azaria, John D. Halamka, MD, Andrew Lippman, ""MedRec" Prototype for electronic health record and medical reseach data," White paper, 2016.