iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52659

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Electronic Health Record System Using Blockchain Technology

Prof. Mrs. A. S. Shinde[1], Vivek Rai[2], Suraj Jauhari[3], Satyam Kumar[4], Sarvesh Watane[5]
Department of Information and Technology, Smt. Kashibai NavaleCollege of Engineering/Savitribai Phule Pune University, India

Abstract: ***Patient's Health Records (PHRs) are valuable assets to individuals because they enable them to integrate and manage their medical data. Due to the rapid growth of HealthCare management, it is crucialto maintain the Electronic Health Record of patients. Electronic Health Record systems face problems interms of security, integrity, and management since a large volume of patient's sensitive data is shared between anonymous bodies. To overcome these issues, this project aims to explain how Blockchain technology can be a solution for Electronic Health Record systems. These records for not only useful for the consultation but also for creation of historic family health information tree that keeps track of genetichealth issues and diseases it can also be used for any health service with the authorization from both the patient and medical organization. Hence, proposed a system consists blockchain technology for ElectronicHealth Record and to provide secure storage of electronic records by defining granular access to the usersby interpreting an Electronic Health Record web application.***
Keywords: Blockchain, Electronic Health Record, Web application, Patient's Health Record

I. INTRODUCTION

Designing and implementing a system for health care data that allows users to store all information in a single blockchain without the usage of a Trusted Third Party (TTP) in a fog computing environment is the goal of the proposed research project. Additionally, the systems ensured data confidentiality, integrity, and elimination of user-facing inconsistencies. The use of block chains for the storage of health care data is highlighted by the system. In the system, if a patient moves to a new city and is subsequently referred to a physician in a different city, the new physician may access the patient's whole medical history over fog networks, and this system use blockchain technology to maintain the integrity of the data. Since the data in this case is processed across numerous servers, the transactions are handled sequentially in a fog network. This clarifies the issue of service quality and time constraints. In this middleware system, threads will be used to balance the load in the processing environment. The resulting request will be saved in parallel across all nodes in a blockchain-based fashion. For the supplied string, a hash will be constructed using a hash creation technique. Peer-to-peer verification is used to verify the data prior to any transaction being carried out. If any chain is invalid, the current server blockchainwill be updated or recovered. This will continue to validate until the query is committed and all nodes are confirmed. The hash created for the query is checked using the mining algorithm until a valid hash is produced.For the purpose of extracting the valuable report, some applications for medical services and pharmaceuticals may be handled by the public and by third parties. In some circumstances, attacks on vital patients' sensitive datamay occur, and this process has dangers including illegal access and mitigation. As a result, each hospital has itsown database that is maintained. Since it is crucial to consider and maintain privacy and security while designinga system for sensitive healthcare data, Also, in order to sustain globalization, it is crucial to connect all databasestogether. It is not simple to connect the hospital databases. Confidentiality must be always upheld, and all recordsmust be kept in a secure way. because medical reports tend to be more delicate. In this initiative, the donor is linked to our system. Another crucial role in the conventional system is the exchange of blood and organs. Withthe conventional approach, the sole option for a transactional emergency is to call each donor individually. But reaching the contributors at the appropriate moment is quite challenging. We are therefore keeping a separate donor database and connecting those facts to the globalized system. It's not too difficult to connect the donor at the right time. Moreover, it reduces death rates and shortens life lengths. EHRs enable quick access to patient records for more coordinated, effective care by giving accurate, complete, and up-to-date information about patients. EHR aids in enhancing the confidentiality and security of patient data, which lowers costs by reducing paperwork and testing duplication. Thus, sensitivity, privacy, immutability, and access by different persons are prerequisites of EHR. These specifications can be met by the characteristics of blockchain technology. When information is stored on the blocks, the chain of connected blocks that make up the blockchain continues to grow. A blockchain offers several advantages, including security, interference-free anonymity, and distributed data sharing architecture.

Electronic health records could be more effective and provide data security thanks to this technology. In this study, we examine how blockchain technology is used in the administration of access to andstorage of electronic health records in the field of medicine. Maintaining patients' electronic health records is essential due to the quick expansion of healthcare administration. Since a lot of sensitive patient data is transferred across anonymous entities, electronic health record systems struggle with security, integrity, and management issues. This research seeks to explain how Blockchain technology can be a solution for Electronic Health Record systems in order to address these problems. Hence By establishing granular access to users and interpreting an Electronic Health Record web application, it is presented in a way to utilize blockchain technology for Electronic Health Records and to enable secure storage of electronic records.

II. LTERATURE REVIEW

In Paper [1], Madine, Mohammad Moussa, “Blockchain for giving patients control over their medical records”.The aim in this paper is to propose Ethereum blockchain-based smart contracts to give patients control over their data in a manner that is decentralized, immutable, transparent, traceable, trustful, and secure.

In Paper [2], Sun, Jin, “Blockchain-based secure storage and access scheme for electronic medical records in IPFS.” In this paper, based on the ciphertext policy attribute-based encryption system and IPFS storage environment, combined with blockchain technology, we constructed an attribute-based encryption scheme for secure storage and efficient sharing of electronic medical records in Inter-Planetary File System (IPFS) storage environment.

In Paper [3], arshini, V. M., “Health record management through blockchain technology”. This paper aim on thepatient-driven model of record maintenance using Blockchain technology where smart contracts can be incorporated in future days making it more potential in data exchange. Finding its huge scope, hoping that moreresearches will be carried out and practically implemented.

In Paper [4], Liu, Xiaoguang, “A blockchain-based medical data sharing and protection scheme”. A prototype for medical data sharing and protection scheme based on the hospital’s private blockchain to improve the electronic health system of the hospital. Firstly, the scheme can satisfy various security properties such as decentralization, openness, and tamper resistance. A reliable mechanism is created for the doctors to store medical data or access the historical data of patients while meeting privacy preservation. The proxy re-encryptionis utilized in the proposed scheme.

In Paper [5], Du, Mingxiao, “An optimized consortium blockchain for medical information sharing”. In this paper it proposed a new business process and a blockchain based platform for medication information sharing and also propose a consensus algorithm and universal anonymous sharing model that Electronic Health Record System Using Blockchain Technology Department of Information Technology, SKNCOE, Pune-41 5 improve EMIs electronic medical information system. Information can be stored, shared and credibly verified among parties in the distributed network.

In Paper [6], Tith, Dara, “Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability”. In this paper, for improving privacy, scalability, and availability, blockchain is being used to retain patient information in Electronic Health Record. Consortium blockchain to create a distributed system using existing Electronic Health Record utilizing Hyperledger Fabric. The address of a patient record in an Electronic Health Record is recorded on the same ledger held by peer nodes. Individual patients are recognized by one-of-a-kind certificates issued by local certificate authorities who operate together in a network channel. When transferring data, we employ a proxy re-encryption mechanism to preserve a patient’s privacy.

In Paper [7], Houtan, Bahar, Abdelhakim Senhaji Hafid, and Dimitrios Makrakis. “A survey on blockchain- based self - sovereign patient identity in healthcare”. In this paper, we focus on implementation of DLTs based on BCs such as Bitcoin, Ethereum and Hyperledger. In these systems, a set of new transactions is collected in ablock and added to Distributed ledger technology (DLT) after the block has been verified via a consensus mechanism, such as Proof of Work (PoW) and Proof of Stake (PoS). Blocks are linked together.

In Paper [8], Sharma, Yogesh, and B. Balamurugan. “Preserving the privacy of electronic health records using blockchain”. In this study the aim was to design a system to implement EHR's (Electronic health record) using Blockchain technology and make EHR's more secure and private. The Blockchain technology will keep controlover access to information using its cryptographic techniques and decentralization. It will also maintain the balance between data privacy and data accessibility. Main objective is to framing the data privacy and security issues in electronic healthcare. This all process is achieved by the help of consensus algorithm which help in achieving the trust between the participants and reliability in network.

III. METHODOLOGY

A. *Existing System*

A centralized records centre is one in which all the physical documents are located in one central location. The location is controlled by the records and information management department staff. The number of people in the records department will depend on the size of the organization. While centralized records centres have many advantages, they also have some drawbacks. First, physical documents are not at the end user's fingertips, so they may need to wait a long time before they can review a file, especially if the file is stored at another office location. Second, hiring a full-time records department staff to manage the centralized location is a big expense. A centralized records centre may also require a large investment in high-density shelving. Thistype of shelving can be very costly, especially if the floor has to be reinforced to meet weight requirements.

B. *Proposed System*

A decentralized records centre is one in which the physical documents are located across theentire office. Documents could be stored in end users' offices, workstations or other workroom space. Unlike a centralized records centre, where the files are controlled exclusively by the records department, a decentralized location is controlled by the end user who creates the file. Now, let's discuss some advantages of a decentralizedrecords centre. The physical file is stored at the end users' desks, not in a centralized location. Of course, this method does not require a full-time records department staff. End users can access their files at all times and are responsible for maintaining accuracy.

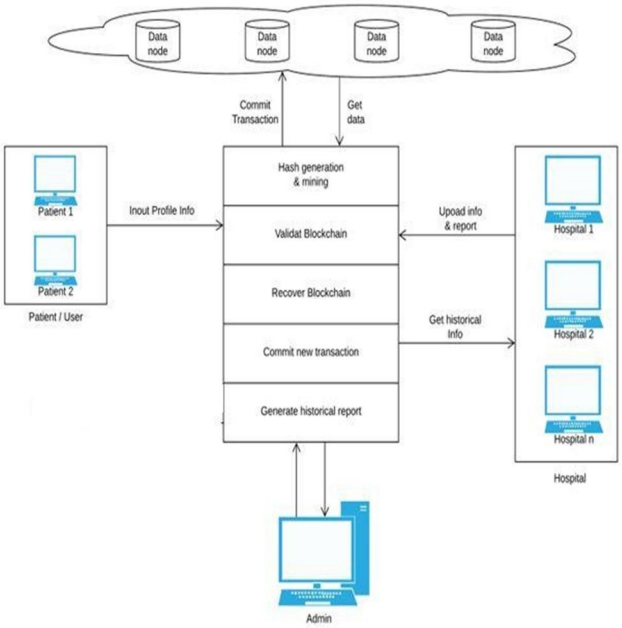


Figure 3.1-Proposed System Architecture

Three access logins are available for the Electronic Health Record web application that was created for our project. It was constructed using Blockchain-based technology. A doctor and patient or a patient and doctor canshare data in a peer-topeer setting. Users include admins, doctors, and patients.

1) *Admin:* Client (Transaction of medical data). Based on the hospital he works at the administrator can log in andregister. Patient accounts can be created by the admin. The hospital's administrative staff can set up accounts forthe doctors who work there in various specializations.
2) *Patient:* By entering their login information, a patient can register and log in. By completing a form detailing their symptoms, patients can schedule a consultation with the doctor. The patient can view the doctor's diagnosisresults.
3) *Doctor:* Upon logging in and signing up, doctors must enter their credentials. In the Dashboard, a doctor can view the appointments that they have scheduled. A doctor has access to the patient's information and can recommend prescriptions depending on the data the patient has provided.

C. SHA-256 Algorithm

SHA-256, which stands for secure hash algorithm 256, is a cryptographic hashing algorithm (or function) that'sused for message, file, and data integrity verification. It's part of the SHA-2 family of hash functions and uses a256-bit key to take a piece of data and convert it into a new, unrecognizable data string of a fixed length. This string of random characters and numbers, called a hash value, is also 256 bits in size.

D. General Description

SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits. Itis a keyless hash function; that is, an MDC (Manipulation Detection Code). A message is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds. Basic operations

1) Boolean operations AND, XOR and OR, denoted by A, ⊕ and ∨, respectively.
2) Bitwise complement, denoted by ¯.
3) Integer addition modulo 232, denoted by A + B. Each of them operates on 32-bit words. For the last operation,binary words are interpreted as integers written in base 2.
4) RotR(A, n) denotes the circular right shift of n bits of the binary word A.
5) ShR(A, n) denotes the right shift of n bits of the binary word A.
6) AkB denotes the concatenation of the binary words A and B.

E. Functions and Constants

The algorithm uses the functions:

Ch(X, Y, Z) = (X A Y) ⊕ (X A Z),
M aj(X, Y, Z) = (X A Y) ⊕ (X A Z) ⊕ (Y A Z),
Σ0(X) = RotR(X, 2) ⊕ RotR(X, 13) ⊕ RotR(X, 22),
Σ1(X) = RotR(X, 6) ⊕ RotR(X, 11) ⊕ RotR(X, 25),
σ0(X) = RotR(X, 7) ⊕ RotR(X, 18) ⊕ ShR(X, 3),
σ1(X) = RotR(X, 17) ⊕ RotR(X, 19) ⊕ ShR(X, 10),

F. Padding

To ensure that the message1 has length multiple of 512 bits:

• first, a bit 1 is appended, • next, k bits 0 are appended, with k being the smallest positive integer such that l + 1 + k ≡ 448 mod 512, where l is the length in bits of the initial message,

• finally, the length l< 2 64 of the initial message is represented with exactly 64 bits, and these bits are added atthe end of the message. The message shall always be padded, even if the initial length is already a multiple of 512.

G. Block Decomposition

For each block M ∈ {0, 1} 512, 64 words of 32 bits each are constructed as follows:

• the first 16 are obtained by splitting M in 32-bit blocks

$$M = W1kW2k \cdot \cdot \cdot kW15kW16$$

• the remaining 48 are obtained with the formula:

$$Wi = \sigma1(Wi-2) + Wi-7 + \sigma0(Wi-15) + Wi-16, 17 \leq i \leq 64.$$

Hash computation

• First, eight variables are set to their initial values, given by the first 32 bits of the fractional part of the squareroots of the first 8 prime numbers:

H (0) 1 = 0x6a09e667 H (0) 2 = 0xbb67ae85
H (0) 3 = 0x3c6ef372 H (0) 4 = 0xa54ff53a
H (0) 5 = 0x510e527f H (0) 6 = 0x9b05688c
H (0) 7 = 0x1f83d9ab H (0) 8 = 0x5be0cd19

• Next, the blocks M(1) , M(2), . . . , M(N) are processed one at a time:
For t = 1 to N
– construct the 64 blocks Wi from M(t) , as explained above
– set
(a, b, c, d, e, f, g, h) = (H (t−1) 1 , H(t−1) 2 , H(t−1) 3 , H(t−1) 4 , H(t−1) 5 , , H(t−1) 6 , H(t−1) 7 , H(t−1) 8)
– do 64 rounds consisting of:
T1 = h + Σ1(e) + Ch(e, f, g) + Ki + WiT2 = Σ0(a) + M aj(a, b, c)
h = gg = ff = e
e = d + T1d = c
c = bb = a
a = T1 + T2
We assume that the length of the message can be represented by a 64-bit integer.
– compute the new value of H (t) jH (t) 1 = H (t−1) 1 + a
H (t) 2 = H (t−1) 2 + bH (t) 3 = H (t−1) 3 + cH (t) 4 = H (t−1) 4 + dH (t) 5 = H (t−1) 5 + eH (t) 6 = H (t−1) 6 + fH (t) 7 = H (t−1) 7 + gH (t) 8 = H (t−1) 8 + h

End for
• The hash of the message is the concatenation of the variables Hi N after the last block has been processed .H = H1 $^{(N)}$ || H2 $^{(N)}$ || H3 $^{(N)}$ || H4 $^{(N)}$ || H5 $^{(N)}$ || H6 $^{(N)}$ || H7 $^{(N)}$ || H8 $^{(N)}$.

H. Implementation: signatures

Implement the cryptographic hash function just described. Define the class sha256 with the method: publicstatic Big Integer hash (byte [] M)
Input: M is a chain of bytes of arbitrary length;
Output: a positive integer in the interval [0, 2 256), the value of the hash of M.

I. Test Values

To check the implementation, you can use the following values, given in hexadecimal notation.

J. Blockchain Technology

input	61 62 63
hash	ba7816bf 8f01cfea 414140de 5dae2223 b00361a3 96177a9c b410ff61 f20015ad
input	61 62 63 64 62 63 64 65 63 64 65 66 64 65 66 67 65 66 67 68 66 67 68 69 67 68 69 6a 68 69 6a 6b 69 6a 6b 6c 6a 6b 6c 6d 6b 6c 6d 6e 6c 6d 6e 6f 6d 6e 6f 70 6e 6f 70 71
hash	248d6a61 d20638b8 e5c02693 0c3e6039 a33ce459 64ff2167 f6ecedd4 19db06c1
input	One million of 61
hash	cdc76e5c 9914fb92 81a1c7e2 84d73e67 f1809a48 a497200e 046d39cc c7112cd0

Figure 3.2-Test Values

A brand-new, developing technology is block chain. It is a group of records that are kept in a block. To keep therecords in a safe and secure way, there are blocks. Cryptographic technology is used to link each block to the next. Block Chain Network: The blockchain is a decentralized network. Without any access authorization, the intrusive party cannot steal the data. The cloud storage of data using the block chain is secure. To store the data, a certain number of blocks can be generated. By using cryptographic technology, new blocks can be added. As a result, no third party is permitted to access the data. The records of the doctor, patient, and donor are maintained on our system's blockchain network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

IV. RESULTS AND DISCUSSIONS

The main problem of the current health care is that the organizations hold multiple and fragmented medical records of patients. The Proposed System aims to solve the health care sector's current problems by hosting medical record transactions on the Blockchain to create a smart ecosystem. The goal is to provide secure access to patient data, avoiding the third party accessing it without permission. EHR Framework uses blockchain technology to securely store the records and maintain a single version of the truth. The stakeholders will have torequest permission to access a patient's history and commit the transaction to the distributed ledger. A solution centered on the blockchain, can permit large scale availability, data confidentiality, cost-effectiveness, and belief in the information system.

```
class Blockchain:

    def __init__(self):

        self.transactions = []
        self.chain = []
        self.nodes = set()
        #Generate random number to be used as node_id
        self.node_id = str(uuid4()).replace('-', '')
        #Create genesis block
        self.create_block(0, '00')


    def register_node(self, node_url):
        """
        Add a new node to the list of nodes
        """
        #Checking node_url has valid format
        parsed_url = urlparse(node_url)
        if parsed_url.netloc:
            self.nodes.add(parsed_url.netloc)
        elif parsed_url.path:
            # Accepts an URL without scheme like '192.168.0.5:5000'.
            self.nodes.add(parsed_url.path)
        else:
            raise ValueError('Invalid URL')


    def verify_transaction_signature(self, sender_address, signature, transaction):
        """
        Check that the provided signature corresponds to transaction
        signed by the public key (sender_address)
        """
        public_key = RSA.importKey(binascii.unhexlify(sender_address))
        verifier = PKCS1_v1_5.new(public_key)
        h = SHA.new(str(transaction).encode('utf8'))
        return verifier.verify(h, binascii.unhexlify(signature))


    def submit_transaction(self, sender_address, recipient_address, value, signature):
        """
        Add a transaction to transactions array if the signature verified
```

First function is created to create the very first block and sets its hash to “0”.

```
def create_block(self, nonce, previous_hash):
    """
    Add a block of transactions to the blockchain
    """
    block = {'block_number': len(self.chain) + 1,
             'timestamp': time(),
             'transactions': self.transactions,
             'nonce': nonce,
             'previous_hash': previous_hash}

    # Reset the current list of transactions
    self.transactions = []

    self.chain.append(block)
    return block


def hash(self, block):
    """
    Create a SHA-256 hash of a block
    """
    # We must make sure that the Dictionary is Ordered, or we'll have inconsistent hashes
    block_string = json.dumps(block, sort_keys=True).encode()

    return hashlib.sha256(block_string).hexdigest()


def proof_of_work(self):
    """
    Proof of work algorithm
    """
    last_block = self.chain[-1]
    last_hash = self.hash(last_block)

    nonce = 0
    while self.valid_proof(self.transactions, last_hash, nonce) is False:
        nonce += 1

    return nonce
```

This function is created to add further blocks into chain. The function is created to display previous hash and thelast function is used for proof of work and used to successfully mine the blocks.

```
# Instantiate the Node
app = Flask(__name__)
CORS(app)

# Instantiate the Blockchain
blockchain = Blockchain()

@app.route('/')
def index():
    return render_template('./index.html')

@app.route('/configure')
def configure():
    return render_template('./configure.html')


@app.route('/transactions/new', methods=['POST'])
def new_transaction():
    values = request.form

    # Check that the required fields are in the POST'ed data
    required = ['sender_address', 'recipient_address', 'amount', 'signature']
    if not all(k in values for k in required):
        return 'Missing values', 400
    # Create a new Transaction
    transaction_result = blockchain.submit_transaction(values['sender_address'], values['recipient_address'], values['amount'], values['signature'])

    if transaction_result == False:
        response = {'message': 'Invalid Transaction!'}
        return jsonify(response), 406
    else:
        response = {'message': 'Transaction will be added to Block '+ str(transaction_result)}
        return jsonify(response), 201

@app.route('/transactions/get', methods=['GET'])
def get_transactions():
    #Get transactions from transactions pool
    transactions = blockchain.transactions

    response = {'transactions': transactions}
    return jsonify(response), 200
```

Creating the Web App using flask and then the object of the class blockchain and mining new block. Displayingblockchain in json format. Checking validity of blockchain and running flask server locally.

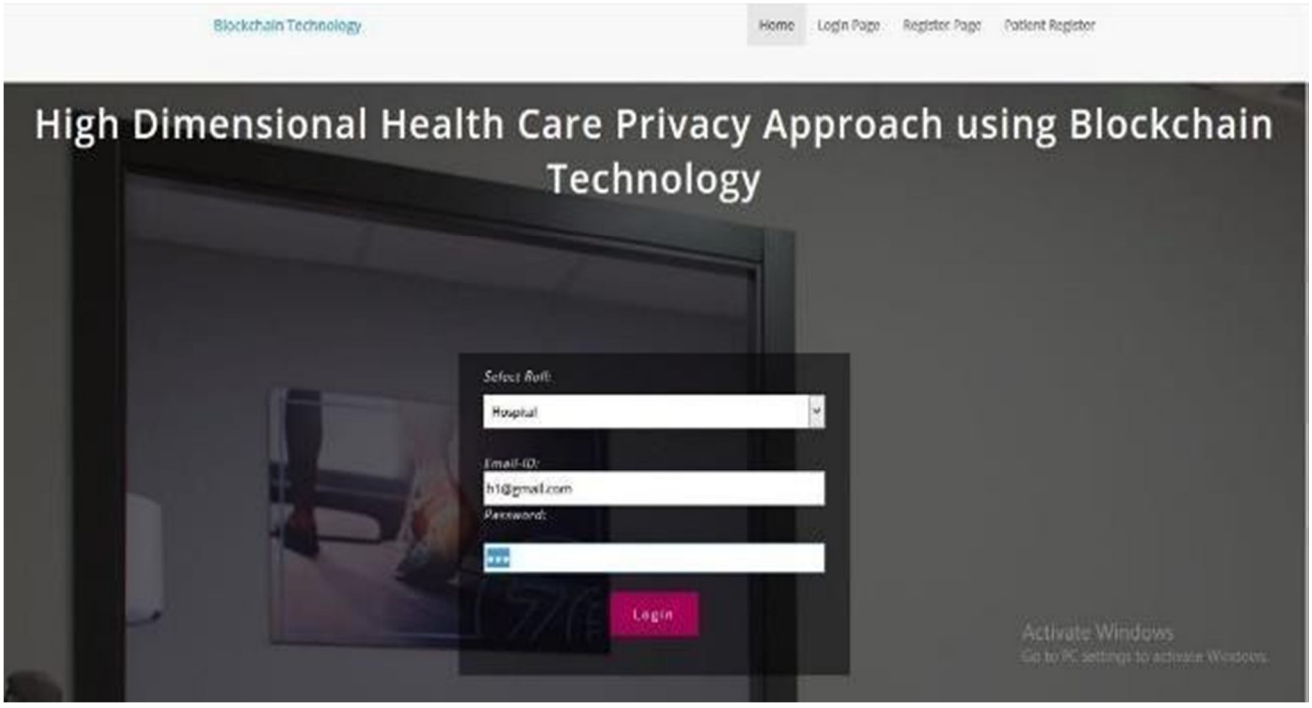


Figure 4.1-Login Page

Login page includes username and password for users who have already registered. For users who have not registered it has option called New User Registration. If user is entering wrong password this page has option called Forgot Password.

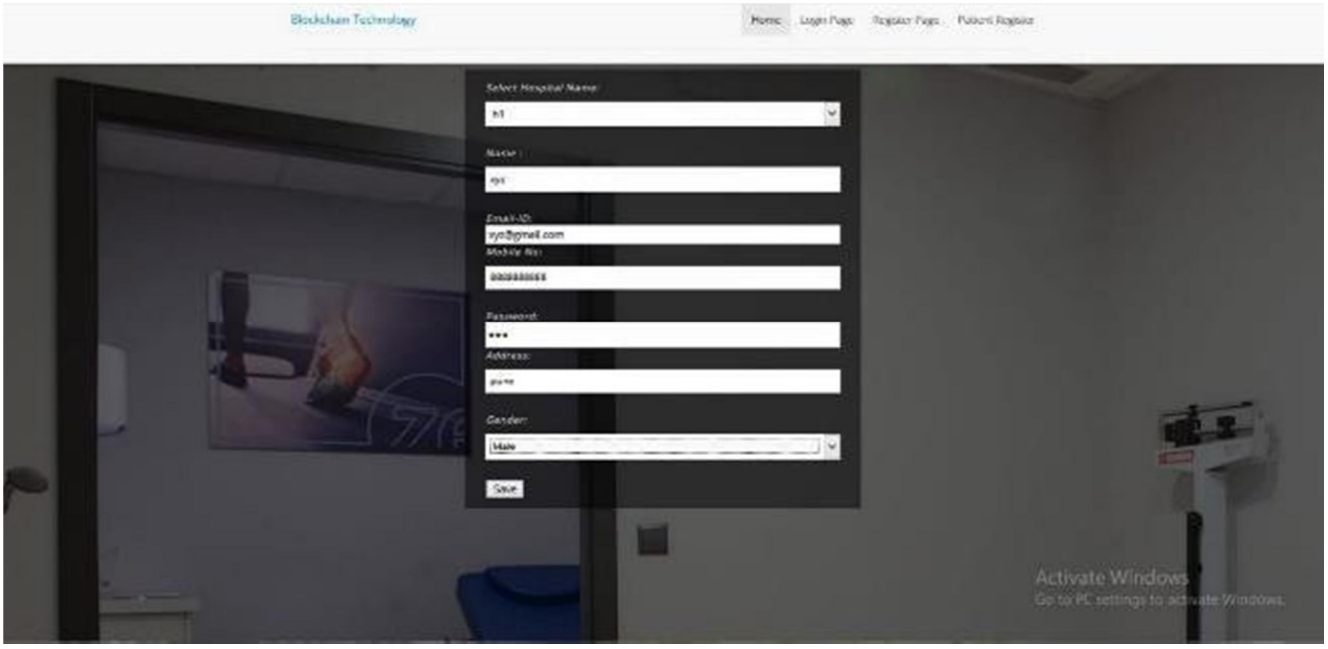


Figure 4.2-Registration Page

On registration page user have to submit personal information like Name, Contact Number, Email, Address, Age, Gender etc. If user enters valid information registration will be done.

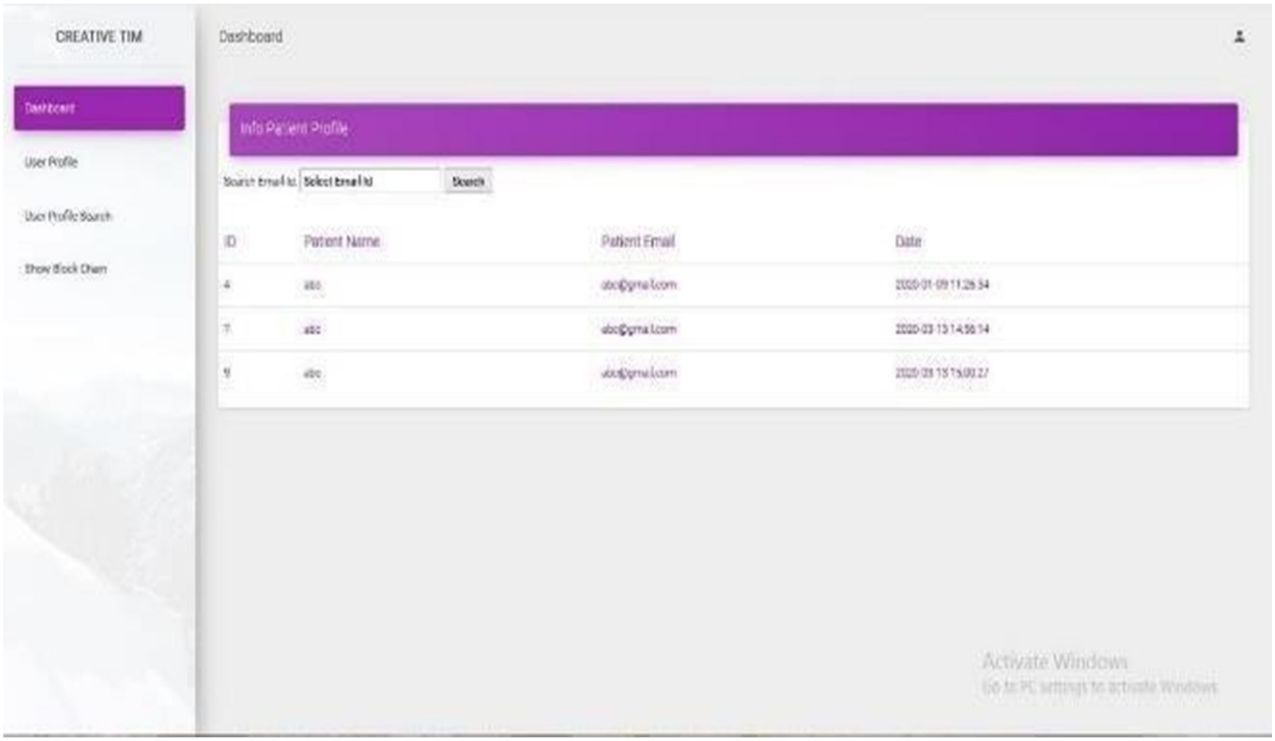


Figure 4.3-Registered Users

This page includes information of registered users. Such as Name, Email-id and Registration Date.

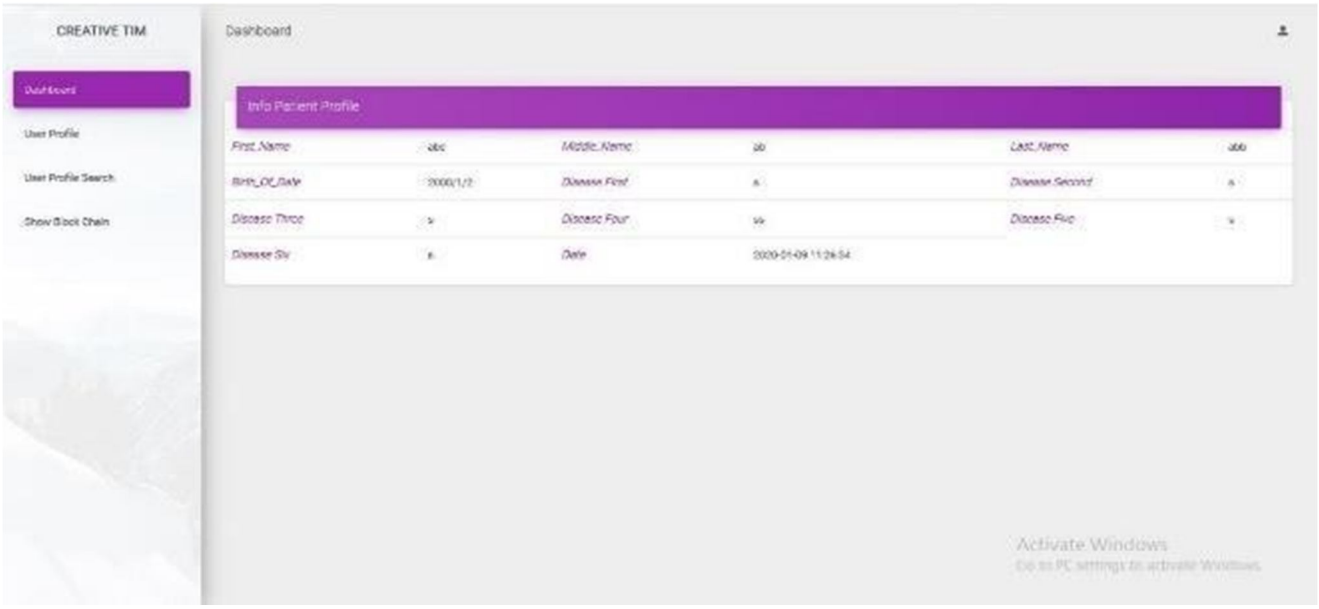


Figure 4.4-Patient Profile

Patient profile include patient's basic information like Name, Date of Birth, Diseases that he has etc.

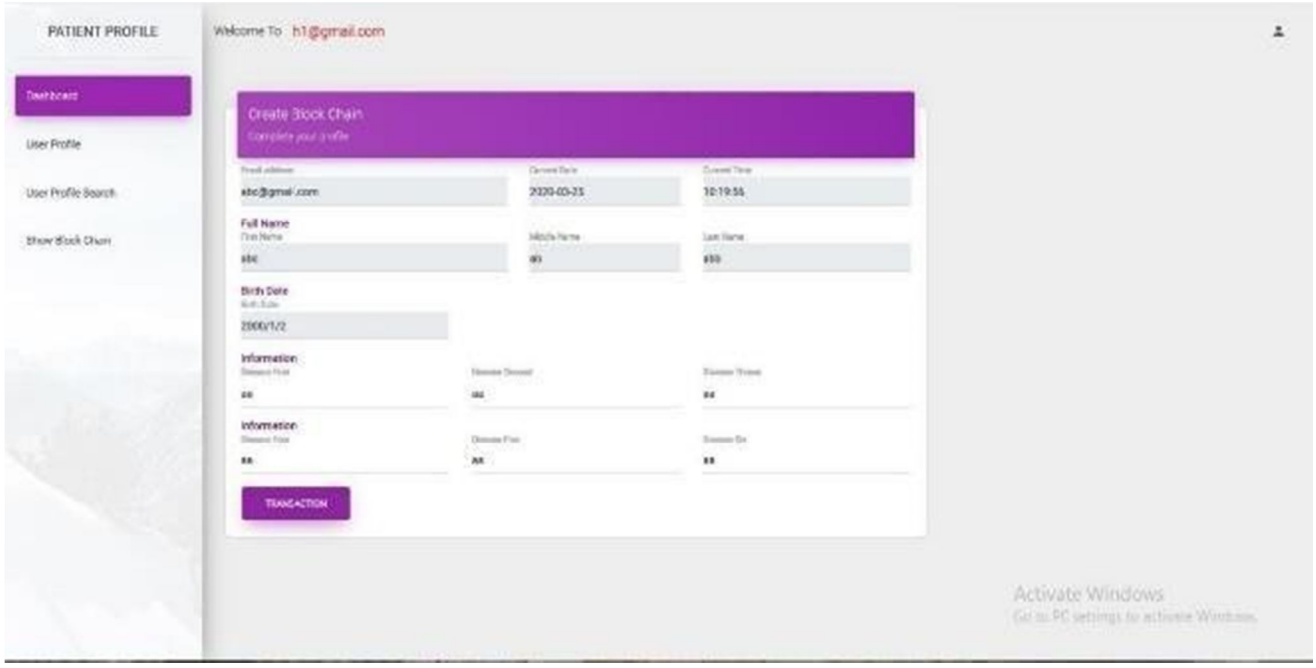


Figure 4.5-Patient Details

These include detailed information of patient like Full Name, Date of Birth, Disease information etc.

V. CONCLUSION

A blockchain-based electronic health record system has been proposed and put into operation. It shows how blockchain can be applied to the healthcare industry and how it can advance current electronic health record systems by addressing their flaws.

A. Future Scope

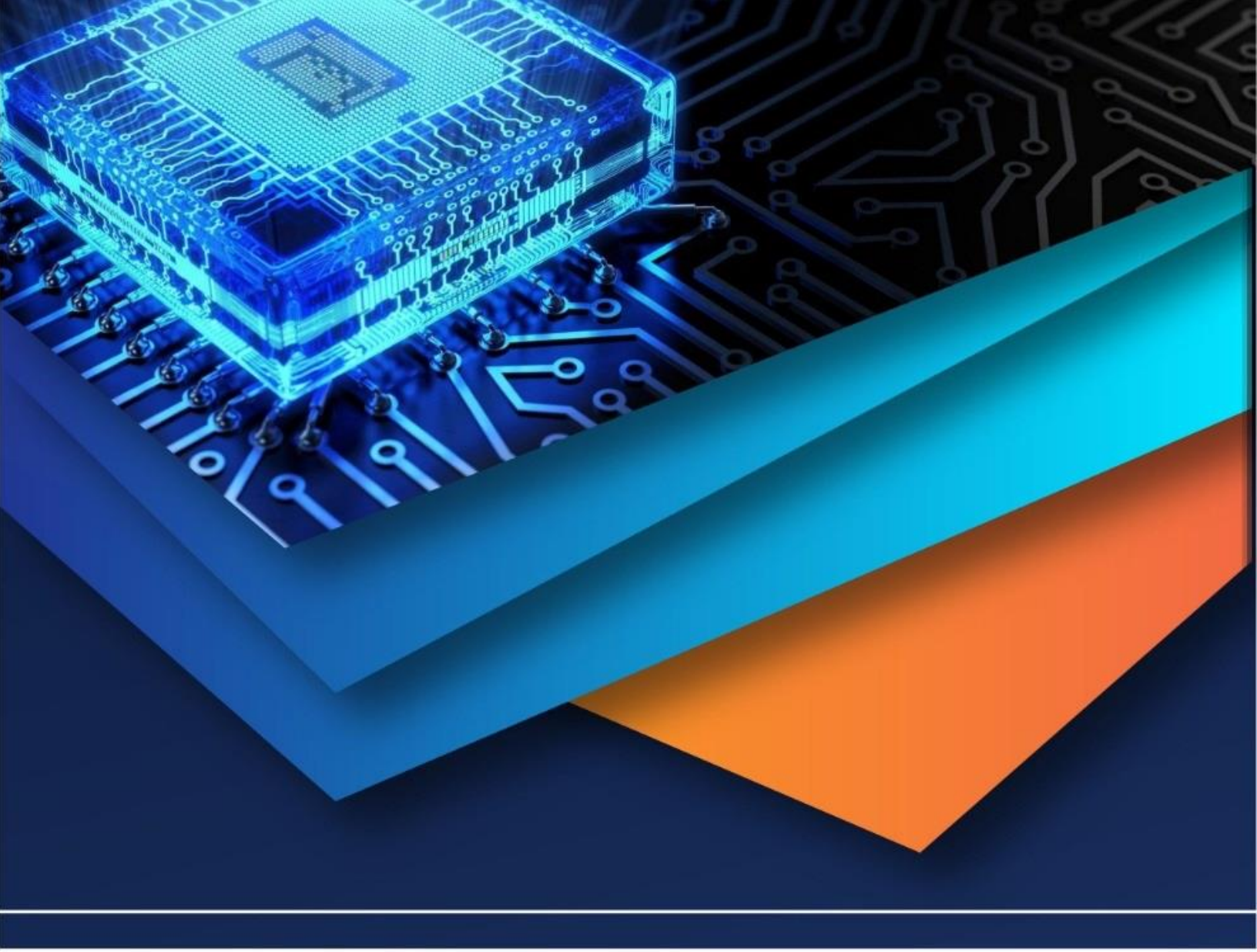
Integration with other technologies: EHR systems on the blockchain could be integrated with other emerging technologies, such as AI and IoT, to provide even more powerful healthcare solutions.

Cost reduction: By improving interoperability, reducing the risk of data breaches, and streamlining data management, blockchain-based EHR systems could help reduce healthcare costs over time.

Regulatory compliance: Blockchain technology could help EHR systems comply with regulations like HIPAA and GDPR by providing a secure and transparent way to manage patient data.

REFERENCES

[1] Madine, Mohammad Moussa, "Blockchain for giving patients control over their medical records". IEEEAccess 8 (2020): 193102-193115.
[2] Sun, Jin, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS". IEEEAccess 8 (2020): 59389-59401.
[3] Harshini, V. M., "Health record management through blockchain technology". 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2019.
[4] Liu, Xiaoguang, "A blockchain-based medical data sharing and protection Scheme". IEEE Access 7 (2019):118943-118953.
[5] Du, Mingxiao, "An optimized consortium blockchain for medical information Sharing". IEEE Transactionson Engineering Management (2020).
[6] Tith, Dara, "Application of blockchain to maintaining patient records in electronic health record for enhancedprivacy, scalability, and availability". Healthcare informatics research 26.1 (2020): 3-12.
[7] Houtan, Bahar, Abdelhakim Senhaji Hafid, and Dimitrios Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare". IEEE Access 8 (2020): 90478- 90494.
[8] Sharma, Yogesh, and B. Balamurugan, "Preserving the privacy of electronic health records usingblockchain". Procedia Computer Science 173 (2020): 171-180.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY