EasyChair Preprint

№ 14735

Blockchain Technology Enabled Secured Medical Records Management System[SMRMS]

Arpitha, T.A. Meghana and M. Dakshayini

September 6, 2024

Blockchain Technology Enabled Secured Medical Records Management System[SMRMS]

[1] [1] [1]
Arpitha , Meghana.T.A , M.Dakshayini
[1]

Dept of ISE, B.M.S.College of Engineering, Bangalore
Arpitha.scn22@bmsce.ac.in[1] Meghana.scn22@bmsce.ac.in[2]

Abstract. Medical record administration has gotten increasingly difficult in the growing digital context. Traditional record-keeping approaches frequently lack interoperability, security, and patientcentricity. Blockchain technology, which is known for being decentralized, immutable, and tamper-resistant, presents a promising answer to these difficulties in the field of medical records. This paper discusses the potential of blockchain technology in transforming medical record administration and implementing blockchain system to develop a secure and efficient environment for medical data management and storage. This is done by exploiting its inherent qualities such as transparency, data integrity, and cryptographic security. The results have proven the potential of blockchain technology in empowering patients with controlled access to their healthcare data and enabling seamless sharing among authorized parties across many healthcare settings.

Keywords: Medical Record, Block Chain, Smart Contract, Ethereum.

1 Introduction

In the world of growing digitalization, medical record management and security have arisen as key problems within the healthcare sector. Traditional methods of storing and transmitting medical information are frequently inefficient with the lack of interoperability and are vulnerable to data breaches[8]. As the demand for seamless and secure health data-sharing apps, creative solutions are needed to meet these difficulties properly. Blockchain technology, with its underlying principles of decentralization, immutability, and cryptographic security, has sparked much interest as a potentially disruptive tool in medical record administration.

This study lays the groundwork for investigating the integration of blockchain technology into the healthcare domain, with a particular emphasis on its application in medical record administration

Emphasizing on the limits that inhibit efficient data sharing, patient-centric care, and data security, this research[9]also explains blockchain technology and demonstrates

its key features and procedures that make it a suitable choice for tackling the listed concerns. Further, the introduction emphasizes the significance of secure medical record management not only for healthcare providers but also for patients seeking greater control over their health data. It highlights how blockchain adoption can empower patients by allowing them to grant access to their information while protecting data privacy and ownership. The essential features and procedures of blockchain technology make it a viable option for addressing the issues stated. Furthermore, blockchain technology is best suitable option for secure medical data record management not only for healthcare providers but also for patients who want more control over their health data. we demonstrate how blockchain adoption may empower patients by allowing them to authorize access to their data while maintaining data privacy and ownership.

The second section shows the study made towards the literature review. The methodology used for securing the patient's medical records is described in the third section. The fourth section goes into details of the proposed SMRMS. The fifth section describes the system implementation and the coding process in depth. The sixth chapter discusses and evaluates the results. The final chapter addresses the conclusion, discusses the innovations and contributions, and makes recommendations for further work.

2 Related Work

The utilization of blockchain technology to enhance the security and efficiency of medical record management has captured significant attention in both academic and industry domains. This literature survey delves into key research studies, projects, and initiatives that explore the application of blockchain in secure medical record management.

Alhaqbani et al.[1] have provided a comprehensive overview of blockchain applications, highlighting its patient-centric approach Xiang-Yang Li et al., in [2], underline the need for secure data sharing and address interoperability issues. PoHan Wu et al. [3] concentrate on improving data security and interoperability within healthcare systems. Kewei Zhang et al. investigate patient privacy while ensuring accessibility [4]. Oussama Al Rifai et al. present real-world examples in [5]. Yue Xue et al., in [6], go into actual implementation, with a focus on transparency and security. Finally, in [7], Xin Lou et al. highlight the importance of blockchain in tackling data security and interoperability challenges. These studies show how blockchain has the potential to change healthcare data management.

2.1 Motivation and Our Contribution

Need for Blockchain Technology in Medical Healthcare Record Management
After surveying the existing work, we felt that it is necessary to create a completely blockchain-enabled medical record management system that addresses the following critical issues identified after going through the related works:

- Mismatch or synchronization of patients' health records hurt the delivery of effective healthcare:
  Statistics suggest that one out of every five patient records is not accurately matched, even within the same healthcare system. When data is transmitted between healthcare systems, up to half of the patient records are incorrectly matched.

- Breach of patient's electronic medical records and private information privacy: Leakage of patient's electronic medical records is a common and dangerous issue in which patients' sensitive individual records are made available to others without the individual's knowledge or authority. When medical organizations sell customers' medical records to other for-profit firms, some records are intentionally leaked. Some medical record leaks are inadvertent, such as when hackers access and disclose medical records.

- Medical record systems are not intuitive, causing medical workers to spend a significant amount of time:
  According to a study of a community hospital emergency department (ED), clinicians spent 43% of their time entering data. Only 28% of clinicians have direct contact with patients.

- Bottlenecks in centralized medical record systems result in a single point of failure: A centralized medical record system is a vulnerable target for unscrupulous individuals who want to manipulate the health system to destabilize a country or steal and expose residents' health record details. This issue would result in the loss of all patient data and would disrupt the county's whole medical record system, costing the country millions of dollars. Furthermore, centralized medical record systems face the potential of a collapse and the loss of all data if the centralized database has problems, implying that a data wipe of the entire medical record system is a real possibility.

Hence, to address these issues related to medical records data, we propose a blockchain-enabled secured medical record management system[SMRMS]. Implement the same using blockchain-enabled tools and technologies.

3. METHODOLOGY

This work demonstrates the system developed to perform Secured Medical Record Management system SMRMS using blockchain technology. SMRMS is designed to keep track of patient health data and personal information for the totality of a patient's life. This information can be seamlessly shared among various hospitals, clinics, and healthcare providers ensuring each patient receives the appropriate prescriptions and treatments. SMRMS manages the highly sensitive patient information crucial for accurate diagnosis and treatment in hospitals. Therefore, the seamless and accurate sharing of healthcare data is of utmost importance, aiming to create an efficient and effective healthcare system.

Our innovation in the SMRMS involves the utilization of a public electronic ledger built upon a peer-to-peer system. This ledger acts as an immutable record of medical transactions, capable of being updated only when system stakeholders reach a consensus. Once new data is added to the blockchain, it becomes unalterable. This means that any attempt to change the health data within the blockchain would be immediately detected as tampering and would be visible to all stakeholders.

Our work is centered on enhancing the delivery of effective healthcare services. SMRMS addresses the risks of privacy breaches by granting users i.e. patients, doctors, and other stakeholders to take complete control over their medical records. Additionally, we prioritize improving the user interface and experience, reducing the time and effort required for entering or updating patient records. This holistic approach aims to transform and optimize the healthcare system for both patients and providers alike. To make SMRMS more effective, we have used the following methodologies.

3.1 BLOCKCHAIN

Blockchain technology is a sophisticated database approach that allows businesses to share information in a network in a transparent manner. It keeps data in blocks that are linked together in a blockchain database, maintaining chronological consistency by prohibiting chain deletion or modification without network consensus.

3.2 SMART CONTRACT

A smart contract is a self-executing digital contract that self-sufficiently enforces an agreement's terms and conditions when certain conditions are satisfied. It runs on a blockchain platform, allowing for the safe, tamper-proof, and transparent execution of contractual agreements without the use of intermediaries. Smart contracts have the potential to transform a wide range of sectors by automating procedures, lowering costs, and enhancing trust in commercial transactions.

3.3 METAMASK

MetaMask is a cryptocurrency wallet software that enables users to connect with the Ethereum network. Ganache is an Ethereum development tool that allows you to build a local blockchain network for testing and development purposes. It may be accessible via a browser extension or a mobile app. It allows you to replicate the behavior of a genuine Ethereum network without requiring network connectivity.

4. THE PROPOSED SMRM-System

The proposed SMRMS consists of various stakeholders like Patients, Doctors, Hospitals, and others who wish to access the patient's health records. Figure 1 shows the proposed Architecture of the SMRMS with all the modules and communication among these models with relevant functionalities.

- Patient Module:
    1. Allow patients to save demographic information such as their name, age, gender, address, and so on.
    2. Patients will be able to access a list of patients whose medical records have been saved.
    3. Patients will be able to look for a particular medical record.
    4. The user of the SMRM will be able to save medications and medication details, allowing them to keep track of and record their medication for doctors' use.
- Doctor Module:
    1. Doctors will be able to view a list of patients that have stored their medical records.
    2. Doctors will only be allowed to view the details of a patient's medical record after being permitted by the patient.
    3. Doctor will be able to search for a specific medical record from the SMRM
- Appointment Module:
    1. Doctors can set an appointment by setting appointment details like date, time, prescription, etc.
    2. Patients can view their appointments in their profile.
    3. The patient or doctor can update the appointment to change its status to completed.
- Grant and Revoke Access Module:
    1. Patients can be granted access to doctors to view their medical records.
    2. Patients can revoke access given to doctors or patients to view their medical records.

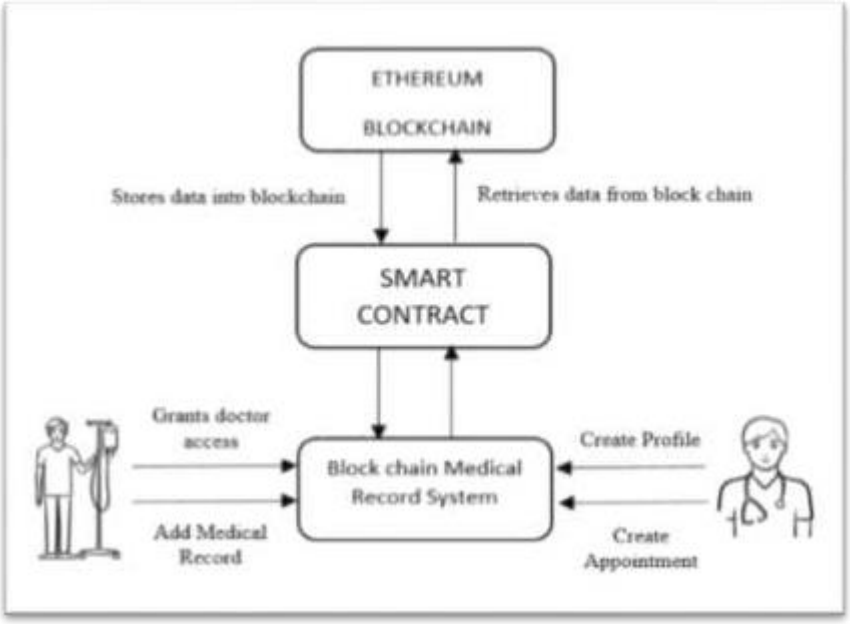

Fig 1: Shows the proposed Architecture of the SMRM

Figure 2 depicts the entities involved in building a secure blockchain-based medical record management within the Blockchain network[BCN].

5. ALGORITHM

The code is written in Solidity, a programming language specifically designed for smart contracts on the Ethereum blockchain. While the code represents the logic of the contract.

A flow diagram (3) shows the essential steps in handling medical information in a medical facility while ensuring data security, transparency, etc... User identification and access control come first, followed by features for patient registration, the creation, and updating of medical records, secure data storage, search, and many more as well as the capabilities of scheduling appointments, payment, and report generation.

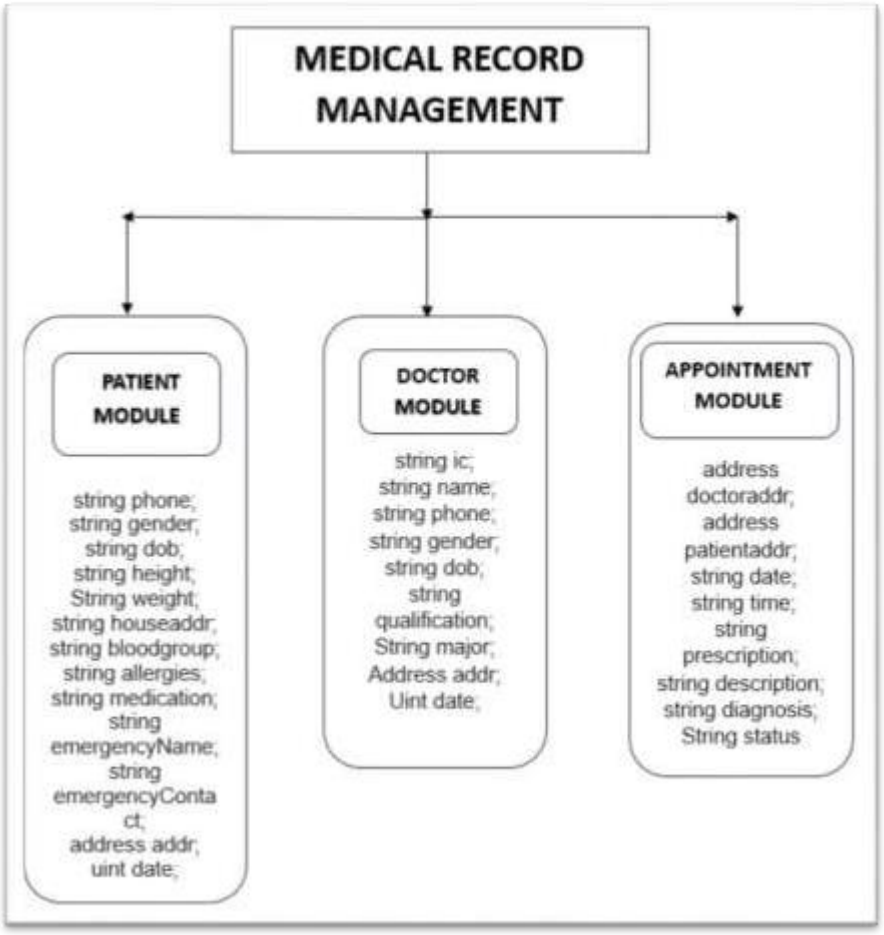

Fig 2: Shows the block diagram of SMRM

The above block diagram (2) shows three important modules that is patient module Doctor module and the appointment module. These three functions have their own parameters to build a Secured medical record management system.

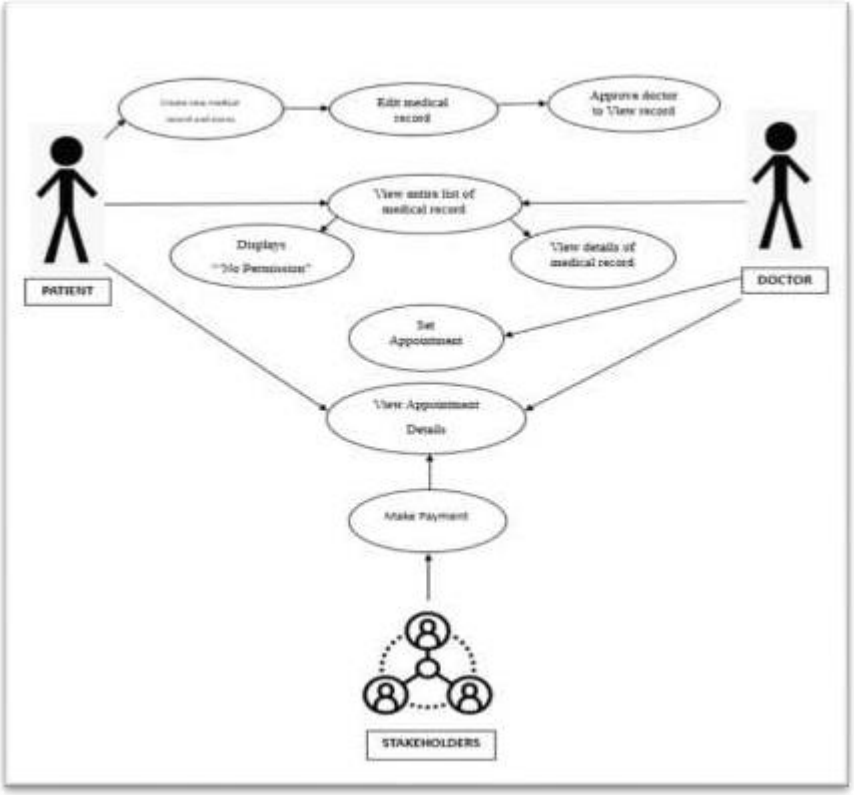

Fig 3: Secured Medical Record Management System flow diagram The steps involved in the key functions of this smart contract are:

1. Set Patient Details (`*setDetails*` function):

Whenever *SMRMS-BCN-Head* receives the request from a new patient for registration to the *SMRMS-BCN*, Head calls the *setDetails* function to check whether the requesting patient's public address/key[pu] is prest in the regitered listof patients[RP^{List}]. If not, *SMRMS-BCN-Head* assigns public[pu] and private keys[pr] for the new patient after verifying their aAadharnumber. Then create a new 'Patients 'sstructure andpopulate it with the provided patient details.A dd its pu a ts id in RP^{List}.Then Update the `*isPatient*` mapping to mark the sender's address as a registered patient. Also, Grant permission to the patient to access their own records.

Algorithm 1: *SMRMS-BCN* Patient Registration

1. Whenever *SMRMS-BCN-Head* receives a request from a new patient for registration,

2. For [k=1, k≤ L, k++]
3. call '*isPatient' SMRMS-BCN-Head* verfies for the P_k^{pu} in RP^{List}
4. if [$P_k^{pu} \notin RP^{List}$]
5. *SMRMS-BCN-Head* create a new Patient struct, add its $P_k{}^{pu}$ and populate it with the provided patient details in *SMRMS-BCN*.
6. Update the `*isPatient*` mapping to mark the New patient's id as a registered patient
7. Add P_k^{pu} to RP^{List}
8. Grant permission to the patient to access their own records
9. else
10. return the P^{pu}
11. endif
12. endfor

---

2. Edit Patient Details (`*editDetails*` function):

Whenever *SMRMS-BCN-Head* receives the request for editing the details of a patient, the *SMRMS-BCN*, Head calls *editDetails* function to verify the pu of the patient, Only if the private key of the patient matches then it permits access for the patient to edit the details and Updates on the `*isPatient*` maps to mark the sender's address as a registered patient. Also Grants permission to the patient to access their own records.

Algorithm 2: *SMRMS-BCT* Updating of Patients Registry

When ever *SMRMS-BCN-Head* receives the request from the new patient for registration,

1. For [k=1, k≤ L, k++]
2. call '*isPatient' SMRMS-BCN-Head* verifies for the P_k^{pu} in RP^{List}
3. if [$P_k{}^{pu} \notin RP^{List}$]
4. *SMRMS-BCN-Head* allows to *editdetails* struct of patient, add its P_k^{pu} and populate it with the provided patient details in *SMRMS-BCN*.
5. Update the `*isPatient*` mapping to mark the Updated patient's id as a registered patient
6. Grant permission to the patient to access their own records
7. else
8. return the P^{pu}
9. endif
10. endfor

---

3. Set Doctor Details (*setDoctor* function):

Whenever *SMRMS-BCN-Head* receives the request from the new doctor for registration to the *SMRMS-BCN*, Head calls *setDetails* function to check whether the requesting patient's public address/key[pu] is present in the registered list of Doctor[RD^{List}]. If not, *SMRMS-BCN-Head* assigns public[pu] and private keys[pr] for the new doctor after verifying their aAadharnumber. Then Create a new `Doctor` struct and populate it with the provided patient details. Add its pu as its id in RD^{List}.Then Update the `*setDoctor*` mapping to mark the sender's address as a registered doctor. Also, Grant permission to the doctor to access their own records.

Algorithm 3 : *SMRMS-BCN* Doctor Registration

1. Whenever *SMRMS-BCN-Head* receives the request from the new doctor for registration,
2. For [k=1, k≤ L, k++]
3. call '*setdoctor' SMRMS-BCN-Head* verifies for the D_k^{pu} in RD^{List}
4. if [$D_k^{pu} \notin RD^{List}$]
5. *SMRMS-BCN-Head* create a new Doctor struct, add its D_k^{pu} and populate it with the provided patient details in *SMRMS-BCN*.
6. Update the `*setDoctor*` mapping to mark the New doctors's id as a registered doctor
7. Add D_k^{pu} to RD^{List}
8. Grant permission to the doctor to access their own records
9. else
10. return the D^{pu}
11. endif
12. endfor

4. Edit Doctor Details (*editDoctor* function):

The *SMRMS-BCN-Head* receives the request for editing the details of the doctor, the *SMRMS-BCN*, Head calls *editDoctor* function checks with D_k^{pu} , only if the private key of the doctor matches then it permits access for the patients to edit the details then the Update of the `*isDoctor*` maps to mark the sender's address as a registered doctor. Also Grants permission to the doctor to access their own records.

Algorithm 4: *SMRMS-BCN* Updating of Doctor Registry

1. *SMRMS-BCN-Head* receives the request from the new patient for registration,

2. For [k=1, k≤ L, k++]
3. call '*isPatient' SMRMS-BCN-Head* verifies for the D_k^{pu} in RD^{List}
4. if [$D_k^{pu} \notin RD^{List}$]
5. *SMRMS-BCN-Head* allows to *editdetails* struct of doctor, add its D_k^{pu} and populate it with the provided patient details in *SMRMS-BCN*.
6. Update the `*isDoctor*` mapping to mark the Updated doctor's id as a registered patient
7. Grant permission to the doctor to access their own records
8. else
9. return the D^{pu}

---

10. endif
11. endfor

---

5. Set Appointment (*setAppointment* function):

The *SMRMS-BCN-Head* receives the request to set the Appointment registration to the *SMRMS-BCN*, Head calls the *setAppointment* function it checks with doctor's D^{pu} and patient's P^{pu} and then allows to make appointments . And then it gets updated through '*updateAppointment' fuction and is stored in both* RP_{List} and RD^{List} .

Algorithm 5: *SMRMS-BCN* Set Appointment

---

1. When ever SMRMS-BCN-Head receives the request from the new patient for Setting Up an Appointment .
2. For [k=1, k≤ L, k++]
3. call 'setAppointment' SMRMS-BCN-Head verifies for the $Pk\ pu$ in $RPList$ and $Dk\ pu$ in $RDList$
4. if [$Pk\ pu \notin RPList$]&[$Dk\ pu \notin RDList$]
5. SMRMS-BCN-Head create a new Appointment struct, add its $RPList$ and $RDList$ and then it is stored in SMRMS-BCN.
6. Add $Pk\ pu$ to $RPList$and $Dk\ pu\ RDList$
7. Grant permission to the patient and doctor view own records
8. else
9. return the $P\ pu$
10. endif
11.endfor

Whenever Patient arrives at the doctor of the Hospital,
For each patient, any doctor D_i broadcasts the patient's record[*PR*] in the *SMRMS-BCN* after completing the detailed diagnosis process. Then *BCN-Head* verifies the *PR* for validity. If the broadcasted *PR* gets through the Verification process, The *PR* of that patient is added in the j^{th} Block$[B]^j$ of *SMRMS-BCN*. Otherwise, *BCN-Head* returns *REJECT*.

Algorithm 6: *SMRMS-BCN* consensus mechanism

1. The patient arrives at the i^{th} doctor of the Hospital,
2. For [k=1, k≤L, k++]
3. Any doctor D_i broadcasts the patient's record PR_k in the *SMRMS-BCN* after the *diagnosis* process
4. *BCN-Head* verifies the PR_k
5. if the PR_k gets through the *Verify* process
6. The PR_k is added in the j^{th} Block B^j of *SMRMS-BCN*$[B^j]$
7. else
8. return *REJECT*
9. endif
10. endfor

This smart contract state the changes based on the required conditionals, along with storage and retrieval of data from the SMRM-BCN. The logic in the contract ensures that only authorized users can access and modify medical record data and that the contract state is updated accordingly.

6 IMPLEMENTATION

In order to implement the proposed blockchain-enabled SMRMS model, the execution environment is set up with all the required tools like Metamask, Remix, and Ganache. Secured Medical Record Management System (SMRMS) was built with Remix IDE and MetaMask by first creating smart contracts in Solidity with Remix IDE, which is an online Ethereum smart contract development environment. The contract specifies the rules and logic for securely keeping medical records on the blockchain. When the contracts have been built and tested, MetaMask, a cryptocurrency wallet and gateway to blockchain apps, is linked into the user interface, allowing patients and healthcare practitioners to engage with the SMRM system via a web-based application. MetaMask handles authentication and transaction processing on the Ethereum blockchain, allowing users to safely access and update their medical records while maintaining control and privacy.

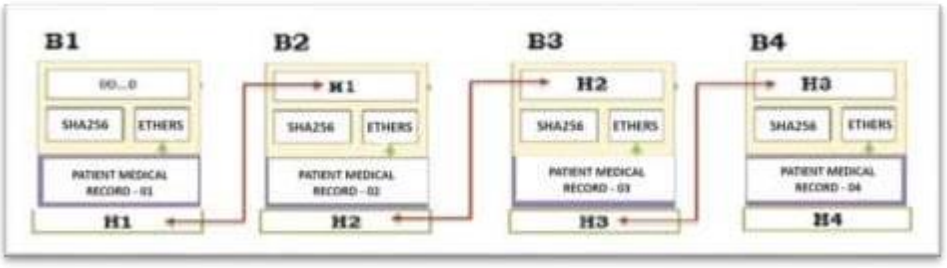

Fig 4:Structure of Blockchain

7. RESULTS and DISCUSSIONS

The implementation of the SMRMS was tested in the Remix IDE. In the Figure 5 the function *GetPermissiongrantedcount* was executed as the user was valid and the patient permitted the stakeholders such as Doctors, Nurses, or any health care provider to view his/her medical record profile. Therefore it signifies the importance of the secure medical record data management.

Figure 5: GetPermission granted

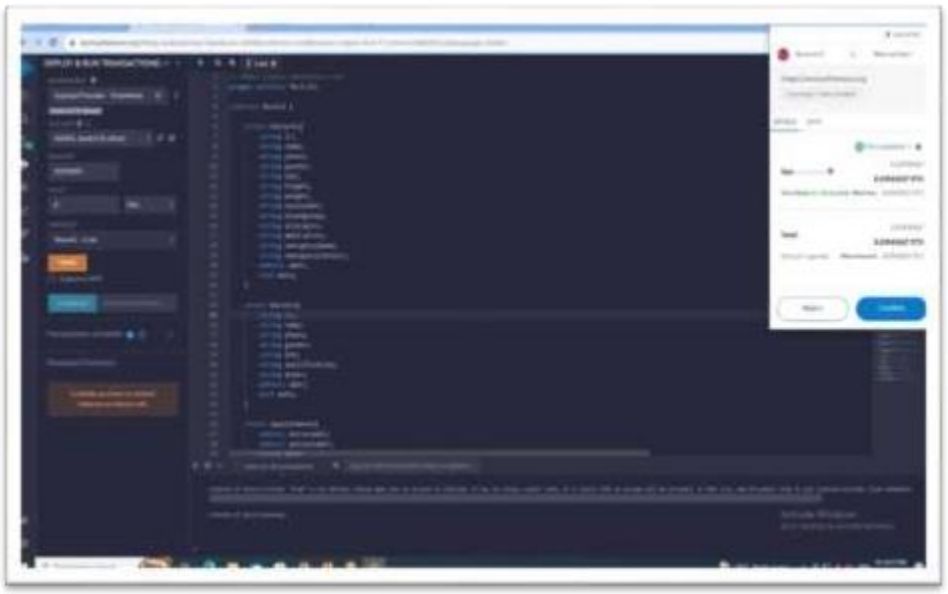

Figure 6: Metamask Transaction1

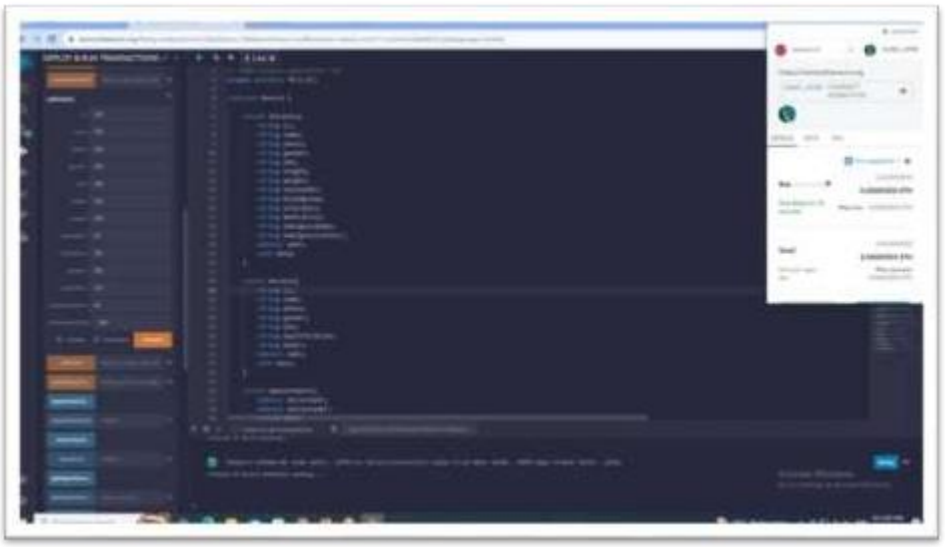

Figure 7: Metamask Transaction2

As can be seen in Figure 6 and Figure 7, whenever any entity of SMRM-BCN tries to make any type of transaction to access any medical data record, a Metamask transaction

will pop up to request the user to confirm or reject the transaction. After clicking confirm, Metamask will load for thirty seconds to a minute and then a confirmation message will appear signaling to the user that the patient's medical record has been created and stored successfully on the blockchain.

So whenever any entity[stackholder] of *SMRMS-BCN* tries to access the medical records of any patient, it can successfully access only if the concerned patient permits that entity. Otherwise, that stackholder can never access the data. Also immediately it is notified to *SMRMS-BCN-head.* So our proposed *SMRMS* successfully achieved our objectives of providing controlled or permissioned access to the medical records of patients. The same can be seen in Figures 6 and 7 as notifications to *SMRMS-BCNhead.*

The *SMRMS-BCN* built with all the mentioned entities[2 entities each] has been executed several times. The execution results have proved that no entity[any healthcare stakeholders of *SMRMS-BCN* could access the patient's medical data without the permission of the concerned patient. Figure 8 shows the level of security, tamperproffness, and controlled access provision to the medical record data of the patients with blockchain-enabled SMRMS and without blockchain implementation.

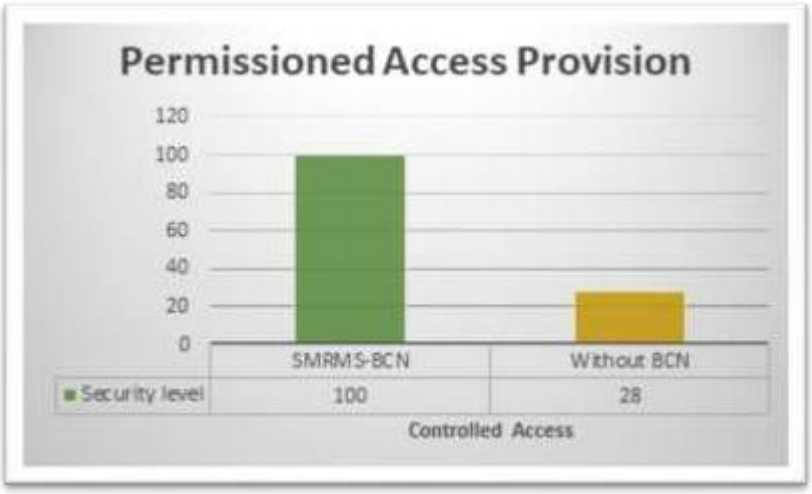

Figure 8: Controlled access provision to the medical record data of the patients with blockchain-enabled SMRMS and without blockchain implementation.

8. CONCLUSION

The implementation of a secured medical record management System(SMRMS) using blockchain has proven its potential to revolutionize healthcare data management. By leveraging blockchain's inherent qualities, including transparency, data integrity, and cryptographic security, this work has empowered patients with greater control over their diagnostic medical data, facilitating seamless sharing among only authorized

parties, enhancing data security, tamperproof among healthcare providers, and significantly reducing fraud and illegal access. So, our proposed SMRMS promises to increase the standards of security, transparency, and patient-centricity in the healthcare industry, ultimately leading to improved patient care and outcomes on a global scale. Further interoperability being the major drawback in the healthcare administration could be addressed in later stages.

9. REFERENCES:

[1]. Shams M. Alhaqbani and Siti Salwah Salim "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research" 2020 – Conference paper.

[2]. Debiao He, Xiang-Yang Li, Neeraj Kumar, and Lijun Wang "A Blockchain-Based Approach for Secure Data Sharing in Healthcare" 2018 - Conference paper.

[3]. Chun-Wei Chiang, Min-Shiang Hwang, and Po-Han Wu "Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related Research" 2018 - Journal article.

[4]. Yucheng Wang, Kai Shuang, Kewei Zhang, et al. "Secure and Privacy-Preserving Sharing of PHR in the Blockchain-Based Edge Computing System" 2020 - Conference paper.

[5]. Oussama Al Rifai, Michel Toulouse, and Elhadi Shakshuki "Blockchain for Secure Sharing of Medical Data: A Review of Current Applications" 2020 - Conference paper.

[6]. Yue Xue, Xuejing Li, and Shuang Xu "Blockchain-Based Electronic Health Records for Secure Sharing of Information among Hospitals". 2021 - Conference paper.

[7]. Fan Yang, Guoqiang Li, and Xin Lou "A Review on the Use of Blockchain for Healthcare Information Exchange". 2017 - Conference paper.

[8]. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3238553/ -National health for medicine

[9]. https://www.mdpi.com/2079-8954/11/1/38- Blockchain Application in healthcare system

[10]. https://www.roadrunnerhealthservices.com/insights/the-importanceof-medical-recordsmanagement