JOURNAL OF BASIC SCIENCE AND ENGINEERING

Blockchain-Enabled Secure and Verifiable Health Records Sharing System: Ensuring Data Integrity and Privacy

Dr Roopa R[1], Pallavi B[2], Kusha K R[3], Lakshmi Neelima[4],Dr JayaDeva T S[5]

[1]Department of ISE, BMSCE, Bangalore &Autonomous under Visvesvaraya Technological University, Belagavi, Karnataka, India
[2]Department of ML(AI&ML), BMSCE, Bangalore & Autonomous under Visvesvaraya Technological University, Belagavi, Karnataka, India
[3]Department of ML(AI&ML), BMSCE, Bangalore & Autonomous under Visvesvaraya Technological University, Belagavi, Karnataka, India
[4]Department of CSE, BMSCE, Bangalore & Autonomous under Visvesvaraya Technological University, Belagavi, Karnataka, India
[5]School of Electronics and Communication Engineering, REVA University, Bangalore, Karnataka, India

DOI: https://doie.org/10.0721/Jbse.2024982643

Abstract: The sharing of personal health records has the potential to enhance diagnostic accuracy and advance medical research. Currently, to reduce data upkeep costs, personal health records are often entrusted to third-party entities, like cloud service providers. This practice, however, raises concerns about patients losing direct control over their records, as these semi-trusted providers may compromise confidentiality and integrity. Addressing these concerns, we propose a new system for sharing personal health records electronically (EHR) built on blockchain technology. Unlike traditional approaches, our system ensures data integrity verification through a combination of symmetric encryption, attribute-based encryption, and fine-grained access control. Notably, patients can transfer attribute private keys, eliminating security issues associated with centralized attribute authorities. In our innovative system, hash values of encrypted personal health information are stored in the blockchain, with the corresponding index set saved in a smart contract. This architecture significantly improves the efficiency of data integrity verification. Through performance evaluation and security analysis, we demonstrate that our system is both secure and practical for real-world use.

Keywords: Blockchain, EHR, data integrity, encryption, security, health records, smart contract.

1. Introduction

In recent years, the rapid development of network information technology and cloud technology has had a significant impact on the way people live. The emergence of a system for sharing Electronic Health Records (EHR) based on electronic data and cloud computing enables patients to store, manage, and share their health information in a convenient, accurate, and efficient manner[1].

As a type of healthcare information recorded and managed by the patient, Electronic Health Records provide the patient with a complete and accurate online medical history. Primarily searched Strategy for symmetric encryption that ensures the cloud server cannot discover the plaintext of the keyword or the plaintext of the search results when the keyword is searched using its ciphertext[2]. Based on the differences between ciphertext and key expression forms and application scenarios, we subdivided attribute-based encryption into key policy attribute-based

encryption and ciphertext policy attribute-based encryption and developed the first key policy attribute-based encryption scheme[4]. A blockchain-based medical data gateway that provides patients with easy and private access to their data. Blockchain technology has the potential to revolutionize the healthcare industry.

The administration of Electronic Health Records (EHR) is one area where blockchain can have a substantial influence. A blockchain-based EHR sharing scheme can offer individuals with a safe and transparent platform for managing and exchanging their health information with authorized organisations. The purpose of this paper is to investigate the viability and possible benefits of a blockchain-based EHR sharing system with verifiable data integrity.

The emphasis will be on the construction of a secure and efficient system that ensures the privacy and confidentiality of sensitive health information and for the secure exchange of data between patients and healthcare providers. In this work, potential solutions to issues such as scalability, interoperability, and regulatory compliance associated with deploying such a system is been investigated. The work carried out, will also examine the possible effects of such a system on the healthcare business, such as improved patient outcomes, decreased healthcare costs, and greater data security and privacy.

On the basis of blockchain, we offer a new system for sharing personal health records whose data integrity can be verified. The new system employs symmetric encryption, attribute-based encryption, and fine-grained access control to address the challenges of privacy disclosure and loss of control rights in the process of sharing personal health records. Unlike earlier schemes of a comparable nature, the novel scheme permits patients to transfer attribute private keys to users, hence eliminating numerous security issues posed by the scheme's attribute authority.

Specifically, the new system maintains the hash values of encrypted personal health information in blockchain, and the corresponding index set is saved in a smart contract, which can further enhance the efficiency of data integrity verification. Lastly, performance evaluation and security analysis reveal that our system is secure and usable in practice.

2. Scope of the work

In the current system, patients often relinquish control of their healthcare data, with service providers assuming primary responsibility. Patient access to Electronic Health Records (EHRs) is constrained, hindering seamless sharing with healthcare professionals or researchers. The lack of interoperability among different providers, hospitals, and research organizations adds complexity to data exchange, resulting in fragmented medical records rather than a unified system. Our Proposed system overcome the flaws of the Existing System such as Patient’s access permissions to electronic health records (EHRs) are extremely restricted, and patients are often unable to easily share these records with researchers and physicians. Also enhances the interoperability issues between diverse providers, hospitals, research, etc. and the reduced safety.

The proposed introduced system leverages the groundbreaking technology of blockchain, utilizing a peer-to-peer distributed ledger for recording transactions, agreements, and

sales[3]. Key benefits of blockchain technology encompass decentralized maintenance, a block-then-chain data storage structure, secure data transfer and access, as well as tamper-proof and highly secure data integrity. Harnessing these distinctive features within an Electronic Health Records (EHRs) system, blockchain facilitates the effective management of authentication, confidentiality, accountability, and data sharing. This includes the secure transfer of information related to privacy, conservation of medical resources, and improved patient facilitation, ultimately enhancing population healthcare.

In a collaborative EHRs system hosted on a cloud storage platform with participation from multiple departments like hospitals, pharmaceutical units, insurance providers, and illness research entities, services for patients are collectively administered. To prevent EHRs misuse, individual department rights are restricted. This establishes a blockchain-based architecture for EHRs, where each patient possesses a dedicated healthcare blockchain. All relevant information, such as EHRs, consumption records, and insurance details, is encapsulated in a single block post-hospital treatment.

The patient's therapeutic journey unfolds in distinct blocks corresponding to different periods. These blocks are then arranged in chronological order to construct a comprehensive healthcare blockchain for the patient. Authorized entities can access the patient's health records through the blockchain but are unable to modify information within established blocks, ensuring the integrity of critical details like drug allergies and dosages. When patients seek treatment at other clinical departments or hospitals in the future, the new entity must authenticate the patient and validate their blockchain. This approach not only conserves medical resources but also prevents redundant examinations.

3. Module Design

The level 1 design (high-level architecture) gives an overview of the system architecture, its components, and their relationships. This design level specifies the system's high-level structure, as well as its primary functional and nonfunctional needs.

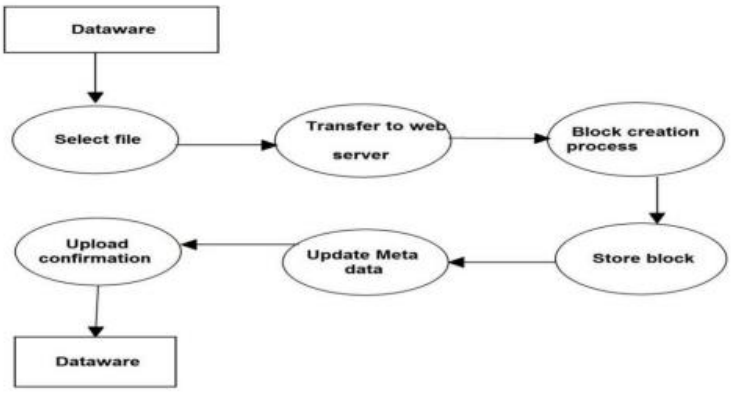

Figure1: Level1-Overview of the system architecture

Level 2 Design (Detailed Component Design): The level 2 design provides a more comprehensive perspective of the system's components and their interactions. This design

level specifies the internal architecture of each component, including algorithms and data structures, as well as component interfaces.

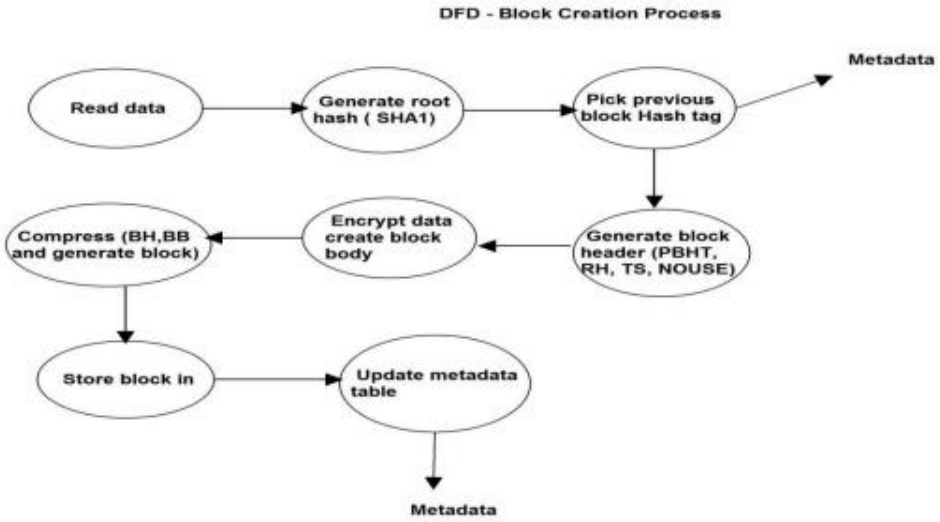

Figure 2: Level2- Data Flow Diagram

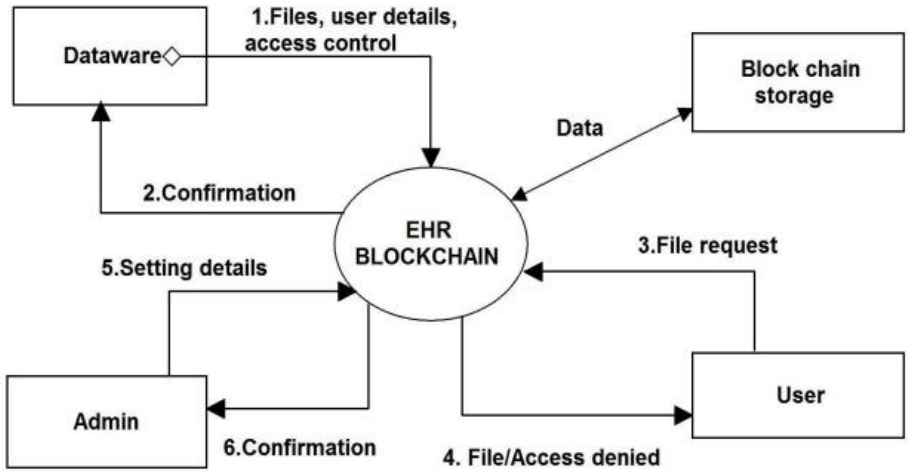

Figure 3: Level3- Data Flow Diagram

Level 3 Design (Implementation Design): The level 3 design outlines how each component will be implemented in code at the lowest level of detail. This level of design specifies the programming language, tools, and libraries that will be utilized, as well as the algorithms and data structures for each component in detail. It also includes the actual implementation of each component's code.

The design and implementation in our work comprises several key components, but not limited to blockchain technology, also includes a peer-to-peer distributed ledger, symmetric encryption, attribute-based encryption, fine-grained access control, smart contracts, and hash values which performs the following functionalities:

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

- Blockchain Technology: The blockchain is established through a consensus algorithm, ensuring a decentralized and tamper-resistant ledger.
- Symmetric Encryption: Utilizing algorithms for secure encryption, ensuring confidentiality of personal health records.
- Attribute-Based Encryption: Employing advanced cryptographic methods for attribute-based access control.
- Fine-Grained Access Control: Developing mechanisms for precise control over access permissions based on attributes.
- Smart Contracts: Creating self-executing contracts to automate and enforce data integrity rules within the blockchain[.
- Block-Chain Service: Verifies transactions on the blockchain to ensure they meet consensus rules and are valid. create new blocks in the blockchain using consensus algorithms. Performing cryptographic operations to secure data on the blockchain, including encryption of sensitive –HER.Manages public and private keys associated with blockchain addresses to facilitate secure transactions and access control
- IPFS service- encompasses a range of functionalities related to decentralized file storage, retrieval, sharing, and content addressing provided by the InterPlanetary File System protocol.

3.1. Integration of Elements:

- The blockchain is implemented as the foundation, with each patient having a dedicated blockchain encapsulating their health records.
- Symmetric encryption and attribute-based encryption are integrated to ensure secure and controlled access to health records.
- Fine-grained access control is applied to manage and restrict permissions for different entities within the system.
- Smart contracts, blockchain and IFS services are employed to automate processes, such as the verification of data integrity, encryption, decryption and access permissions.

A patient registers into the system to access their own health records, which may include their medical history, lab results, and prescription information. The patient is able to examine their information, change it as needed, and share it with approved healthcare practitioners.

✓ Access to Patient Records by Healthcare Providers A healthcare provider logs into the system to access a patient's personal health records. The provider can see the patient's information, add new information, and modify existing data as necessary. The provider must be permitted to access the patient's information, and any modifications they make must be validated to ensure data integrity.

✓ A researcher logs into the system in order to get de-identified health records for a clinical research project. The researcher must possess the required authorizations and adhere to stringent privacy and security measures. The integrity of the data utilised in the study must be confirmed.

✓ A healthcare provider logs into the system to access the patient's personal health records in preparation for a telemedicine appointment. During the consultation, the physician can view the patient's information and add new information to the patient's

record. The data integrity of the modifications made to the patient's record must be validated.

✓ A healthcare professional logs into the system to exchange health information with another healthcare practitioner. The provider must be permitted to access the data and comply with stringent privacy and security measures. The integrity of the data being exchanged must be checked.

✓ Clinical Decision Support: A healthcare provider logs into the system to view the personal health records of a patient in order to support clinical decision-making. To make informed treatment decisions, the practitioner can access the patient's information, including lab findings and medical history. The data integrity of the information used to support clinical decision-making must be checked.

The combination and integration of these elements collectively contribute to the effectiveness and innovation of the Blockchain Based Personal Health Records Sharing Scheme with Verifiable Data Integrity.

4. Implementation snippets and Results

Overall, the implementation of a Blockchain based personal health records sharing scheme with verifiable data integrity has the potential to revolutionize how personal health information is managed, shared, and utilized, with numerous benefits for patients, healthcare providers, and the healthcare industry as a whole.The snippets of implementation are as shown below:

- Smart Contracts steps and snippet:

Install Solidity: To develop and test smart contracts, you'll need to set up a development environment like Truffle or Remix. Here, we'll use a basic Solidity contract structure.

```
pragma solidity ^0.8.0;

contract HealthRecords {
    // Structure to store health record
    struct HealthRecord {
        uint256 id;
        string patientName;
        string dataHash;  // Hash of the health record data for integrity
        address owner;    // Owner of the record
        address[] sharedWith;  // Addresses with whom the record is share
        bool exists;      // Check if record exists
    }

    // Mapping of record ID to HealthRecord
    mapping(uint256 => HealthRecord) private records;
```

```
    // Function to create a new health record
    function createRecord(uint256 id, string memory patientName, string memory dataHash) p
        require(!records[id].exists, "Record with this ID already exists");

        // Create a new health record
        HealthRecord memory newRecord = HealthRecord({
            id: id,
            patientName: patientName,
            dataHash: dataHash,
            owner: msg.sender,
            sharedWith: new address ,
            exists: true
        });

        // Store the record in the mapping
        records[id] = newRecord;
```

- Blockchain Service snippet:

```
import { HttpClient } from '@angular/common/http';
import { Injectable } from '@angular/core';
import { rejects } from 'assert';
import { resolve } from 'dns';
import Web3 from 'web3';
import { IpfsService } from './ipfs.service';
import { ECIESService } from './ecies.service';
import { log } from 'console';

const Contract = require('../../build/contracts/Contract.json');

declare let window: any;

@Injectable({
    providedIn: 'root',
})
export class BlockchainService {
    account: any = [];
    netId: any;
    web3!: Web3;

    address: any;
    contract: any;
    networkData: any;
    abi: any;

    admin: any;

    balance: any;

    blockNumber: any;
```

- IPFS Service snippet**:**

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

```
import { Injectable } from "@angular/core";

const IPFS = require("ipfs-mini");

@Injectable({
  providedIn: "root",
})
export class IpfsService {
  ipfs: any;
  infura: string = "ipfs.infura.io";
  local: string = "127.0.0.1";
  constructor() {
    this.ipfs = new IPFS({
      host: this.local,
      port: 5001,
      protocol: "http",
    });
  }

  getIPFS() {
    return this.ipfs;
  }
}
```

```
import { TestBed, async, inject } from '@angular/core/testing';
import { IpfsService } from './ipfs.service';

describe('Service: Ipfs', () => {
  beforeEach(() => {
    TestBed.configureTestingModule({
```

- Environments snippet:

```
export const environment = {
  production: false
};

export const infuraAPI = 'https://ipfs.infura.io/ipfs/'
export const localAPI = 'http://127.0.0.1:8080/ipfs/'

export const JAVA_API = 'http://localhost:4201/api/'
export const NODE_API = 'http://localhost:4202/'
```

- Python (Django) steps for Disease Prediction Based on chest X-Ray:

  - **Model Loading and Prediction**: Load a pre-trained model and use it to predict diseases from chest X-ray images.
  - **Blockchain**: Implement a simple blockchain to record predictions securely.

- **Django**: Create a Django application to upload images, make predictions, and record them in the blockchain.

- Django models snippet:

```
from django.db import migrations, models


class Migration(migrations.Migration):

    initial = True

    dependencies = [
    ]

    operations = [
        migrations.CreateModel(
            name='Doctor',
            fields=[
                ('id', models.BigAutoField(auto_created=True, primary_key=True, serialize=False, verbose_name='ID')),
                ('fName', models.CharField(max_length=50)),
                ('lName', models.CharField(max_length=50)),
                ('dateOf', models.DateTimeField()),
                ('email', models.EmailField(max_length=254)),
                ('city', models.CharField(max_length=20)),
                ('state', models.CharField(max_length=20)),
                ('docId', models.CharField(max_length=100)),
                ('department', models.CharField(max_length=10)),
                ('image', models.ImageField(upload_to='')),
            ],
        ),
    ]
```

- Encrypt and Decrypt EHR snippet:

```
    public String encryptEHR(String _SK, String EHR) throws Exception {

        byte[] decodedKey = Base64.getDecoder().decode(_SK);
//        rebuild key using SecretKeySpec
        SecretKey SK = new SecretKeySpec(decodedKey, 0, decodedKey.length, "AES");

        Cipher cipher = Cipher.getInstance("AES");
        cipher.init(Cipher.ENCRYPT_MODE, SK);

        byte[] cipherEHR = cipher.doFinal(EHR.getBytes());

        return Base64.getEncoder().encodeToString(cipherEHR);
    }

    public String decryptEHR(String _SK,String _CEHR) throws Exception{
//        decode the base64 encoded string
        byte[] decodedKey = Base64.getDecoder().decode(_SK);
//        rebuild key using SecretKeySpec
        SecretKey SK = new SecretKeySpec(decodedKey, 0, decodedKey.length, "AES");

        Cipher cipher = Cipher.getInstance("AES");
        cipher.init(Cipher.DECRYPT_MODE,SK);

        byte[] cipherEHR = cipher.doFinal(Base64.getDecoder().decode(_CEHR));

        return new String(cipherEHR);
    }
```


Vol. 21, No. 1, (2024)
ISSN: 1005-0930

- Symmetric Key Controller snippet**:**

```java
@RestController
@RequestMapping("api/getSymmetricKey")
@CrossOrigin("*")
public class SymmetricKeyController {

    Logger logger = LoggerFactory.getLogger(SymmetricKeyController.class);
    AESFunctions aes = new AESFunctions();

    @GetMapping()
    public ResponseEntity<SymmetricKeyResponse> generateSymmetricKey() {
        SymmetricKeyResponse symmetricKey = new SymmetricKeyResponse();
        try {
            long startTime = System.nanoTime();
            String sk = aes.generateSK();
            long endTime = System.nanoTime();
            symmetricKey.setSK(sk);
            symmetricKey.setTime(endTime - startTime + " ns");
            logger.info("SK : " + sk);
            return new ResponseEntity<>(symmetricKey, HttpStatus.OK);
        } catch (Exception e) {
            logger.error("ERROR : " + e.getLocalizedMessage());
            return new ResponseEntity<>(null, HttpStatus.NOT_FOUND);
        }
    }
```

4.1. RESULTS:

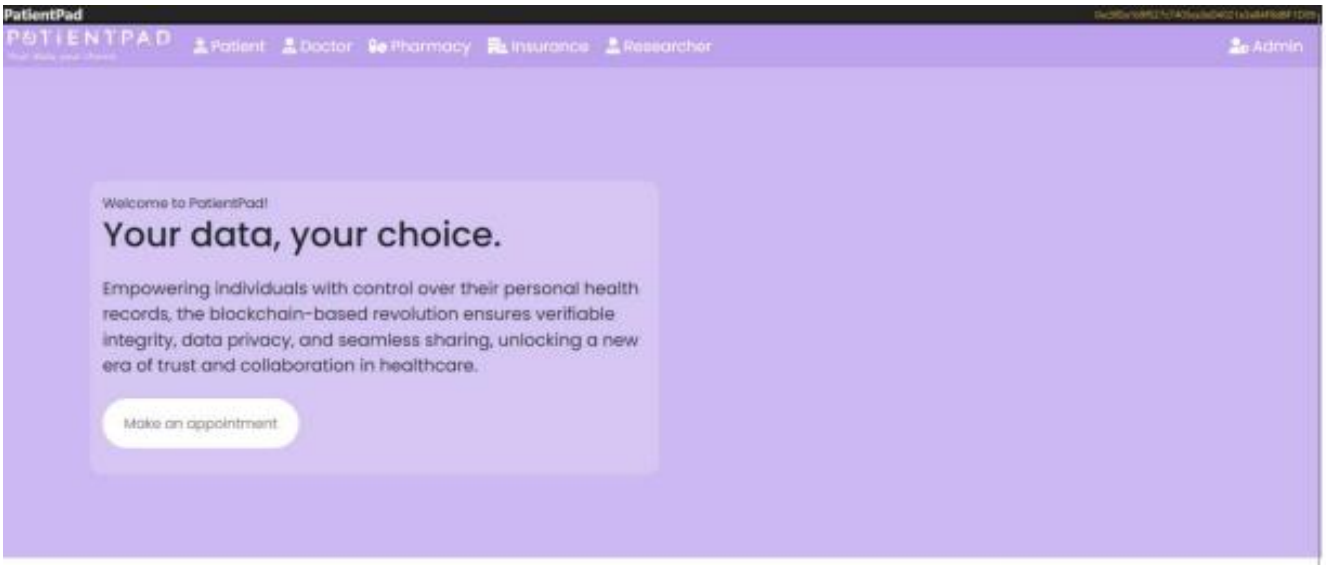

Figure 4: Homepage of PatientPad

The homepage showcases a user-friendly interface where patients can easily make appointments. The navigation bar prominently features login options for patients, doctors, researchers, insurance providers, and administrators, ensuring secure access for different stakeholders.

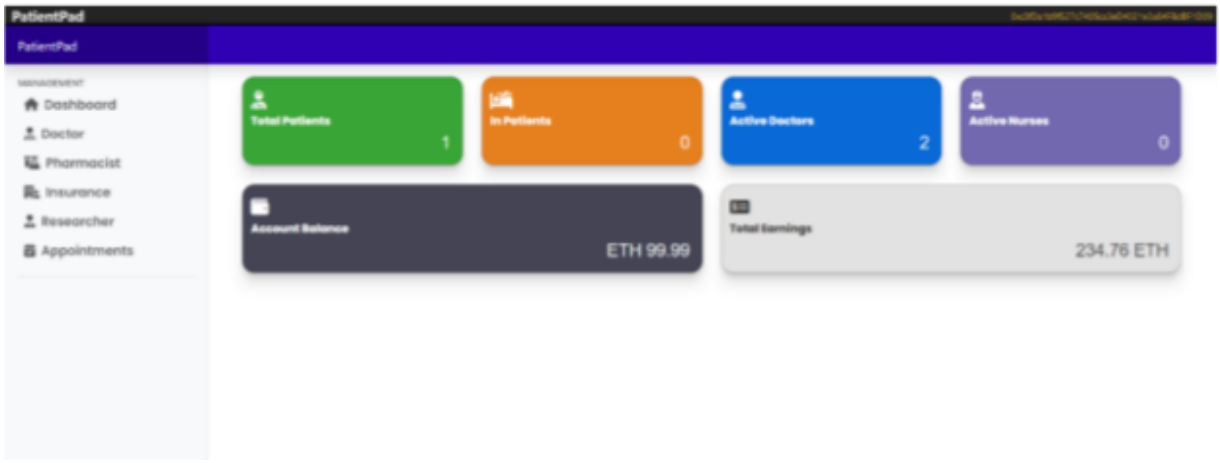

Figure 5: Admin Dashboard

The admin dashboard provides a centralized interface for managing healthcare actors. Admin can add doctors, researchers, insurance, and pharmacies, facilitating seamless collaboration. The dashboard displays essential information such as total patients, account balance, and active doctors, enabling efficient monitoring and administration.

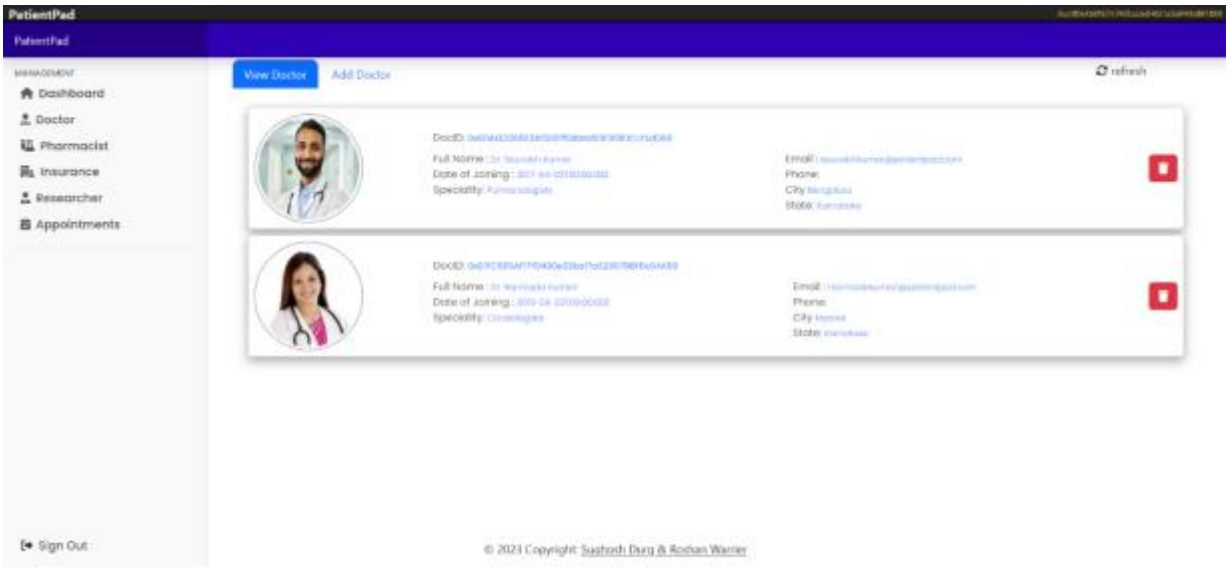

Figure 6: Admin Login-Doctor Management

The appointment booking interface empowers patients to select doctors based on their preferred choice and specialty. This user-friendly interface enhances patient engagement and promotes a patient-centered healthcare experience.

Vol. 21, No. 1, (2024)
ISSN: 1005-0930

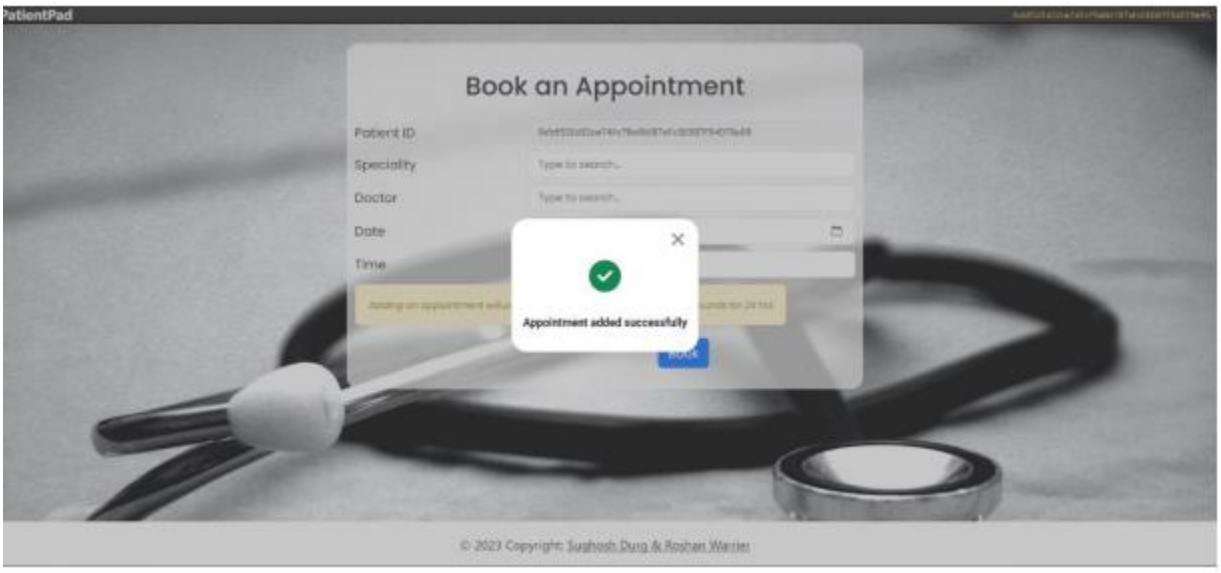

Figure 7: Booking an Appointment

The doctor prescription and diagnosis interface allows doctors to seamlessly write prescriptions for patients, including symptoms, dosage, and medicines prescribed. The interface also enables doctors to predict chest diseases by uploading patient images, enhancing diagnostic accuracy.

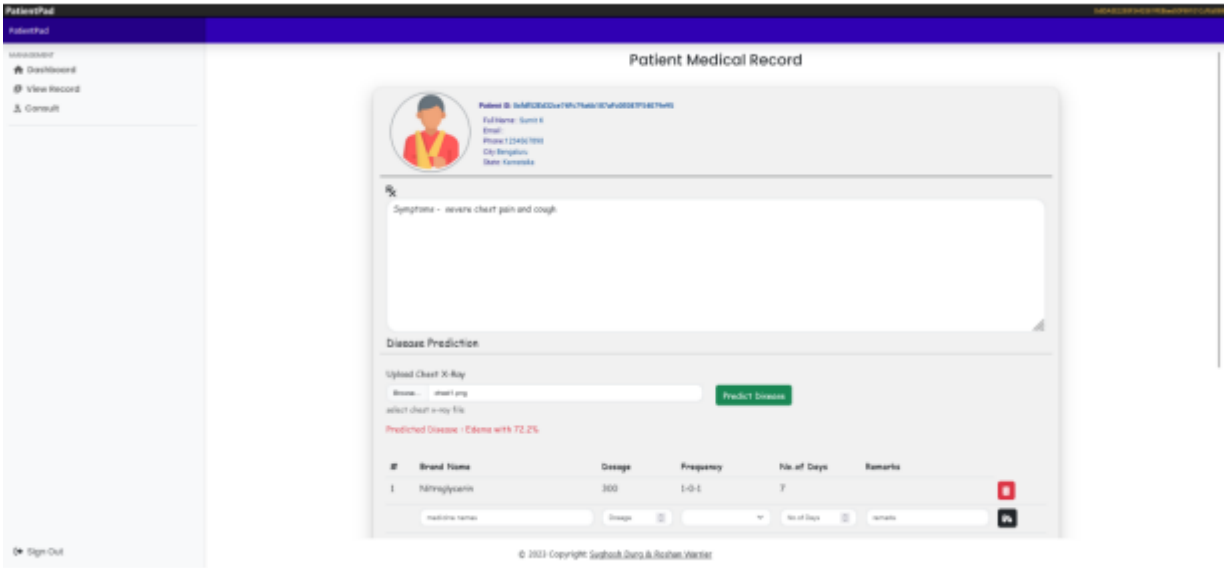

Figure 8: Doctor noting the Prescription

The patient dashboard offers a centralized platform for individuals to access and manage their medical records securely. Patients can view their health information, share record selectively with doctors, pharmacies, insurance agencies, and researchers, fostering collaborative care.

The dashboard enables patients to maintain control over their health data while facilitating personalized and informed healthcare decisions. Additionally, patients can appoint a nominee to ensure continuity of care and support in their healthcare journey.

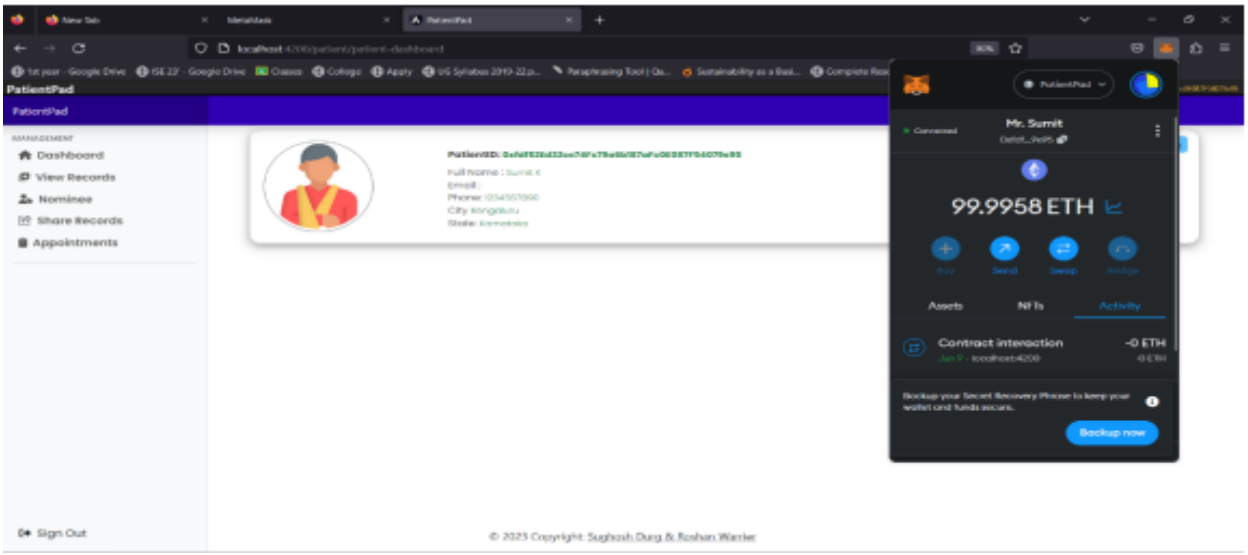

Figure 9: Patient Dashboard

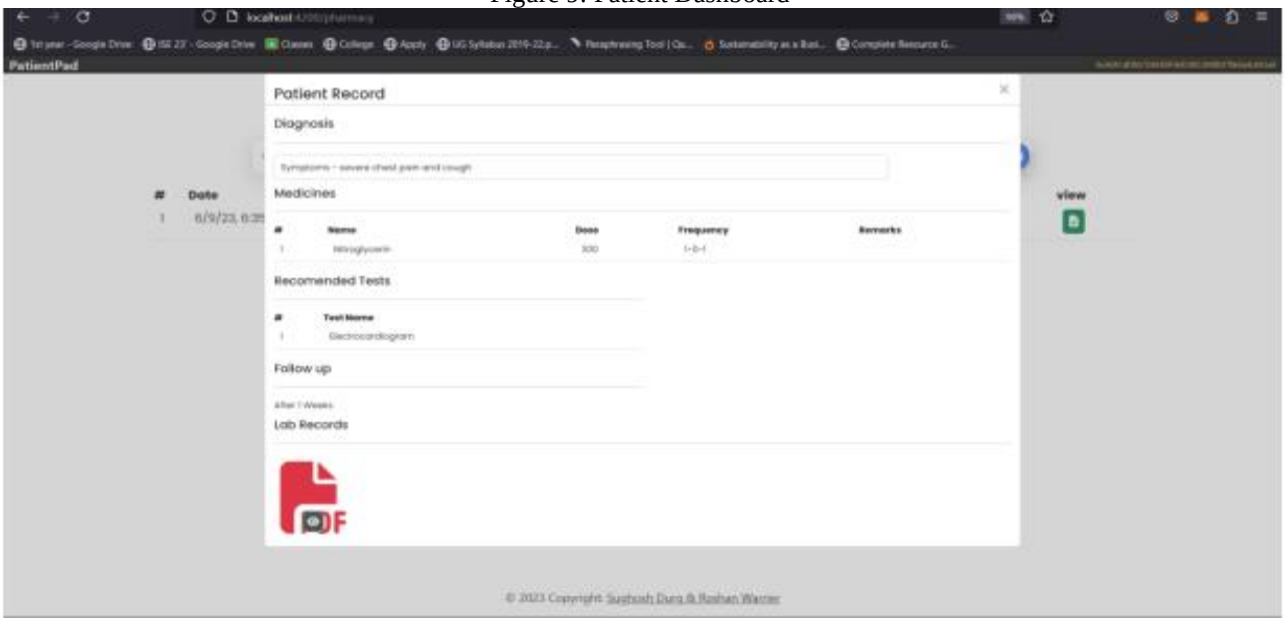

Figure 10: Pharmacy Viewing Patient's Record

The pharmacy interface allows pharmacies to view patient records that have been shared with them. This secure access enables pharmacies to retrieve relevant medical information and ensure accurate dispensing of medications.

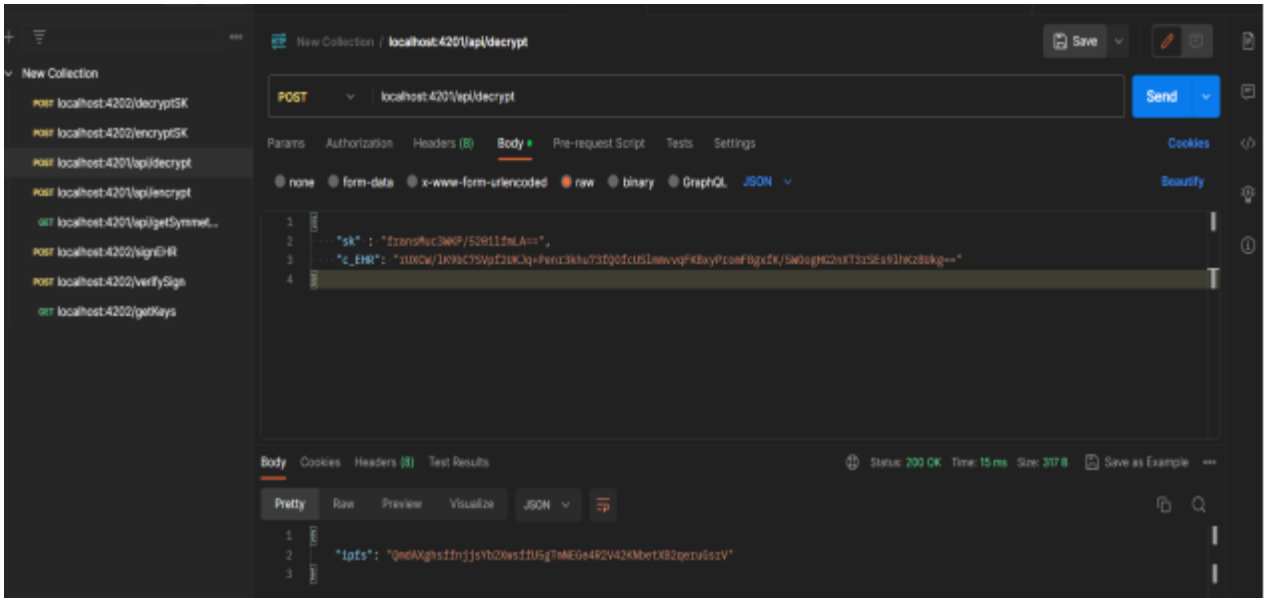

Figure 11: Encryption and Decryption Testing on Postman

The figure illustrates the encryption and decryption testing process on Postman, utilizing symmetric key encryption and PR-SHA (Pseudorandom Secure Hash Algorithm). This testing verifies the effectiveness of encryption algorithms in securing data during transmission. By simulating various scenarios, the encryption testing ensures that sensitive information remains protected and inaccessible to unauthorized parties.

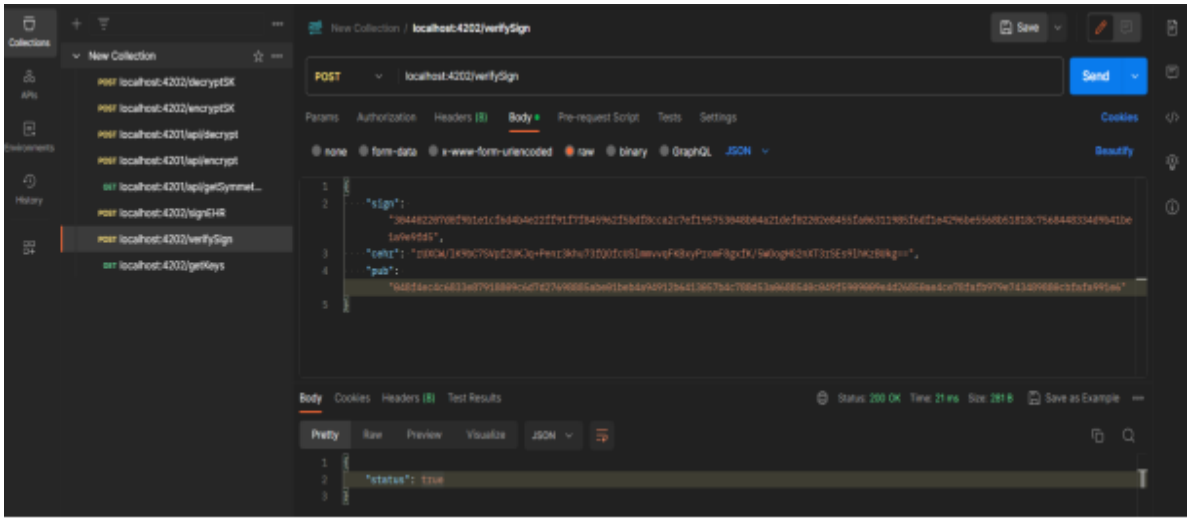

Figure 12: Verifying Signature Keys

The figure 12 demonstrates the process of verifying signature keys on Postman, ensuring the authenticity and integrity of data transmitted. By validating the signature keys, the system confirms that data originates from a trusted source and has not been tampered with during transit.

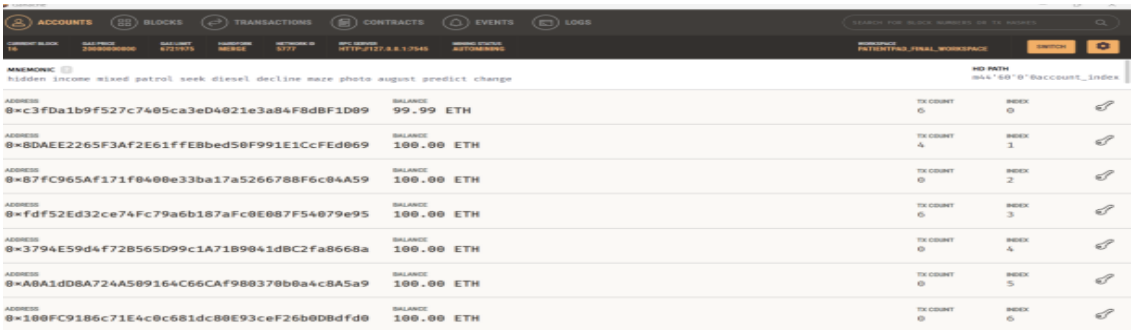

Figure 13: Ganache

The figure 13 showcases the simulation of the Ethereum blockchain platform on Ganache, a local blockchain development tool. This simulation environment enables developers to test and deploy smart contracts, interact with decentralized applications, and simulate blockchain transactions.

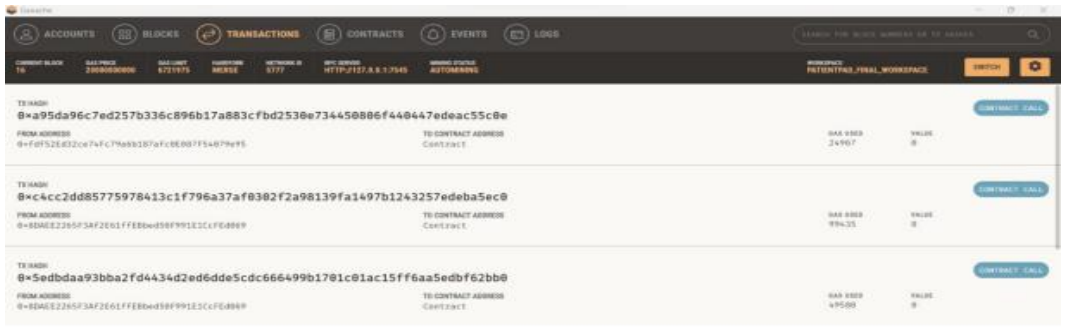

Figure 14: Transactions

The proposed implemented system enables rapid access to patient records to enhance care coordination and efficiency, provides accurate, current, and comprehensive patient information at the point of care, securely supports sharing electronic information with patients and other physicians. Also provides the clinicians diagnose patients more accurately, eradicate medical errors, and provide safer treatment and improves patient-provider engagement and communication, as well as health care accessibility by facilitating safer and more reliable prescription.

5. CONCLUSION AND FUTURE ENHANCEMENTS:

In conclusion, the PatientPad – A Decentralized Solution for EHR Sharing presents a robust solution for seamless Electronic Health Record (EHR) sharing using blockchain technology. The application offers a user-friendly interface that caters to the needs of different healthcare actors, including admins, doctors, and patients. Through the implementation of smart contracts and decentralized storage, the application ensures data integrity, privacy, and secure access to medical records.

The system successfully addresses the challenges of interoperability and data security in healthcare by leveraging blockchain's immutable and transparent nature. The admin functionalities allow for efficient management of doctors, pharmacies, insurance companies, and researchers, ensuring seamless collaboration and coordination among these stakeholders. The patient-centric approach

enables patients to book appointments, consult specific doctors, and grant access to authorized entities, empowering them to take control of their healthcare journey.

The work carried can be further enhanced by implementing enhanced data analytics capabilities, Integration with Telemedicine to facilitate virtual consultations, integration of AI and Machine Learning: Integrate AI and machine learning algorithms and continuously enhance the security measures by implementing multi-factor authentication and regular security audits to safeguard sensitive patient data and prevent unauthorized access.

References:

[1 S. Wang, D. Zhang and Y. Zhang, "Blockchain-Based Electronic Health Records Sharing Scheme With Data Integrity Verifiable," in IEEE Access, vol. 7, pp. 102887-102901, 2019

[2] Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," in IEEE Access, vol. 5, pp. 14757-14767, 2017

[3] Tsung-Ting Kuo, Hyeon-Eui Kim, Lucila Ohno-Machado, Blockchain distributed ledger technologies for biomedical and health care applications, Journal of the American Medical Informatics Association, Volume 24, Issue 6, November 2017, Pages 1211–1220

[4] Huige Li, Fangguo Zhang, Jiejie He and Haibo Tian, “A Searchable Symmetric Encryption Scheme

using BlockChain”, arXiv - CS - Cryptography and Security(IF)Pub Date: 2017-11-03

[5] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), 2016, pp. 25-30

[6] Kumar, Adarsh et al. “A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes.” IEEE Access 8 (2020): 118433-118471.

[7] Omar, Ilhaam & Jayaraman, Raja & Debe, Mazin & Salah, Khaled & Yaqoob, Ibrar & Omar, Mohammed. (2021). Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts. IEEE Access. PP. 1-1.

[8] Sabita Khatri, Fahad Ahmed Alzahrani, Md Tarique Jamal Ansari, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan “A Systematic Analysis on Blockchain Integration With Healthcare Domain: Scope and Challenges” Received April 17, 2021, accepted June 3, 2021, date of publication June 9, 2021, date of current version June 17, 2021

[9] Lee, Ah & Kim, Min & Won, Kyung & Kim, Il & Lee, Eunjoo. (2020). Coded Dynamic Consent framework using blockchain for healthcare information exchange. 1047-1050

[10] W. Bodeis and G. P. Corser, "Blockchain Adoption, Implementation and Integration in Healthcare Application Systems," SoutheastCon 2021, 2021, pp. 1-3

[11] M. Kaur, M. Murtaza and M. Habbal, "Post study of Blockchain in smart health environment," 2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), 2020, pp. 1-4

[12] M. A. Bazel, F. Mohammed and M. Ahmed, "Blockchain Technology in Healthcare Big Data Management: Benefits, Applications and Challenges," 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA), 2021, pp. 1-8

[13] S. Aich et al., "Protecting Personal Healthcare Record Using Blockchain & Federated Learning Technologies," 2021 23rd International Conference on Advanced Communication Technology (ICACT), 2021, pp

[14] Yue, Xiao & Wang, Huiju & Jin, Dawei & Li, Mingqiang & Jiang, Wei. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. Journal of medical system

[15] G. Zyskind, O. Nathan and A. '. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," 2015 IEEE Security and Privacy Workshops, 2015, pp. 180-184