Journal
of the
Oriental Institute
M.S. University of Baroda
ISSN: 0030-5324

CLOUD SERVICES FOR MEDICAL VIA BLOCK CHAIN

Dr. I. Satyanarayana[1],Dr. D.Lakshmaiah[2], K.Satya vara prasad[3], K. Rishitha reddy[4], K.Lahari[5]

[1]Professor and Principal, Dept. of ME, Sri Indu Institute of Engineering & Technology, Hyderabad.

[2]Head of the Department, Dept. of ECE, Sri Indu Institute of Engineering & Technology, Hyderabad.

[3-5]Student, Dept. of ECE, Sri Indu Institute of Engineering & Technology, Hyderabad.

Abstract*—A block chain is nothing more than a chain and a list of blocks. Each block in a block chain will have its own digital signature and contain Details such as health insurance, doctor, lab results, medicine details, and so on. If a patient visits a different hospital, they use the patient key to identify the patient's previous information. Healthcare insurance and pharmacies are also aware of patient information. Using Elliptic-Curve cryptography, we create a system that allows users to create wallets and provides wallets with public and private keys. It secures the transfer of funds by proving ownership with a digital signature algorithm. Finally, users will be able to conduct transactions on your block chain. Hashes Calculating and comparing hashes allows us to determine whether or not the block chain is valid. In this paper,we discuss our perspectives on block chain-based healthcare data management, specifically for EMR data sharing among healthcare providers and research studies. We propose a framework for managing and sharing EMR data in the contextof patient care. The proposed work can significantly reduce the turn around time for EMR sharing, improve medical care decision-making, and lower overall costs.

Keywords*—*EMR, Cryptography, digital signature

I. INTRODUCTION

Electronic medical records (EMRs) are critical, highly sensitive private information in healthcare that must be shared with peers on a regular basis. Block chain provides a shared, immutable, and transparent history of all transactions, allowing developers to create applications that are trustworthy, accountable, and transparent. This presents a once-in-a-lifetime opportunity to use block chain to create a secure and trustworthy EMR data management and sharing system. The block chain is the fastest emerging technology that can be used in a variety of secure applications. Block chain is used in numerous systems. Block chain technology is one of the most important and disruptive technologies in the world.

In block chain technology, the information is stored as a ledger feature that can monitor the patients in accessing the medical records. The term block chain was formed from the Block chain concept is having some additional characteristics which would be helpful to provide more and more security. Sharing EHRs is an important research topic because it has a significant impact on patients and healthcare providers. Several cloud-based solutions have been proposed, but the credibility of a third-party cloud service is a concern. Block chain technology has recently been adopted in the healthcare domain to improve the quality of healthcare providers and make healthcare systems smarter by eliminating the involvement of a third party.

II. SYSTEM HIERARCHY

The transmission of patients' medical information poses a variety of threats to patients' privacy, as harmful activities on these records inflict severe damage to the reputation, finances, and other assets of all parties associated with the data, whether directly or indirectly. Current approaches for successfully managing and safeguarding medical records have been shown to be insufficient. Electronic Medical Records (EMRs) are currently stored in a centralized cloud-based database in which medical records are largely unportable. Centralization raises security concerns and necessitates faith in a single authority. Centralized databases, regardless of controlled access and de-identification, cannot guarantee data integrity or security. The disadvantages of the current system are significant and must be addressed, necessitating the development of a new solution for sharing EMRs that is more secure, reliable, and capable of handling all data privacy, data redundancy, and other security issues associated with the Healthcare Information Exchange System.

The patient should be able to access his EHRs and manage and share them independently under the proposed future system. The patient has direct access to his medical report and is free to share the digitalized version with

anyone. The user's data is protected by storing it in the block chain. In the etherscan, encrypted data is stored as blocks. The user saves information using two-factor authentication. Obtaining a secret key generated by Metamask is an example of a process. Systems for Electronic Health Records are proprietary and, by design, centralized. This means that there is only one supplier in charge. At the same time, the code base, database, and system output provide monitoring tools. This system will be implemented using smart contracts, which are highly permission block chains in which the network owner, i.e. the patient, controls all EMR access rights. In the event of an emergency, and the patient is unable to provide access to his medical records, the ability to view certain information is required in order to provide the best possible care. As a result, this system includes a backup access system for gaining partial access to patients' Electronic Medical Records. Wearable smart contracts can be used to accomplish this. Medical representatives can scan and provide medical information to patients. The main goal of this proposed system is to provide a more secure and efficient way to store and share health information. The patient's medical data[6] must be consistent and accessible when needed, with the terms of access- controlled solely by the patient. The secondary goal is to share medical data[6] in such a way that its structure and meaning are easily understandable in order to improve data utilization, which will lead to better patient care. Patients, doctors, and hospital management have a hard time trusting centralized systems.

This problem is solved by open-source, independently verifiable systems. This system was created to give patients control over the creation, management, and sharing of electronic health records. Other authorized data consumers include family, friends, healthcare providers, and others. Furthermore, provided that healthcare researchers and service providers have access to these EHRs from all overthe world, The healthcare solution transition program is expected to be completed. A block chain is run by a network of computers, with no single computer responsible for data maintenance or storage, and any computer can join or leave the network at any time. The use of Block chain for records can make the entire process verifiable from beginning to end. transparent. The stored data will be transactions, from which a blockchain will be created. Keep track of the patient records database. All patients can benefit from this method. They can use the records on their own, and they can do so thanks to the block chain. using the secret key given to me without any permission request from the organization.

III. RELATED WORKS

With its distinct characteristics such as decentralization, security, immutability, persistency, anonymity, and auditability, blockchain technology[2] is expected to transform the healthcare ecosystem. Blockchain has the potential to reshape traditional EHR sharing across multiple healthcare entities in order to improve healthcare quality by making it smarter and more efficient. As a result, this section discusses some previous research contributions to EHR sharing.

MedRec was among the first to investigate the use of block chains in the healthcare system. It was created in 2016 by researchers at the Massachusetts Institute of Technology (MIT) to improve the handling and sharing of electronic health records (EHRs). In its initial release, MedRec addressed four major issues in healthcare: disjointed data, interoperability, patient centricity[13-15], and research data. The project addressed interoperability issues in the healthcare and research communities. Proof-of-Work (PoW), aconsensus scheme, was implemented to prevent tampering with EHRs. However, as the number of network participants grows in block chain, the computational cost of PoW rises, resulting in low throughput in a high-transaction-volume network. MedRec did not provide a solution for scaling out control who has access to their health data thanks to Medcal Chain the technology in this regard.

EHRs have been stored in the cloud in the context of cloud computing-based healthcare systems. Cloud computing has several advantages, including quick communication, advanced sharing, storage, low cost, easy access, and dynamic association. However, cloud-based healthcare systems are vulnerable to privacy and security concerns from both legitimate and unauthorized users. Several studies have combined block chains with existing technologies.

MedRec 1.0 attempted to address the scalability issue by avoiding the block chain for patient notification and limiting block chain storage for the creation and modification of identities and relationships. This method solved the storage problem; however, high transaction volumes of new node identity creation and modification had an impact on transaction throughput. Furthermore, there was no mention of any mechanism for patient notification, despite the fact that it must be kept in the blockchain for tracing previous records.

IV. BLOCKCHAIN'S IMPORTANCE IN HEALTHCARE

One of the key characteristics that distinguish Blockchain as cutting-edge healthcare technology is the lack of a central administrator. Because the database is still viewed as a physical object made up of bits and bytes, this is the case. Because the data is a physical item, the chances of it being misplaced, misused, or accidentally deleted from manual records are extremely high. Have you given it any thought? What if the data you've saved in your system's

physical memory was lost? those who have access to it have harmed it? One of the most pressing issues in Blockchain healthcare is the security of network infrastructure at all levels. applications. All participants' identities are checked and verified. Access to electronic health records necessitates consistent authorization.

The Blockchain may be able to store data while keeping the information private and secret. Reorganize this medical database so that it can be distributed safely. As a result, the you've an All-in-one system with scalability, data confidentiality, and quick access.

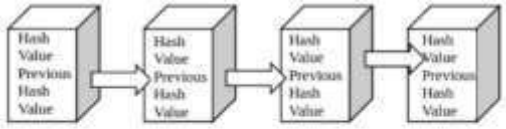


Figure 1. Structure of Blockchain

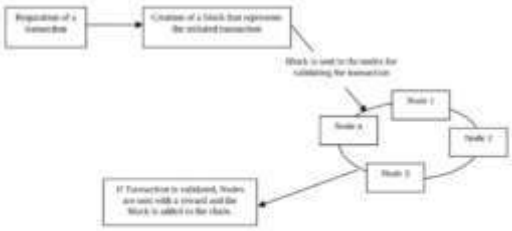


Figure 2. Working of Blockchain

Blockchain technology's introduction to the healthcare industry may be disruptive at times, but it will never be a panacea for database problems. Instead, it could be a thrilling adventure involving the gradual implementation of Blockchain.

V.Issues and Risks with the Blockchain Technology

The general issues that arise with blockchain technology[2] are discussed. This work focuses on studying theblockchain's security concerns; only the issue at hand is considered. Other blockchain security concerns are taken into account. They are summarized in the table below. It also goes into detail about the various vulnerabilities in relation to these risks.

It is possible that a user's identity will be stolen.

- Miners, who are key players in the blockchain ecosystem, are the primary targets of risk.
- Because of the distributed nature of the blockchain environment, it is vulnerable to a variety of risks, including malicious code injection and data leakage from individual nodes. The general challenges in implementing blockchain technology[2] in the healthcare domain are listed below.
- It is observed that in the case of smart health care systems, there is no rule of thumb to be followed in various activities such as data collection, data sharing, and other associated communication mechanisms.
- Because the model is user-centered, there is a chance that users, in our case, patients, will be unable to grant access in some circumstances.
- There may be issues when data is transferred from the electronic health record to the blockchain. Other general issues include the lack of government policies or rules to govern various aspects of blockchain, such as data ownership, legal issues, and penalties in the event of a violation.

VI.Healthcare Applications of Blockchain Technology

By allowing safe and pseudo-anonymous transactions and direct agreements between participants, blockchain technology[2] eliminates the need for a centralized authority to guarantee information integrity and ownership, as well as to mediate transactions and the exchange of digital assets. Patients' personal health information. Interoperability allows software apps and technology platforms to connect in a secure and seamless manner, share data, and use that data across health organizations and app suppliers, resulting in a more efficient and effective healthcare system. Healthcare today suffers from a lack of interoperability, data silos and fragmentation, delayed communications, and separate systems workflow software The Blockchain allows for secure and pseudo-anonymous access to longitudinal,complete, and tamper-proof medical records in a disjointedsystem.

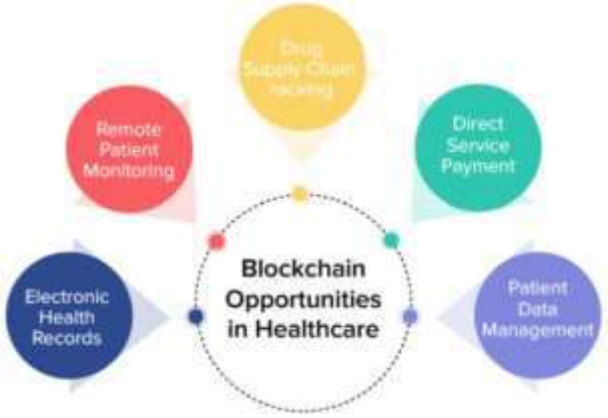


Fig.2. Blockchain Technology

VII.Blockchain in Cloud Environment

The following is a summary of various cutting-edge models that make use of blockchain technology[2] in the cloud environment. In cloud storage environments, various

access control mechanisms are used. proposes a blockchain-based access[15] control mechanism that can be used in a cloud environment. The various integrated processes of any access control mechanism, such as key generation, providing access to various requests, assigning access control policies, making changes to the assigned policies, revoking the assigned policies, and their corresponding logs, are implemented with the help of blockchain technology known as the decentralized ledger.

The work employs attribute-based encryption as its encryption model. The Ethereum virtual machine is used to implement it. In a cloud environment, the owner is unsure about their data's ability to be restricted in terms of access control while maintaining data integrity. The authors of the[9] have set out to create a blockchain-enabled database that is suitable for use in a cloud environment. It also aids in the preservation of the database's integrity. The model employs two layers of blockchain, the first layer employing the proof-of-work consensus algorithm and the second layer employing miners. The proposed design approach also addresses the various research questions concerning data integrity.

VIII.OBJECTIVES

A. Smart Contracts

When an action is triggered by an instance, the smart contract acts as a finite state machine, carrying out predetermined instructions. In this study, we use smart contracts to report actions taken by a requestor on data requested from a data owner's system. This enables data owners to obtain complete assurance and control over data provenance because the entire lifecycle of the supplied data is monitored in a regulated and trustworthy environment where the data owner does not require any assurance of confidence from the requestor.

The data sensitivity is divided into two levels: high and low. These sensitivity levels are determined by consensus node processing of data sets collected from the database architecture. Based on the sensitivity of the package, certain activities performed in the data are either exempted from theinfractions list or serve as violations. If a data has a low sensitivity level, the data owner can configure the smart contracts to ignore activities based on the required data to avoid retaining extraneous data.

Smart contracts are software programs that run in a decentralized fashion using blockchain technology. They, like all computer programs, are vulnerable to flaws in their code, and, like all emerging technologies, they are the target of hackers looking to exploit these flaws. To date, a wide range of vulnerability analysis tools for smart contracts exist, each with its own approach, algorithm, and result frominput and output formats, making it difficult for smart contract developers to take advantage of them.

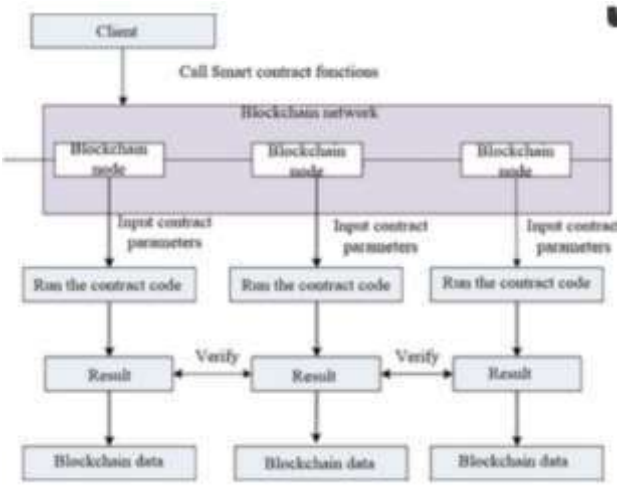


Fig.3. Smart Contracts with Blockchain

The main contributions of this work are to study, organize, and test the various existing security tools in smart contracts, demonstrating their characteristics, dependencies, installation requirements, and so on, and to develop a framework with several tools that facilitate the analysis of vulnerabilities in smart contracts using the various tools analyzed in a combined manner.

The goal of this framework is to make it easier for smart contract developers to analyze vulnerabilities without having to worry about the various installation and operating requirements of each of these tools. Similarly, the developed framework has the potential to be used in ongoing blockchain security analysis tasks by "monitoring" certain smart contracts of interest throughout their useful life, as even if they were not vulnerable at the outset, they may turn out to be vulnerable later due to changes in detection algorithms or the addition of new tools.

IX.SMART CONTRACT FRAMEWORKS

Ethereum is one of the most popular platforms for developing smart contracts. On the Ethereum platform, smart contract developers are free to create anydecentralized application (DApp) they want. The decentralized applications execute exactly as specified by the code conditions, with no risk of censorship, deception, or downtime. As a result, parties involved in the contract may suffer significant financial losses as a result of theunresolved agreement. Other smart contract platforms, in addition to

Ethereum, are used for the development of DApps. Smart contracts are one of the most powerful use cases for blockchain. Smart contracts and their digital agreements are suitable for any domain, including healthcare, due to the security and safety of blockchain technology[2]. Many practitioners are finding it difficult to manage their patient's health information, records, and data. Furthermore, there have been numerous cases of fraud as a result of the vulnerability of the outdated systems currently in use. These problems cannot be solved solely by practitioners. Smart contracts come into play here.

Fig.4. Blockchain-based EHR

X.METHODOLOGY

Giving patients the ability to choose who they share their keys with effectively gives them control over what may be done with their health information, including who can access it and when. No one should be able to view patient information without express consent since data cannot be encrypted without a key. Hackers that gain encrypted health.

Using blockchain also offers an environment in which all players, including patients, examine information before it is formally recorded. This allows healthcare practitioners and patients to review information, ensuring data integrity across the blockchain. Because 40 percent of patient health records already include inaccuracies, implementing this type of collaborative system has the potential to improve patient care while lowering the danger of potentially fatal errors.

Data reported to the data owner's system is processed, indexed, and broadcast into the blockchain network. Reports are reported and stored in a smart contract permissioned database in some circumstances, where they are indexed based on the data ID of the requested and used data, and where sets of actions from the data owner apply to the data used by the requestor. We give action sets that can be applied to any form of data collected from the system of the data owner. The following are the basic action sets: read, write, delete, duplicate, move, and copy. When these sets of actions are performed on the data, smart contracts are triggered to deliver a report based on the rules specified for that specific data.

Smart contracts are scripts that are stored on the blockchain in the blockchain context. (They are roughly equivalent to stored procedures in relational database management systems .) They have a distinct address because they live on the chain. A smart contract is activated by addressing a transaction to it. It then executes independently and automatically on every node in the network in accordance with the data included in the triggering transaction. (This implies that each node in a smart contract-enabled blockchain runs a virtual machine (VM) and that the blockchain network functions as a distributed VM.).

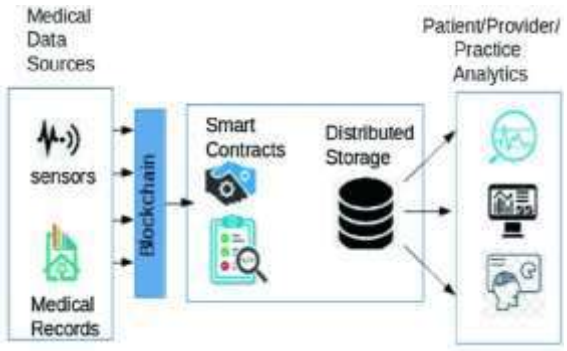


Fig.5. Medical Data Sharing with Blockchain

XI.METHOD AND MATERIALS

Existing medical record systems at healthcare institutions are very prone to data loss, falsification, and modification.

A patient[13-15] with a long history of medical issues may also have to cope with the hassle of bringing a big number of reports to their doctor's appointments. Healthcare institutions may choose to digitize the information they collect about their patients, but human verification and entry into their database will always be essential.

This is an untrustworthy approach to handling such sensitive material. Patients must go from one help desk to another to receive the information they require under the current record-keeping system.

The information received from the end-user is first encrypted to guarantee that only that person has access to it. The security and accessibility of data in a decentralized system are ensured by having it authenticated and added to blocks. The data is stored as key-value pairs in each block, with each block properly linked to the one before and after it.

The process of updating, retrieving, and displaying medical data[6] will be much more frictionless using a blockchain-based system for storing and retrieving data. As a result, the hospital's operations might be considered as information services within the blockchain architecture. Smart contract design may thus be considered a necessity in a blockchain-driven cyber environment that replicates real-world EHR operations.

XII. IMPLEMENTATION OF SYSTEM

A doctor, a patient, and a hospital are the three main consumers of blockchain architecture. Furthermore, thanks to the system's own private keys, everyone in the blockchain ecosystem[4] will have a unique capability. Some features may be restricted to doctors, patients, and hospitals.The doctor will obtain access to the web app using his or herprivate key (Frontend).

The patient communicates with the doctor using his own private key. Both parties will use a web app to share medical information (Frontend). After obtaining the service, patients must transact via a smart contract. The Ethereum network is being used as backend support. Below, the roles of every character in this figure are described:

[1] Doctor: doctors will have access to the system via a private key provided by the patient's unique key.

[2] Patient: Patients will furnish doctors with a private key. Patients can use our site to share personal information.

[3] Hospital administration can look into the process but not the specifics. They can keep the communications system running smoothly.

[4] Website: Frontend programming is being done on the website. It uses smart contracts to connect to the backend.

[5] Intelligent contracts: It is the foundation of our entire system. A log will be kept for each change in a block.

[6] Ethereum network: We leveraged the Ethereum network for backend processing.

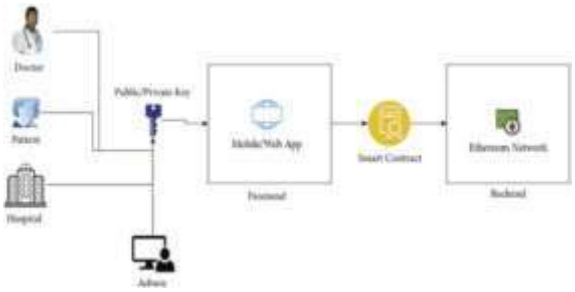


Fig.6. Implementation of the System

A. Process of System

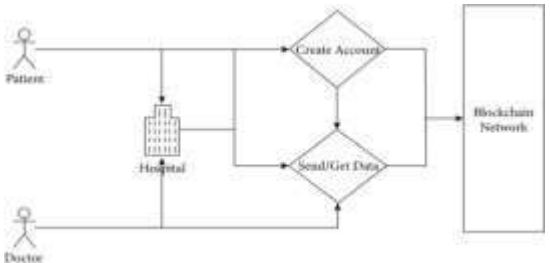
Patients must first seek medical advice from a doctor at the hospital. A network account is required for both the patient and the doctor. A new patient must first create an account and complete the essential profile information. The doctor will consult with the patient after filling out the form and searching the network for his or her information. After consulting with the doctor, the hospital will update the patient's information on the blockchain network. As a result, all of the procedures are web-connected to the blockchain network.

Fig.7. Process of System

The patient's public key[13-15] is accessible to the hospital, but only the patient has access to his or her personal private key. If a doctor wants to see a patient's medical records, he or she must ask the patient for them. When the patient receives the queue request through his mobile app or website, he or she can authorize access by entering their private key. The blockchain network will be updated after the procedure is completed.

We focused on storing patient, doctor, and lab report information. To begin, the patient should go to the websites and make an account. Users can register and select a hospital, but we only provide one option. The user has access to their prescription history as well as other medical data[6]. New features will be added to our project's tasks in the future. The patient, doctor, and laboratory are the three key features in the figure. Login, Signup, Select Hospital, View Past Records, and Make an Appointment are all options for patients. By giving patients snacks, we were able to introduce them to doctors.Doctors have access to view appointments, diagnose patients, schedule appointments with patients, and add lab tests. Doctors and laboratories are connected. Because he or she has the authority to make decisions for patients, they caninform them whether or not a lab test is required. We realized that we can use the lab test to see the lab test, generate a lab test report, and do lab test

Fig.8. Simple way of System Implementation



When the patient receives the queue request through his mobile app or website, he or she can authorize access by entering their private key. The blockchain network will be

Fig.9. Use case for system design

updated after the procedure is completed. Select Hospital, View Past Records and Make an Appointment are all options for patients. By giving patients snacks, we were able to introduce them to doctors.

Both the doctor and the patient will benefit from it. To log in to their individual accounts, each must fill in their names and log in by address. On this page, you can establish three different types of accounts. This page's three main features are the admin account, patient account, and doctor account. If the user already has an account, the username and private key will be requested. If someone is creating a private address for the first time, it is required. Every action can be monitored and managed. This website system was built with JavaScript, CSS, HTML, and Solidity.

Fig.10. Output for Patient

XIII. CODE

```
import pymongo,dns

'''contract={
    '_id':'PAT003REC01' ,
    'accesssors': 'DOC1',
    'owner':'PAT001',
    'timestamp':'0',
    'record':'',
    'status':-1

}'''


client = pymongo.MongoClient
("mongodb+srv://Antony:
A8939469555@blockchainehr-kpbxk
.mongodb.net/test?retryWrites=true&w
=majority")
db = client.test
mydb=client["Blockchain"]

#mycol=mydb["SMART_CONTRACT"]

myview=mydb['SMART_CONTRACT']
myquery = {'owner':'PAT003' }
newvalues = { "$set": {"status": 1
 } }
```

```
client = pymongo.MongoClient
("mongodb+srv://Antony:
A8939469555@blockchainehr-kpbxk
.mongodb.net/test?retryWrites=true&w
=majority")
db = client.test
mydb=client["Blockchain"]

#mycol=mydb["SMART_CONTRACT"]

myview=mydb['SMART_CONTRACT']
myquery = {'owner':'PAT003' }
newvalues = { "$set": {"status": 1
 } }

#y=myview.update_one(myquery, newval
ues)
#y=myview.find(myquery)
#myquery = {'accesssors':
{'id':'DOC1','status': 1}}
my=myview.find_one(myquery)
#print(my)
#Insert to contract
#y=mycol.insert_one(contract)
```

Fig .11. Code

OUTPUT

Patient Record Blocks:

id: Pat001rec1

Owner: Pat001

Type:Information

Gender: Female

Weight:42

BP:80/120.

XIV. RESULTS AND DISCUSSION

EHR is laying the groundwork for the future of healthcare on the blockchain. Similar projects exist, but EHR's distinct vision stands out. It includes the specialization of utilizing the blockchain. Blockchain technology[2] makes it simple to monitor population health, identify risks, and track trends in the spread of any disease. issues because the patient's medical report has been updated This contributes to the promotion of effective treatment for the patients all over the world Because it is decentralized, and the data is not owned by a single entity. They are cryptographically stored and highly secure. The system produced the following results expected.

XV. CONCLUSION

We believe that continued blockchain integration[11] in smart contracts will result in significant transformations across several industries, bringing about new business models and forcing us to reconsider how existing systems and processes are implemented.

The combination of blockchains and smart contracts has the potential to be quite powerful. Blockchains[16] enable us to build resilient, truly distributed peer-to-peer systems and interact with peers in a trustless, auditable manner. We can use smart contracts to automate complex multi-step processes. The IoT ecosystem's devices are the points of contact with the physical world.

The patient can access their report in the EHR system and keep it for the rest of their lives. The patient is given a private key, which can be used to access the reports later. Those without the private key are unable to participate in the data retrieval process. As a result, patients' health records are more secure with BlockChain and can be used with it. They have their own private key, which they can use for future reference.

XVI. REFERENCES

1. D. B. Taichman et al., "Sharing clinical trial data: A proposal from the international committee of medical journal editors free", PLoS Med., vol. 13, no. 1, pp. 505-506, Apr. 2016.
2. P. T. S. Liu, "Medical record system using blockchain big data and tokenization", Proc. 18th Int. Conf. Inf. Commun. Secur. (ICICS), vol. 9977, pp. 254-261, Nov./Dec. 2016.
3. M. M. Hassan, K. Lin, X. Yue and J. Wan, "A multimedia healthcare data sharing approach through cloud- based body area network", Future Gener. Comput. Syst., vol. 66, pp. 48- 58, Jan. 2017.

4. K. Peterson, R. Deeduvanu, P. Kanjamala and K. Boles, ”A blockchain-based approach to health information exchange networks”, Proc. NIST Workshop Blockchain Healthcare, vol. 1, pp. 1-10, 2016.

5. Kar, Estonian Citizens Will Soon Have the World’s Most Hack-Proof Health-Care Records, 2016.

6. Fan, K.; Wang, S.; Ren, Y.; Li, H.; Yang, Y. Medblock: Efficient and secure medical data sharing via blockchain.J. Med. Syst.2018

7. Shen, B.; Guo, J.; Yang, Y. MedChain: Efficient healthcare data sharing via blockchain.Appl. Sci.2019.

8. smail, L.; Materwala, H. Blockchain paradigm for healthcare: Performance evaluation.Symmetry2020.

9. Kokoris-Kogias, E.; Jovanovic, P.; Gasser, L.; Gailly, N.; Syta, E.; Ford, B. Omniledger: A secure, scale-out, decentralized ledger viasharding. In Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–24 May 2018.

10. Mettler M.Blockchain technology in healthcare: the revolution starts here.IEEE18th International Conference on eHealth Networking,September 14–16, Piscataway, NJ: IEEE, 2016

11. X.Liang,et al., “Integrating blockchain for data sharingand collaboration in mobile healthcare applications,”2017IEEE 28th Annual International Symposium on Personal,Indoor, and Mobile Radio Communications (PIMRC), 2017.12.X.Zhang, “Blockchain Support for Flexible Queries with Granular Access Control to Electronic MedicalRecords (EMR),”2018 IEEE International Conference on Communications (ICC), 2018.

13.J Liu la Protecting mobile health records in cloud computing secure, efficient, and anonymous design — ACM Trans. Embed. Comput Syst., Apr. 2017, vol. 16. 10. 2.

14. K. Gu, W. Jia, G. Wang, and S. Wen, Efficient and secure attribute-based signature for monotone predicates, Acta Inf., 2017, vol. 54. no. 5, pp, 521-541,.

15. ang H, Qin H, Zhao M, Wei X, Shen H, Susilo W. Blockchain-based fair payment smart contract for public cloud storage auditing. Information Sciences. 2020 May 1;519:348- 62.

14. ei P, Wang D, Zhao Y, Tyagi SK, Kumar N. Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems. 2020 Jan 1;102:902-11.

15. Bakhtawar, R. J. Abdul, C. Chinmay, N. Jamel, R. Saira, and R. Muhammad, “Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic,” Personal and Ubiquitous Computing, vol. 1-17, 2021.