Implementation of Ethereum Blockchain In Health Care Using IPFS

Jimit Andarpa[1], Aishwarya Vaidya[2], Neha Raut[3]
[1, 2, 3] Vidyavaridhi College of Engineering and Technology Vasai, India

Abstract- *Blockchain technology is quickly gaining popularity as a means of protecting sensitive data. The healthcare sector is one of the organizations with high risk factors, and since it has drawn the interest of many technological companies, it needs security to protect their data. The healthcare sector has several chances to succeed and benefit from the use of blockchain technology. For example, lower transaction costs, greater regulatory reporting transparency, effective administration of healthcare data, universality of healthcare information, and data access from anywhere. Blockchain may offer certain advantages in the context of a smart healthcare system, particularly from a context-aware perspective where citizens and society may be given with effective and individualized solutions.This recommended methodology's primary goal is to successfully protect patient data, and patients must have the right to maintain their information. Regarding their records, patients have confidentiality. This system implements the Ethereum blockchain. It costs a lot to provide Ethereum for the blockchain to store a patient's record. The InterPlanetary File System (IPFS) and Ethereum blockchain were both implemented for this purpose.*

Keywords- blockchain, Ethereum, health care, IPFS, smart contract, secure health care system.

I. INTRODUCTION

Blockchain technology has the ability to kill ten birds with one stone, among other difficulties. Blockchain is being used as a secure platform for data sharing in the financial sector, supply chain management, food industry, energy sector, internet of things, and healthcare [1]. The problems of centralized systems are resolved by blockchain, a decentralized framework. Blockchain applications combine peer-to-peer networks and cryptographic techniques to make them secure and reliable [2]. A blockchain is a collection of data that is arranged in blocks and is consecutively sorted. Each data block contains a hash (digital fingerprint or unique identifier), timestamped batches of recent transactions, and a hash of the prior block [3, 4]. Blockchain is a technique for storing data that makes it hard or impossible to change, hack, or deceive. A blockchain is a decentralized ledger of transactions that is replicated and dispersed across the network of computers that make up the blockchain. A record of each transaction is added to the ledger of each party whenever a new transaction on the blockchain takes place. Each block in the chain contains a number of transactions. DLT, or distributed ledger technology, is a decentralized database that is managed by numerous users. In other words, if only one block in a chain is changed, it will be obvious that the entire chain has been tampered with [5]. If hackers intended to compromise a blockchain system, they would need to make changes to every block across all distributed versions of the chain. This design links each block sequentially, and the collection of linked blocks is referred to as a blockchain. Since every block after the changed block must also be adjusted at the same time, changing a block in the middle of the chain is almost impossible. On the blockchain network, data is persistent [6]. When the conditions are satisfied, a smart contract is a separate entity from the original blockchain technology and executes automatically. The fundamental goal of this suggested healthcare management system is to safely transfer patient information to the blockchain in order to retain medical histories and provide patients confidence in their medical records [8]. This system can encompass various applications, such as securely managing electronic health records (EHRs), tracking pharmaceutical supply chains, enabling patient consent management, and facilitating secure data sharing among healthcare providers, researchers, and patients. In essence, a blockchain healthcare system leverages the unique characteristics of blockchain, such as decentralization, immutability, and cryptographic security, to transform the way healthcare data is stored, shared, and accessed for the benefit of patients, healthcare providers, and other stakeholders in the healthcare ecosystem.No one is allowed to alter their records in any way. The Ethereum blockchain implementation is done along with IPFS.

1.1 Literature Review

M. A. Lambey et al., (2020) conducted a thorough investigation into Big Healthcare Data. Discuss how you can improve patient outcomes, predict infectious outbreaks, gain valuable information, avoid preventable infections, lower health-care costs, and improve overall quality of life. However, deciding on the best use of data while maintaining patient confidentiality and the right to privacy is a challenging

job. The limitations of current technology must be identified, and guidelines for future research must be considered [1].

M. Zalloum et al., (2020) uses the traditional health system's concept of e-Healthcare. However, current e-Healthcare systems are not yet fully developed and mature, and therefore lack the level of confidentiality, integrity, anonymity, and user trust necessary for widespread adoption. Patient interest in the healthcare sector and the quality of healthcare services are two important aspects of any functioning healthcare business. Addressing privacy concerns necessitates addressing security issues such as access control, authentication, non-repudiation, and transparency, without which end-to-end privacy is difficult to achieve [2].

Koosha Mohammad Hossein et al., (2019) propose a blockchain-based architecture for e-health applications that offers an effective access control system while maintaining privacy. By taking advantage of Blockchain (BC) special features, such as immutability and user confidentiality, while changing the traditional blockchain structure to address IoT application problems (low throughput, high overhead, and latency) [3].

Farhad Ahamed et al., (2018) propose personalized healthcare (PH) is a radical patient-centered approach to healthcare that aims to change the current system. Patient data from electronic health records (EHR), Internet of Things (IoT) sensor devices, wearables and mobile devices, web-based knowledge, and social networking is the subject of this new advancement. To develop disease progression approaches, disease detection, patient self-management, and clinical intervention, PH applies Artificial Intelligence (AI) techniques to the collected dataset. In order to create analytic models, machine learning techniques are often used [4].

Dash et al., (2019) propose a healthcare-focused architecture, in which hospital records, patient medical records, medical exam reports, and Internet of Things devices are all sources of big data. Biomedical science generates a large amount of Big Data relevant to public health. This data must be carefully managed and analyzed in order to obtain valuable information. Otherwise, identifying a needle in a haystack by examining big data is akin to finding a needle in a haystack. Discuss also by offering early signs of sickness symptoms and helping to identify new biomarkers and smart methods for clinical action to enhance the quality of life [5].

K.M. Hossein et al., (2019) described Blockchain as a form of database used to store data in a distributed system. The differences between Blockchain and Bitcoin were also discussed, with a focus on future work on using Blockchain technology for electronic health records. It will look into how a hospital or health authority can use or request a patient's medical records from a third party (external stakeholder) without jeopardizing the patient's privacy [6].

S. Pariselvam et al., (2019) proposed that difficulties and different protection methods for protecting the privacy of health records in the cloud are discussed. A new scheme based on DES was proposed for preserving health records based on challenges and different securities. This scheme allows for powerful and privacy-preserving indexes to be encrypted using different symmetric keys, and encrypted data from multiple providers to be merged in the cloud without the content being known. It also offers stable database processing, allowing users to send a single data query to the cloud without knowing the contents [7].

V. Ramani et al., (2019) says that one of the most important considerations of today's smart healthcare systems is the security of confidential patient data from possible attackers. As a result, it's critical to have safe data access systems in place to ensure that only approved parties have access to a patient's medical records. The proposed framework is also capable of protecting patients' privacy. Our scheme's security review reveals that it can withstand well-known attacks while retaining system integrity. But the problem here is data will be on centralized server [8].

N. Rifi et al., (2017) says that patients and approved users of this vital medical data are concerned about the privacy and confidentiality of medical information. Scalability and interoperability, on the other hand, are critical issues that must be addressed in the final solution. Author illustrates the basic issues and benefits of blockchain technology for deploying a reliable and scalable solution for medical data sharing in order to achieve the best possible output [9].

X. Liang et al., (2017) A mobile application is used to capture health data from wearable devices, manual reporting, and medical devices, then coordinate the information to the cloud for sharing with healthcare providers and insurance companies. To maintain the integrity of health records, a proof of integrity and authentication is permanently retrievable from the cloud database and anchored to the blockchain network for each record [10].

1.2 Problem Statement

Due to its decentralization, immutability, accountability, and traceability functionality, blockchain is a viable technology that can enhance the healthcare data sharing and storing method. Data tampering is one of the most serious

problems in current technology. Although it may be possible to detect and forecast patients' states using data analytics within a single entity, handling and correlating patients' related data across various organizations is difficult. The issue isn't a lack of resources rather, it's a lack of resource management. The patient may have some way in how their medical data is used and shared by physicians. Any party interested in obtaining a patient's medical data may use the Blockchain to obtain the necessary permission. Medical records created and stored on the blockchain would be completely secure

1.3 Use of Block chainin Healthcare

The platform's potential benefits have been demonstrated by a variety of blockchain applications in the healthcare industry. The blockchain's most notable benefit, according to some, is the encryption methods known as hash algorithms that verify each block, or collection of transactions, within the system. Each transaction block from the past is examined before beginning a new transaction. Each transaction within the blockchain is guaranteed to be valid because hash algorithms cannot be modified until the transaction is encrypted. Transactions made on the blockchain are also irreversible and permanent, making it impossible to change or undo them. The blockchain is known as a "append-only ledger," meaning that if a record needs to be altered, a new record must be produced. Additionally, all blockchain transactions are time-stamped, which enhances transaction accountability and transparency [7]. Healthcare stakeholders in this situation will keep an eye on how and when medical data is used. Additionally, because the data in the ledger is dispersed among a number of nodes within the distributed network, the entire ledger remains unaffected in the event that one node within the blockchain is compromised. Patient health records cannot be altered while being sent since blockchain is permanent. Patient identities cannot be revealed when personal health records are shared across healthcare stakeholders because blockchain uses public private keys to encrypt data. Additionally, blockchain's smart contracts let a patient choose how to utilize or disclose his or her data [10].

1.4 Motivation

1) The patient can have some influence over how the doctors utilize and disclose their medical information.
2) The Blockchain might be used by any party seeking access to a patient's medical information to confirm that they have the required authorization.
3) The blockchain's creation and addition of medical records will guarantee their complete security.

1.5 Objective

1) Accuracy of Health Data: When blockchain technology and healthcare are integrated, blockchain medical records are conceivable. It is possible to significantly improve the accuracy with which therapies are administered.

2) Health Data Interoperability: Digital medical records could be advantageous for any healthcare organization. Regardless of where the facility is located, it is supported by Blockchain technology.

3) Security of Health Data: A Blockchain's data records cannot be altered once they have been entered. Thus, there is a lower possibility of data tampering or management errors. Health data kept on a Blockchain is secure from natural disasters since there is no single point of failure.

4) Health Data Handling Costs: Data is securely stored in a Blockchain architecture and is readily accessible by pertinent Doctors whenever necessary with the patient's consent.

1.6 Issues and Challenges

One of the most important issues with modern technology is data manipulation. Within a single institution, it could be conceivable to use data analytics to identify and predict the statuses of patients, but managing and correlating patient-related data across numerous organizations is challenging. The problem is not a dearth of resources, but rather a dearth of resource management.

1.7 Security and Privacy analysis

We assess the security and privacy capabilities of the suggested architecture. We look at our architecture's CIA security triad (Confidentiality, Honesty, and Availability) to show that it can withstand multiple attacks. We are addressing elements of the CIA triad in the context first and foremost.

Confidentiality: - In accordance with confidentiality, only authorized users have access to the messages. To maintain confidentiality and safeguard user data (produced by sensors) from being snooped, we encrypt communication between modules.

Integrity: The ability of the healthcare system to predict patient flow is made possible by flow management for patients based on previous test findings.

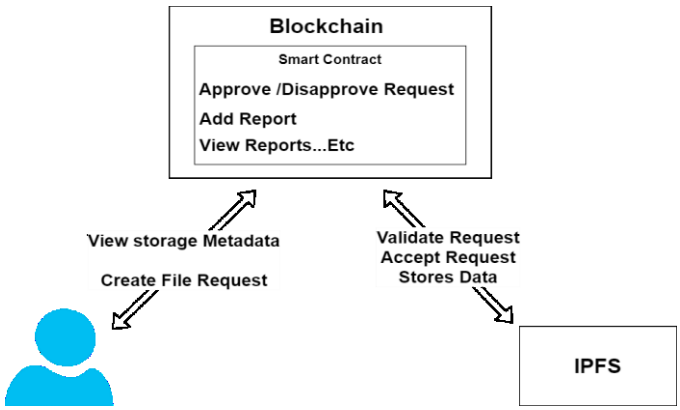
Availability: BC makes sure that the data is always accessible.

1.8 Proposed System

The main objective of the proposed system is to protect patient information against unwanted access. Access to historical reports is an additional choice because it is not possible to maintain data over a lengthy time period.

1) The patient is unable to always carry all of his information with him. In order to maintain data, the patient must register on a blockchain address.
2) The patient is treated in hospital 'XYZ'. The doctor needs the patient's permission before they may upload the patient's records. This suggests that patients have full control over the privacy of their data.
3) The patient must receive an approval request each time.
4) In this scenario, the patient is required to give hospital "ABC" access to his initial report; all that is needed is for the patient to provide their own address.
5) After logging into his account, the patient can view the Transactions for each report.
6) Because doing so would encourage the upload of fake reports, the patient is unable to upload their own reports.

1.9 Proposed Methodology Architecture



Ethereum Blockchain: - Ethereum is an open-source, blockchain-based, decentralized software platform that was founded in 2015 and is powered by its own cryptocurrency, ether. It enables the development and deployment of Smart Contracts and Distributed Applications (Apps) without the need for downtime, fraud, control, or third-party intervention.
Smart

Contracts: -The term "smart contract" refers to a program that runs on the Ethereum blockchain. It is a list of code (its functions) and data (its state) recorded on the Ethereum blockchain at a single address.

IPFS: -The InterPlanetary File System (IPFS) is a peer-to-peer network and distributed file system protocol used for data storage and sharing. IPFS uses content-addressing to uniquely define each file in a global namespace connecting all computing devices.

II. IMPLEMENTATION

The Ethereum Blockchain is used for system implementation. Ethereum is used with the aid of Ganache. With the help of Ganache, you may build a personal Ethereum blockchain to test your Solidity contracts.

- Ethereum Blockchain:-Ethereum has been used to develop the healthcare Blockchain smart contract architecture. One of the largest public blockchain networks at the moment is this open-source one, which also has a sizable public Dapp repository and a vibrant community.
- Dapps: A decentralized application (dapp) is a program created on a decentralized network that includes a smart contract and a front-end user interface. Ethereum's smart contracts are just as open and transparent as open APIs. A smart contract for a dapp may also be created by a third party.
- Ganache: Ganache is a blockchain created specifically with Ethereum developers in mind. It can be used to keep an eye on the chain's performance as tests, commands, and state inspections are being conducted.
- Smart Contract:- Solidity is an object-oriented programming language created exclusively for creating smart contracts. It is a high-level programming language that incorporates elements of JavaScript, C++, and Python. Your source code is translated into bytecode by the Solidity compiler and then executed on the Ethereum Virtual Machine (EVM).
- MetaMask: - A browser-based bitcoin wallet called MetaMask is compatible with Chrome, Firefox, and Brave. Additionally, there is a browser add-on for it. In other words, it serves as a bridge between common web browsers and the Ethereum blockchain.

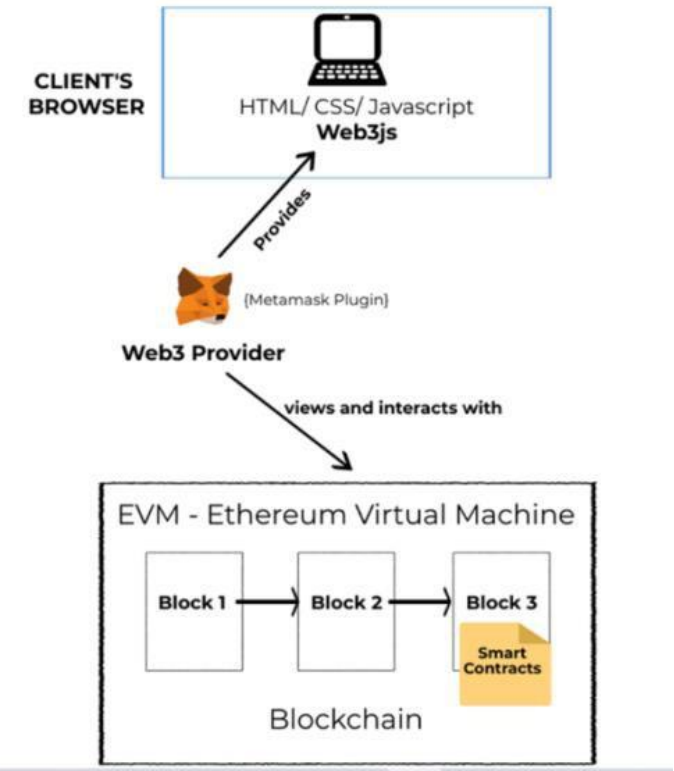


Figure02:WorkingModel

Utilizing the Ethereum Blockchain for implementation. Ganache Truffle aids in the construction of the MetaMask system. We will store patient records in our system, which may be in any format, including pdf, jpg, png, etc. Due to the fact that Ganache uses the Ethereum blockchain, it is not viable to store large document formats because their cost is inversely correlated with eth price. IPFS is used to address this issue. With the aid of IPFS, direct documents will be stored on IPFS and their hash values will be stored on blockchain, which will ultimately lower system costs.

1) Client'sBrowser:- For any web application that is HTML, CSS, or JavaScript-based, it performs similarly to a normal browser.

2) Web3.js:- A group of libraries known as Web3.js enable communication between your browser and blockchain. It enables the transfer of ether between accounts as well as the reading and writing of data from smart contracts.

3) Web3Provider:- Nodes, which make up the Ethereum network, contain identical copies of data on each one. To notify our code which node to read and write data from, web3.js requires us to define a "web3 provider". MetaMask, which integrates its web3 provider into the browser, is what we utilize in our solution. Users may safely manage their Ethereum accounts and private keys with the help of the Chrome and Firefox browser extension Metamask, which also enables them to use these accounts to interact with Web3.js-enabled websites.

4) Ethereum Virtual Machine:- The EVM implementation, which is used by each Ethereum node in the Ethereum network, is in charge of executing the same smart contract instructions throughout the Ethereum network.

With the Ethereum blockchain, we must deploy smart contracts, and Ganache and MetaMask are available for this purpose. We are creating a system that is highly useful for keeping patient medical histories in addition to some protocols that are expressed as smart contracts by connecting all of these modules.

The home screen will look like this.

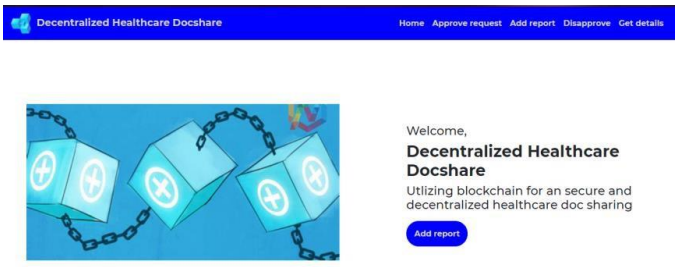


Figure03:Home page

The doctor needs the patient's consent. Otherwise, the doctor won't have access to the patient's prior health records. To grant access for that reason, the patient must approve the doctor's address.

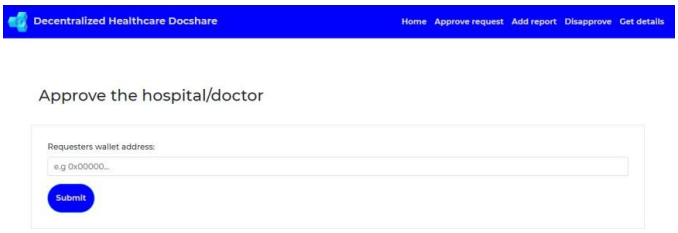


Figure04:Approve Doctor

The doctor can add the patient's new records after receiving the patient's approval. Any type of new medical report is acceptable, including an MRI, blood work, X-rays, prescriptions, etc. Anything, even documents and PDFs, can be used. Doctor must include patient address and other pertinent information for this reason.

Figure05:AddReport

The patient's prior medical history may be all that the doctor needs to see in order to treat him appropriately. If the patient and doctor agree, this may be possible. Doctors must get permission each time they view a patient's record; otherwise, the confidentiality and privacy of the patient's data won't be upheld.

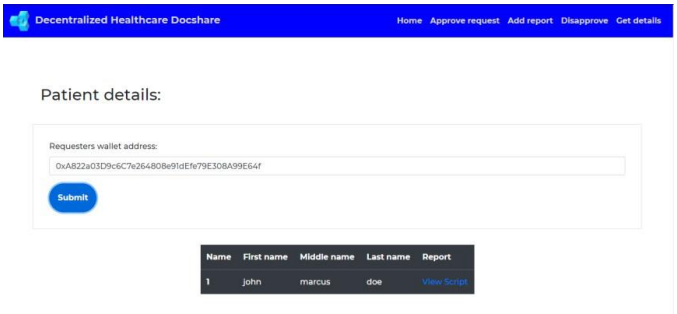


Figure06:PatientsDetails

Patients have the option to disapprove a doctor with the help of his address if they feel that they no longer want him to have access to their medical records.

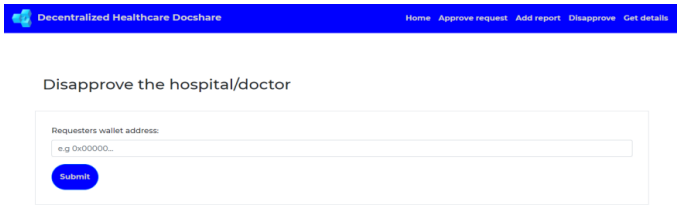


Figure07:Disapprove Doctor

There is image storage capacity on the Ethereum blockchain. It is not advised to do this, though. This is brought on by how expensive it is to store photos on the Ethereum blockchain. We will still require a centralized server if the blockchain can only hold a few kilobytes of data. Fortunately, there is a way to store data on a decentralized network thanks to the Inter Planetary File System (IPFS). using a DApp to store the IPFS hash of a file that is uploaded to IPFS on the Ethereum blockchain. The IPFS hash number will be transmitted to the Ethereum blockchain after which the user will be given a transaction receipt. We'll use the Create-React-App framework to create a front end. This Dapp is accessible to everyone with MetaMask loaded in their browser. The cost of the system is decreased with the implementation of IPFS.

III. EXPERIMENTAL RESULTS

Table 1: Feature analysis on various parameters.

Features	[4]	[6]	[8]	Proposed System
Availability	Yes	Yes	Yes	Yes
Decentralized	No	Yes	Yes	Yes
Data Privacy	Yes	Yes	Yes	Yes
Patient Centric	Partially	No	No	Yes
Immutability	Partially	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
Trustful	Partially	Yes	Yes	Yes
Storage Flexibility	Yes	No	Partially	Yes

1) Availability: -

System accessibility is essential since healthcare services are provided around-the-clock.

2) Decentralized:-

Multiple local authorities have jurisdiction over system storage and management rather than just one. Since data is kept on blocks, blockchain is a decentralized storage system.

4) Data Privacy:-

By utilizing the security features of blockchain and smart contracts, our access management system assures data privacy and individual ownership. The user's capacity to be recognized and the smart contract's authorization stop malicious access.

4) Patientcentric:-

Patients must handle all authority in relation to data sharing and uploading. The patient will make all decisions regarding the required doctor approvals and rejections under our proposed approach.

5) Immutability:-

Data should not be modified after it has been uploaded. The data cannot be modified once it has been uploaded to a blockchain.

6) Integrity:-

Integrity guarantees the undisturbed communication of patient data between authorized users. Maintaining integrity is achievable because blockchain is unchangeable.

7) Trustful:-

The patient is the only authority who can determine whether our system is reliable.

8) Storage Flexibility:-

We are using IPFS to store data, which lowers the cost of the Ethereum blockchain.

Medical records for patients are kept on the Blockchain. However, keeping such a large amount of data directly on the blockchain would be exceedingly expensive, thus we built IPFS to address this issue.

The patient controls who have access to his data. Once a patient gives a doctor their consent, that doctor has all the necessary authorization to upload and view the patient's medical history.

IV. DISCUSSION

Blockchain offers the patient's data the highest level of confidentiality and privacy. As long as the patient wishes the doctor to do so, the patient can give permission for the doctor to view his records and prior documents. Patients no longer need to worry about carrying a complete set of documents or about other people altering or deleting their data once it has been uploaded. Large files cannot be efficiently stored on blockchains. One issue is that as more data is added, the blockchain grows larger and requires more network propagation. But because the blockchain is duplicated over many nodes, a significant quantity of storage space is required without immediately having a function, especially if the node operator does not require access to every file kept on the blockchain. Additionally, as more data must be processed, transferred, and kept, the cost of maintaining blockchain nodes increases. It is possible to store and transfer large files more efficiently by using the file-sharing technology IPFS. It is based on cryptographic hashes, which may conveniently be stored on a blockchain. This strategy can help down the higher cost of ethereum. Additionally, smart contracts are in use to provide the highest level of security.

The proposed solution was created using the Ethereum blockchain, which is used to store patient-related data on IPFS. Data on patients are now more private. The patient is in complete control. It is a patient-centered model. The patient can give the doctor their approval or disapproval, as well as permission to view prior histories and add new data. Utilizing IPFS improves its capacity for large-scale data storage. The technology will eventually be able to schedule appointments, reservations, payments, and insurance.

V. ACKNOWLEDGMENTS

I would like to use this occasion to convey my sincere gratitude to my mentor Neha Raut and Dr. Kamal Shah, Professor & Dean, TCET, for her strong attention, inspiring leadership, and continual support with my work across all stages, to bring this research to fruition.

REFERENCES

[1] M. A. Lambay and S. PakkirMohideen, "Big Data Analytics for Healthcare Recommendation Systems,"2020 International Conference on System, Computation, Automation and Networking (ICSCAN), 2020, pp.1-6,doi:10.1109/ICSCAN49426.2020.9262304.

[2] M. Zalloum and H. Alamleh, "Privacy Preserving Architecture for Healthcare Information Systems," 2020IEEE International Conference on Communication, Networks and Satellite (Comnetsat), 2020, pp. 429-432,doi:10.1109/Comnetsat50391.2020.9328985.

[3] K.M.Hossein,M.E.Esmaeili,T.DargahiandA.khonsari,"Blockchain-BasedPrivacy-PreservingHealthcareArchitecture,"2019IEEECanadianConferenceofElectricalandComputerEngineering(CCECE),2019, pp. 1-4, doi:10.1109/CCECE.2019.8861857.

[4] F. Ahamed and F. Farid, "Applying Internet of Things and Machine-Learning for Personalized Healthcare:IssuesandChallenges,"2018InternationalConferenceonMachineLearningandDataEngineering(iCMLDE), 2018, pp. 19-21, doi:10.1109/iCMLDE.2018.00014.

[5] Dash, S., Shakyawar, S.K., Sharma, M. Big data in healthcare: management, analysis and future prospects. JBigData6, 54 (2019). https://doi.org/10.1186/s40537-019-0217-0

[6] K.M.Hossein,M.E.Esmaeili,T.DargahiandA.khonsari,"Blockchain-BasedPrivacy-PreservingHealthcareArchitecture,"2019IEEECanadianConferenceofElectricalandComputerEngineering(CCECE),2019, pp. 1-4, doi:10.1109/CCECE.2019.8861857.

[7] S. Pariselvam and M. Swarnamukhi, "Encrypted Cloud Based Personal Health Record Management UsingDES Scheme," 2019 IEEE International Conference on System, Computation, Automation and Networking(ICSCAN),2019, pp. 1-6, doi:10.1109/ICSCAN.2019.8878773.

[8] V. Ramani, T. Kumar, A. Bracken, M. Liyanage and M. Ylianttila, "Secure and Efficient Data AccessibilityinBlockchainBasedHealthcareSystems,"2020 IEEE Global Communications Conference (GLOBECOM), 2018, pp. 206-212, doi:10.1109/GLOCOM.2018.8647221.

[9] N.Rifi,E.Rachkidi,N.AgoulmineandN.C.Taher,"Towardsusingblockchaintechnologyforehealthdata access management," 2017 Fourth International Conference on Advances in Biomedical Engineering(ICABME),2017, pp. 1-4, doi:10.1109/ICABME.2017.8167555.

[10] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration inmobile healthcare applications," 2019 IEEE 28th Annual International Symposium on Personal, Indoor, andMobileRadio Communications(PIMRC),2017, pp. 1-5, doi:10.1109/PIMRC.2017.8292361.