Patient Data Management Using Blockchain

Bharath H[*], Rahul N[*], Shylash S[*], Vinny Pious[**]

*Department of Computer Science and Engineering, Mar Baselios College of Engineering and Technology, Kerala Technological University, Kerala, India
[**] Assistant Professor, Department of Computer Science and Engineering, Mar Baselios College of Engineering and Technology, Kerala Technological University, Kerala, India

DOI: 10.29322/IJSRP.10.07.2020.p10339
http://dx.doi.org/10.29322/IJSRP.10.07.2020.p10339

Abstract- The conventional system of patient-data management has several issues. The system includes information being stored as unstructured records presented as paper prescriptions, files and other traditional forms of storage. All the important data pertaining to the patient is stored by the centralized hospital authorities or the concerned medical practitioners. Reproducibility of this data when it comes to second – opinions or for the judgment of medical history, is a mammoth task. Even if there is a disease which is common, the treatment will mostly be not common for each individual as there should be considered the fact that there is a certain level of uniqueness with each patient. If a treatment strategy works on one patient, that does not mean it will work for all because there will be differences between each patient. Thus, the entire medical record history should be accessed so as to give the treatment which is best suited for the particular individual. Commonly, when a patient visits a new doctor, the doctor might recommend performing tests that have been previously performed. This might be because the proof of the previously conducted test cannot be produced as the test results might have been lost. This project deals with how Blockchain can be used to beat the odds faced by the conventional centralized system that greatly lacks interoperability. With the help of Blockchain, the patient's data can be managed into a single record owned by the patient. The patient's details pertaining to all healthcare services he/she has received will be managed into an easily accessible format for use anytime and anywhere. The project also deals with other aspects improving the interaction between the application and the patient, such as, real-world token tracking for appointments, appointment booking and so on. With the help of Blockchain, the current system can be completely disrupted and revolutionized, allowing for better transparency and ownership of the sensitive data thereby promoting and transforming the healthcare industries.

Index Terms- Blockchain, Ethereum, Ganache, Transaction, Truffle.

I. INTRODUCTION

The traditional approach to managing health records have been and inconvenient since its dawn. The amount of effort, time and space used up by traditional health information management systems are so massive that there is a great sense of wonder as to why a better system has not been introduced and implemented on a large scale. There are additional problems associated with the traditional paper-based management which include redundancy, proneness to loss of record, and so on. The use of technology in Blockchain is the health industry has the potential to have finest utility of Blockchain, since it involves store, use and transfer of sensitive information pertaining to any individual. Surprisingly, there has been little to no works or experiments done on this field as it comes up with many difficulties like scalability and awareness. A distributed platform providing technology like Blockchain, if utilized in health sector, and utilized properly, can yield amazing results in many aspects. The basic idea of our product is to minimize the effort and to overcome the aforementioned difficulties by making use of electronic health records to store and maintain the health information of every person. For the secure storage and transmission of sensitive health information, the blockchain technology, which is currently on an upsurge, is used.

II. LITERATURE REVIEW

Blockchain is a relatively new technology, which was conceptualized only in 2008 by a person or a group of people by the name of Satoshi Nakamoto. So, as the concept is relatively new, most of the individuals and even organizations focus on the one standout feature presented by Blockchain technology, which is crypto currency. Bitcoins and other forms of crypto currencies are still worth a lot and many individuals and organizations are still looking to invest in those crypto currencies and make tremendous profit from them. Other aspects to Blockchain technology are not yet fully discovered. This review dwells into the field of management of medical records which are electronic and which have the primary oversight on the efficiency of the system during emergency and catastrophic situations. A major part of the literature is based on software frameworks and other techniques introduced prior to blockchain and its capabilities of smart contracts. With the introduction of the ability to represent complicated data on the chain with the help of a language that is Turing-complete helped start a new field of distribution and p2p mode of communication. After the introduction of Ethereum , new software-frameworks that can use and employ blockchain have been developed by academic institutions and the IT-industry. Electronic Health Records and Electronic Medical Records are not the same thing . These terms are sometimes interchanged, but there is a big difference in the records containing medical information, stored digitally. An electronic medical record is the digital or electronic equivalent of the paper-records maintained by a patient and the doctor. It contains the history of the patient and other diagnostic and treatment details. The first system to use blockchain for Health records used a modular method for the sake of integration purposes. For the sake of scalability, the actual records are stored off-chain which is the provider's RDB.

blockchain contains the meta-data and other location information. In simple terms , a smart contract manages all the interaction between the participants of the system and defines the access matrix or access rules and other data-pointers. The pointers will contain tuples along with a query that will run on both the machines of the provider and the host. The health record software is designed according to the protocols of the network designed as Ethereum and the public as well as the private keys will have to decide which parties (network participants who act as miners of the system) get the permission. This means that every participant must have a node associated to the blockchain for interacting with the network. The concerning drawback of this kind of system is that every participant has to maintain a copy of the data. The other drawback would be the scalability issues because of the consensus mechanism used. If the host does not specify any limit, it is still possible to put a maximum transaction count per second of sixty. The projects were completed by focusing on data-sharing, access-controls and integration mechanism.

The research also focused on the patient-side, on how to ensure security constraints in the patient-data while aggregating the system. The various frameworks and blockchain software's that have been developed so far can be categorized as two permissioned and the permissioned. In a permissioned network, since the participants know each there , it is possible to take advantage of the consensus mechanisms and any network interaction lag can be evaded from while also ensuring security, privacy and transparency. It is not associated to any cryptocurrency models, so the system does not need to be incentivized. This software-framework is most suitable for 2 or more organizations that know each other and want to transfer sensitive information.

III. PROPOSED APPROACH

Prior to the introduction of Blockchain and its Smart Contract-capabilities, the most widely discussed topic on Electronic Health Records was "How to store EMRs" whether to use a cloud based platform for storage or to use the localized systems itself. This meant centralization of information which indicated that every Health care Provider and hospital has to maintain all information pertaining to the patient records in their own premise that is the locally maintained storage and databases. The centralized model for storing patient record information has several issues associated with it, they are:

a. **Not patient-driven:** The patients do not have any control over the data as it is not owned by the patient. A patient's data should be owned and controlled by the respective patient. As all records are made and stored in the hospital or healthcare service provider, the data is not technically owned by the patient. In order to improve privacy and security one should own one's own healthcare data. A patient-centric model can disrupt the centralized manner of sensitive health care data storage.

b. **Scattering of records:** The manner in which a patient receives treatment can varied and in different structures and this might cause the replicating of records.

c. **Limitation in the interoperability of systems:** All hospitals and healthcare service providers have different systems and methods for storing data . This will lead to issues in the sharing and viewing of data between the different healthcare service providers . A particular hospital's system will only be equipped to view the details of that particular hospital. Patient transfers between hospitals may lead to redundant overheads.

d. **Inconvenient secure sharing:** The conventional ways and methods in which health care data is shared can be very complicated and time consuming . For example , Direct is an e-mail standard that allows physicians to transfer data via e-mail in a secure manner. It encrypts the transmission between the physician and the receiver.

The solutions brought forward seemed to solve a lot of the early specified issues, but they suffered some form of vulnerability which led to the search of a better solution in the centralized lines leaving some or the other drawbacks unsolved, such as privacy, data-ownership and transparency. Furthermore, in scenarios like a disaster, the centralized model seemed to really suffer as the response is generally disorganized and any harm to the central storage can leverage a lot of important data. Even though natural calamities are events that are rare, the field of healthcare can greatly be leveraged by them by means of replication and sharing of the concerned information, the network grows powerful in the lines of reliability and robustness even in cases of huge failures. Also, peer to peer networks can allow ownership of data because sensitive data can be requested and stored only to the concerned system-node. A multiple number of such nodes can improve the accessibility of the stored information. Anyhow, this task of achieving consensus while maintaining privacy , security and anonymity can be extremely challenging. Blockchain technology has made it possible to achieve all these challenges in addition to improving transparency and reliability. Blockchain is a structure that stores data in a singly linked list manner as a sequence where every block is connected to the following block forming a chain . Breaching such a system will require rechaining all the blocks while maintaining consensus which is close to impossible.

http://dx.doi.org/10.29322/IJSRP.10.07.2020.p10339

IV. DESIGN

1. *Ethereum*

Figure 1: Ethereum

Ethereum is the second largest platform for cryptocurrency, falling second to the bitcoin network. It is an open source and decentralized platform that provides the tools and requirements to build smart contracts. As reward for validating the transactions, the miners receive ether , which is the incentive of the system. Today, Ethereum is the platform for lakhs of cryptocurrencies, including three of the top leading cryptocurrencies.

Ethereum network contains an Ethereum virtual machine that compiles scripts using a network of nodes connected internationally. The network also uses an internal transaction unit called gas that is used to allocate resources on the network. Ethereum platform was developed by Vitalik Buterin who is a cryptocurrency-researcher. In 2016 due to an exploitation in the smart contract of the DAO project and the theft of millions of dollars, Ethereum split into two different blockchains - ETH and ETC. The ETH had the theft reversed while the ETC continued along the same lines. Proof Of Work and the Proof Of Stake are the most widely used consensus algorithms in Ethereum. The POS consensus algorithm checks to see if the participant has high enough stakes of the concerned currency - this is a drawback as it opens the door to Monopoly, but POS has its own way to control it which is selecting a random stake holder on subsequent rounds.

2. *Web3*

Figure 2: Web3

In order to communicate with the components in the chain, validations of the transactions should be done in chain. For a participant in the network of some other offline framework to create and validate a transaction, it has to relay it to the p2p network which is the underlying network. It also contains a library collection that facilitates the communication between the Ethereum nodes and the in-chain components .It is used in the server side for applications developed in Node.js.

It connects to the Ethereum network with the help of an Ethereum-node using an HTTP connection. This can be a node in the local system provided by Infura or HD wallet. The integration of Ethereum and the web application can be done using Metamask which is an in- browser extension that allows to operate from Ethereum accounts. Metamask is an Ethereum wallet present in the browser that introduces the browser to a Web3 provider object. A Web3 provider provides a link to Ethereum nodes which are publicly accessible and is also a data- structure. With the help of metamask, a user can use, store and manage public and private keys which is unique to the account. The combination of Ethereum, metamask and web3js along with a web interface makes back end- front end communication very easy.

3. *Ganache*

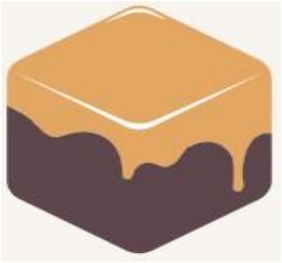


Figure 3: Ganache

Ganache is a local blockchain for the rapid development distributed applications on Ethereum. Ganache can be used throughout the development cycle so as to deploy, develop and test DAPPS in a deterministic and secure environment.

Ganache User Interface is desktop app that supports both: Ethereum and Corda technology. Ethereum is also available as a command line version : Ganche-cli.

4. *Truffle*

http://dx.doi.org/10.29322/IJSRP.10.07.2020.p10339

Figure 4: Truffle

It is a powerful developing environment for Ethereum Virtual Machine (EVM) using blockchains and also acts as an asset pipeline and a test network/framework to the same. This component provides the following:

- The compiling , linking and development of smart contracts and the maintenance of binary dependencies.
- Automated smart contract test environment.
- Scriptable, extensible deployment & migrations framework.
- Management of Packages.
- Communication with Contracts directly.
- Build pipeline which are configurable with tight integration support. Truffle environment to run scripts.

5. Smart Contract

The smart contract used in Medicare makes the project patient centric . The patient is able to make all decisions pertaining to which medical practitioner can view and edit the record. On the patient's end , there are 5 operations that correspond to the patient's record : Per missioning and Revoking of View and Write Permissions to the Medical practitioner .The record details added by the medical practitioner will be stored in the blockchain .This acts as proof of existence for the recorded data. Only a validated practitioner can add recorded data and not any other network participant. The smart contract specifies the functionality for the access control. Access to a patient's record can only be controlled by the patient.

6. Patient Flowchart

The patient's has mainly four operations to perform are:

a. **Give View Permission:** Permissions a Doctor/Practitioner to view the record. This function takes the doctor's Address as input which is shared to the patient offline. The address is unique to the practitioner which maps to the corresponding Ethereum account.

b. **Give Write Permission:** Permissions a Doctor/Practitioner to Write to the record. This function takes the doctor's Address as input which is shared to the patient offline. The address is unique to the practitioner which maps to the corresponding Ethereum account. Only a permissioned practitioner can write to the record.

c. **Revoke View Permission:** Revokes View permission from a practitioner who was earlier given permission to view the record, by the patient. Permission can only be revoked from a practitioner who had the View Permission already. The practitioner will no longer be a participant in the patient's private chain unless permissioned by the patient.

d. **Revoke Write Permission:** Revokes Write permission from a practitioner who was earlier given permission to write to the record, by the patient. Permission can only be revoked from a practitioner who had the Write Permission already. This function will deny the doctor/practitioner from adding any further record details to the patient's private chain. The practitioner will no longer be a participant in the patient's private chain unless permissioned by the patient.

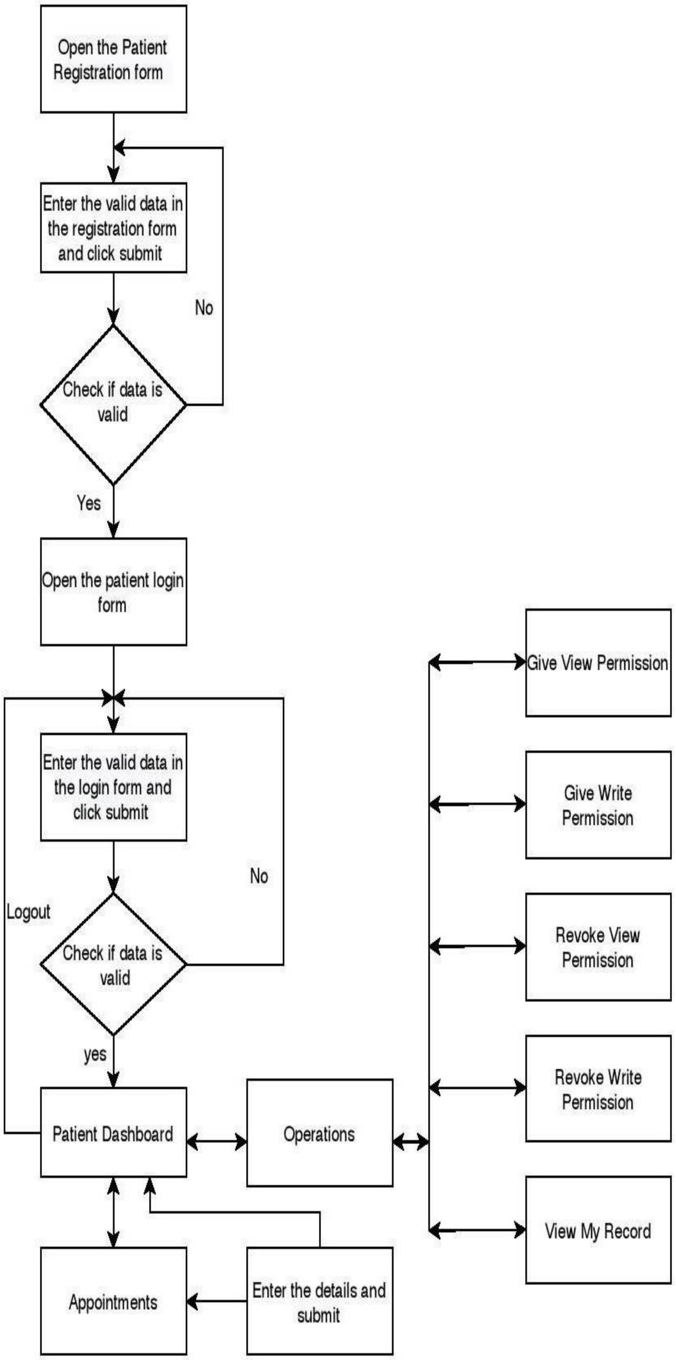
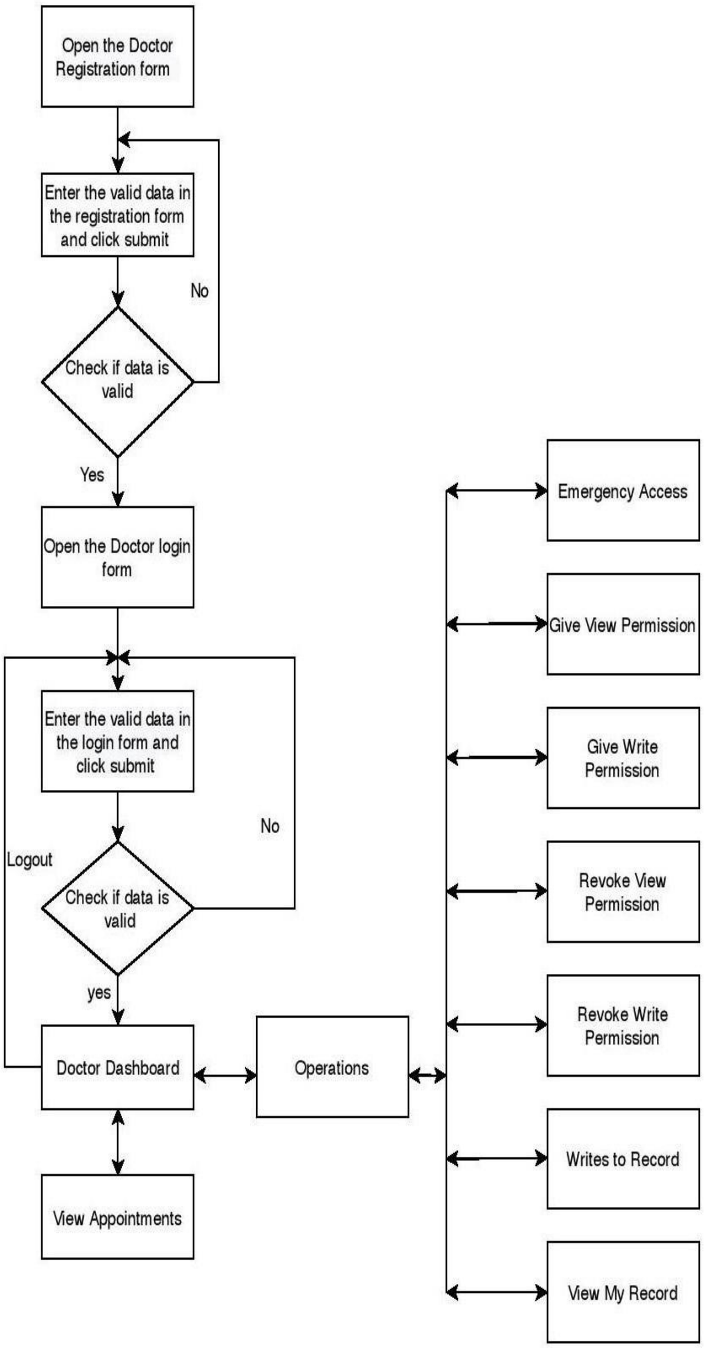

Open the Patient Registration form
Enter the valid data in the registration form and click submit
No
Check if data is valid
Yes
Open the patient login form
Enter the valid data in the login form and click submit
No
Logout
Check if data is valid
yes
Patient Dashboard
Operations
Appointments
Enter the details and submit
Give View Permission
Give Write Permission
Revoke View Permission
Revoke Write Permission
View My Record

Figure 5: Patient's Flowchart



7. Practitioner's Flowchart

Figure 6: Practitioner's Flowchart

The practitioner can also be a patient to another doctor/practitioner. Along with all the functions included in the patient-end , the practitioner has two additional functions are:

a. **Write to Record :** The practitioner can write to the patient's record. All this information will be stored in the private chain of the patient. A doctor can , at a time, be permissioned to multiple patient-accounts depending on the number of patient the doctor can tend to.

b. **Emergency Access:** In case of an emergency situation where the patient is incapacitated or for any other reason the patient is unable to provide view permission to the doctor , the doctor can invoke emergency access to view lifesaving and sensitive information about the permission that will help with the treatment of the patient. When such an access has been invoked , an alert will be sent to the patient's account which can be viewed by the patient whenever the patient is able to do so . The patient can then further authorize the permission or revoke it. If the access was illegitimate, the doctor's permission will be revoked by the patient and this can be used as proof for any law-proceedings.

10. Use Case

The use-case of this application has two main entities as actors, one is the patient and the other is the doctor. Now, it is to be noted that emergency access, which is a special feature given to the doctor is also included in the list of operations. Out of the seven of the list of operations, five can be accessed by the patient while the doctor has access to all of the seven operations. The operation which can bring a change in the block data once accessed is write to patient's record operation which can be done only by the doctor. Giving and revoking view or write permissions can affect the network in a way that changes the corresponding doctor's view of access to the corresponding operations. The Figure 7 represents the Use case diagram.

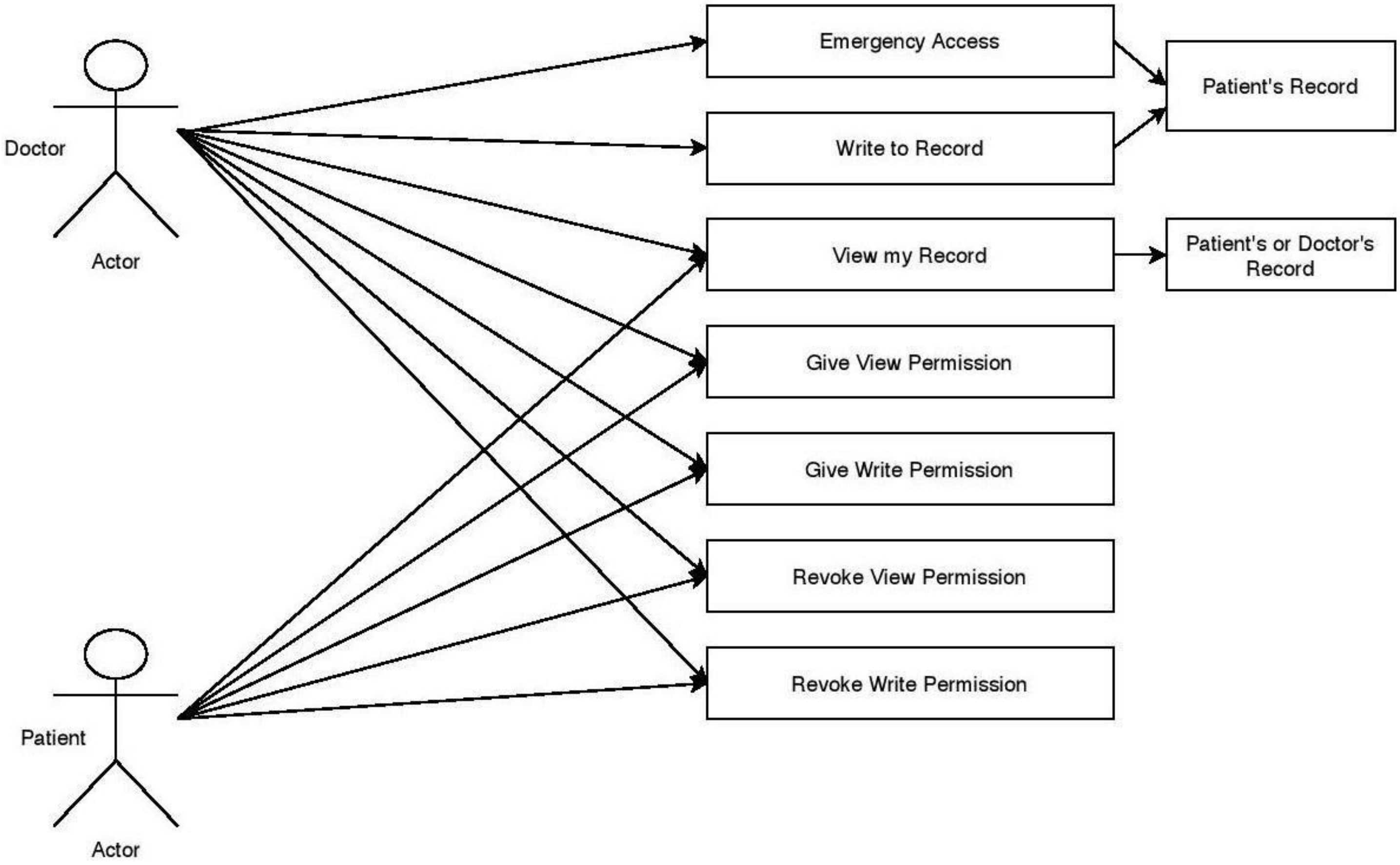


Figure 7: Use case

VI. CONCLUSION

The traditional system for maintaining the records in medical sector is difficult and it requires large space to store the results of medical test for all patients. In previously used systems the data is in unstructured manner and it is difficult to exchange the data. So, for solving the above issues we plan on implementing the given model for managing health records in block chain using Medicare.

The EHR using blockchain is a revolution in the medical industry. It solves most challenges which exist today just in the name of trust in the medical sector. It not only provides a reliable platform for patient data exchange, but also a faster and empowering system. The time and effort expended in managing patient data, can be greatly minimized using EHR with effective and efficient results.

REFERENCE

[1] Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) 2016 Aug;:25–30.

[2] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, “Secure and Trustable Electronic Medical Records Sharing Using Blockchain,” in AMIA (American Medical Informatics Association) Annual Symposium Proceedings ,2017

[3] Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” White Paper, 2008.

[4] Wood, “Ethereum: A secure decentralised generalized transaction ledger,” Ethereum Project Yellow Paper, 2014.

[5] The Office of the Nat. Coordinator for Health InformationTechnology, “Report on health information blocking,” U.S. Department of HHS, Tech. Rep., 2015.

[6] Health Information and the Law, “Who owns medialrecords: 50 state comparison,” 2015.

[7] Lu, Z.; Liu, W.; Wang, Q.; Qu, G.; Liu, Z. A Privacy-Preserving Trust Model Based on Blockchain for VANETs. IEEE Access 2018, 6, 45655–45664.

AUTHORS

First Author – Bharath H, Department of Computer Science and Engineering, Mar Baselios College of Engineering and Technology, Kerala Technological University, Kerala, India and bharathariharasubramoni@gmail.com.

Second Author – Rahul N, Department of Computer Science and Engineering, Mar Baselios College of Engineering and Technology, Kerala Technological University, Kerala, India and therahuln@gmail.com.

Third Author – Shylash S, Department of Computer Science and Engineering, Mar Baselios College of Engineering and Technology, Kerala Technological University, Kerala, India and shylashss@gmail.com.

Correspondence Author – Vinny Pious, Assistant Professor, Department of Computer Science and Engineering, Mar Baselios College of Engineering and Technology, Kerala , India, vinnypious243@gmail.com, 9048019355.