Original Article

DRBAC-Healthchain (DRBAC-HC): Decentralized Role Based Access Control Framework For Achieving Security And Privacy Using Blockchain In Healthcare System

Avani Dadhania[1], Dr.Hiren Patel[2]

[1]Assistant Professor, Department of Computer Engineering, LDRP Institute of Technology and Research, Sarva Vidyalaya Kelavani Mandal, Gandhinagar, Gujarat, India. Email:avani26.22@gmail.com

[2] Professor, Department of Computer Engineering, Vidush Somani Institute Of Technology and Research, Sarva Vidyalaya Kelavani Mandal, Kadi, Gujarat, India. Email:hbpatel1976@gmail.com

Corresponding Email:avani26.22@gmail.com

DOI: 10.47750/pnr.2023.14.03.368

Abstract

With the Internet of Things' (IoTs) rapid expansion, effect, and potential, the healthcare industry is shifting to a new paradigm that permits wearable devices to collect patient medical data and use it for monitoring and diagnosis. Tamper-proof data and avoidance of the centralized record-keeping mechanism are crucial requirements in any wellness system due to its exigent and precise necessity of data requests. Along with the same, transactions' auditability and revocation of access rights upon certain records for specific stakeholders are also a few of the other prerequisites in the medical segment. Blockchain, as a distributed ledger, offers a solution for securely storing data while providing transparency in transactions and interactions among stakeholders. Synchronous interaction among patient, doctor, pharmacy, consultant, hospital, etc. with all possible data security is another concern that could be resolved through the usage of Blockchain's smart contracts wherein interaction among these stakeholders is permitted in a traceable and irreversible mode. The purpose of this paper is to discuss the potential use of Blockchain technology in the healthcare sector to achieve data security, transparency, and reliability without the involvement of a trusted third party. In terms of security and privacy, we survey and provide an exhaustive review of Blockchain-based access control systems for the healthcare system. In addition, for the healthcare system, we propose and implemented a decentralized role-based access control model based on Ethereum smart contract.

Keywords: Internet of Things, Role Based Access Control, Healthcare System, Blockchain technology.

I. INTRODUCTION

The Internet of Things (IoT) has been revolutionized due to a large growth in the number of wireless sensors, wearable devices, and smart objects that collect information, analyze it, and perform some actions in inventive ways to connect the world. The IoT is a digital infrastructure that allows different resources, users, objects, and devices to communicate with one another. Numerous IoT applications from a variety of industries, including agriculture, healthcare, smart cities, smart homes, and smart cars among others, considerably improve our daily life. Healthcare sectors have become more advanced due to adaptation of IoT. However, security and privacy of patient's healthcare records is a major concern in IoT. The limited processing capabilities of IoT devices prohibit the direct deployment of conventional security countermeasures and privacy enforcement. Additionally, there are scalability problems caused by the large number of connected devices. Security measures should include protection for data integrity, confidentiality, and anonymity. In order to prevent unauthorized users (people and machines) from accessing the system, authentication and authorization mechanisms are also needed [1]. In recent years, access control mechanism been presented as a solution to the problem of unauthorized users accessing secured network resources illegitimately. Access control combines set of policies and rules for accepting or denying the access or constraint access to the resources or services for legitimate users [2]. Access control architecture is developed based on access control model, mechanisms and access control policies for

authorization of data, resources and services [3]. Access control mechanism in healthcare system, where user' access to electronic health records, is highly regulated to prevent data leakage and misuse. The static and centralized architecture in the aforementioned domain puts several limits on access control frameworks for healthcare systems. Centralized access control is extremely difficult to implement, as it can quickly become a bottleneck and it is hard to survive with traditional solutions. To deal with the large-scale and distributed existence of healthcare system, access control must be decentralized and trustworthy (i.e., resistant to attacks). In the healthcare system, a general policy could be, "Authorized doctors should access specific patient's record." Since there are various specializations of doctors, and sometimes only one specialization (e.g., cardiologist) is permitted to view the record, or even more precisely, only the cardiologist in charge of specific patient. This policy is too complex to reliably monitor user request. As a result, fine-grained access control is one of the most satisfying criteria for it [4]. The access control system should also be distributed to prevent single points of failure, flexible and scalable to support a large number of users, lightweight to suit resource-constrained environments, and installed at the edge of the network to provide real-time response [2].It is required to get the answers of these concerns to accomplish the different form of routine life.

1.1 Problem Statement

The IoT is encouraging technology for developing the novel applications to provides healthcare system for doctors, patients and other stakeholders. Primary concerns about the healthcare domain are the privacy (to be specific, access control), confidentiality and integrity. Privacy of the patient's records is the major challenge for IoT infrastructure. End-to-end security cannot be ensured without addressing the privacy issues like access control, authentication and non-repudiation. Dynamic nature of IoT devices, limited storage capacity, low computational speed and centralized architecture require high level security of patient's sensitive information. So, these characteristics require the solutions that are explicitly intended for the healthcare field. In the healthcare system, where IoT devices are resource constrained and with its large scale management, the appropriate access policies for resources and users are critical and complex issue [5].

Following questions prompted us for the work.

How to built access control framework for healthcare records?

How to implement privacy for health care records for distributed architecture?

How should access control be handled for patient's data in the context of a healthcare system?

1.2 Contribution

The goal of this study is to analyze the applicability of a fine-grained role-based access control system for a healthcare system. This paper proposes decentralized Role-based access control architecture for authorization of users and privacy of patient's records using Blockchain Technology.

We contribute the following in order to meet the aforementioned requirements:

- We provide access control architecture based on access control policies that are role-based, fine-grained, and decentralized.
- We provide the data encryption and decryption based on public key cryptography.
- We provide system design, architecture, and implementation with Performance and security analysis.

1.3 Organization

The rest of the paper is organized as follows: Section 2 examines related works. Section 3 shows the Blockchain Technology. The system architecture is presented in section 4. The proposed work and algorithms are presented in Section 5. Section 6 shows experimentation setup. Section 7 describes the results obtained using various performance measurements. Section 8 shows security analysis and, finally, Section 9 concludes.

II. RELATED WORK

In this section, we provide a systematic literature review of the access control solutions for data sharing using Blockchain Technology in the medical field. IoT devices or wearable devices are used in smart healthcare systems to track patient's health and capture healthcare data. The collected health data can then be uploaded to a server and shared with a limited number of registered users viz. doctors and nurses, for instance. Since medical reports are normally confidential, it is

important that security concerns of user's health records are addressed [6,7,8]. It is crucial to manage and keep track of who is using which resources in the healthcare system. The resources are connected in IoT network which require the scalable and secure healthcare system [6]. It is critical to ensure that smart healthcare records are stored and accessed securely in modern systems. So, in recent years, major contribution has been carried out for the usage of IoT in the Healthcare sector. Security issues in IoT enabled healthcare system are highlighted in several existing research contributions. The Internet of Things (IoT) promises to make our everyday lives easier by transforming any physical item into a smart object that can sensing the environment, interact with other devices, and respond accordingly to changes in the general environment. While this reduces the cost of usage and improves the client experience, it also raises a number of security and privacy concerns. [7, 8, 9]. In this [10] Author proposed an Ancile Framework to achieve decentralization using blockchain to manage electronic healthcare records by giving ownership of the records to patient to control the access of the record and protect from unauthorized users to derive the personal healthcare information and cryptographic techniques to achieve privacy and interoperability of nodes. Dabbagh, M et al. [11] proposed a policy-based access control framework for lightweight healthcare resources to provide fine grained access control to the users to services by using attribute, roles and capabilities for this architecture which employing attributes for role assignment and issuing capabilities to access specific services provided by IoT devices. Shantanu Pal et al. [12] proposed a policy based access control architecture for constrained resources for fine grained access which combine the attributes, roles and capabilities together in the policy. In this architecture roles are assigned to users by using attributes for policy management and based on that capability is generated for access authorization. Na Shi et al. [13] introduced a blockchain based access control scheme for distributed IoT environment for access right authorization and revocation that provides privacy using symmetric encryption algorithm by implementing private blockchain network. In [14] author proposed a secure architecture for access rights delegation in large scale IoT system using public and private blockchain to maintain privacy of attributes. Joao Pedro Dias et al. [15] proposed a blockchain based access control approach for E-health care records that provides fine grained access control by preserving the information in the form of transaction in the blockchain that contain information about access policy state machine, record life-cycle state machine and individual authorization state machine. Gautami Tripathi et al. [16] provided a model that collects the patient's sensitive and personal healthcare records from different sensors attached to patients are encrypted and stored in the distributed storage using blockchain technology So that data can be accessed by legitimate users only. Randhir Kumar et al. [17] presented an improved Bell–LaPadula model and enforced access control policies in smart contracts using the permissioned blockchain framework to solve scalability concerns in IoT. In the Bell–LaPadula model, a subject can only access resources if and only if the subject has a clearance level higher than the object. Sara Ruhani et al. [4] proposed a distributed attribute-based access control system for digital libraries that uses permissioned blockchain to achieve high efficiency and low computational overhead, as well as providing an authentication service for off-chain parties.

III. BLOCKCHAIN TECHNOLOGY

3.1 Blockchain

Blockchain technology is emerging as the next technological advance, following the introduction of crypto- currencies such as Bitcoin [18]. It plays a crucial role in the shift from centralized client-server architecture to a decentralized, cryptographically secure system. Furthermore, the blockchain is a decentralized, unchangeable ledger that may be used to track financial transactions. It is made up of a series of time-stamped blocks connected together by cryptographic hashes [19].

3.2 Blockchain Features

3.2.1 *Immutability*: Immutability refers to the inability to change or alter anything. The distinguishing characteristic of blockchain is that the network won't alter and will always exist.

3.2.2 *Decentralized Network*: The blockchain is a decentralized network, meaning no single authority is in charge of all the decision. The identical copy of the ledger is shared by each node in the blockchain network.

3.2.3 *Distributed ledger*: Each member of the network has a copy of the ledger, which guarantees total transparency. A public ledger will contain complete information about all network participants and transactions. Each network participant has their own identical copy of the distributed ledger, which is a consensus of replicated, shared, and synced digital data that covers the whole blockchain network.

3.2.4 *Consensus*: Blockchain technologies are highly successful due to the consensus algorithm. For the group of network nodes, reaching a consensus is a decision-making process. In this case, the nodes can concur fairly rapidly. When millions of nodes are validating a transaction, a consensus is necessary for the system to function properly.

3.2.5 *Security*: All the records in the network are individually encrypted which offers additional degree of protection to the entire blockchain process network. Due to their cryptographically hashing, each piece of data on the block has a distinct identity. Each block has a unique hash as well as the previous block's hash.

3.2.6 *Transparency*: Members can look into the status of any transaction while it is in progress, even if the structure is significantly altered. As a result, on a Blockchain, any activity or transaction is completely transparent.

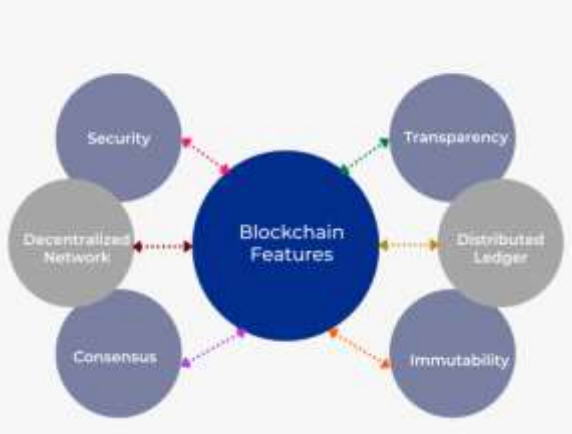

Figure 1: Features of Blockchain

3.3 Types of Blockchain

3.3.1 *Public Blockchain*: The public Blockchain network is open to everyone with no restrictions on validation or participants. On the public blockchain, user has permission to mine, read recent and old records, confirm transactions, or carry out proof-of-work for incoming blocks.

3.3.2 *Private Blockchain*: A blockchain with permissions or restrictions that may only be utilized in a closed network is referred to as a private blockchain. In a firm or organization where only a small number of people are permitted to participate in a blockchain network, private blockchain are often used.

3.3.3 Consortium Blockchain: A consortium blockchain is a semi-decentralized, in which a blockchain network is managed by more than one organization.

3.3.4 Hybrid Blockchain: The benefits of both private and public blockchains are combined in a hybrid blockchain. It allows for both private and public permission-based systems and offers to the advantages of both private and public blockchain.

3.4 Smart Contract

According to Nick Szabo, an American computer scientist who introduced a virtual currency called "Bit Gold" in 1998, Smart contracts are computerized transaction protocols that carry out the conditions of a contract [21].Smart contracts are nothing more than computer programmes that are stored on a blockchain may automatically execute and enforce an agreement when certain conditions are satisfied [20]. The code, as well as the agreements it contains, are disseminated throughout a decentralized blockchain network. Transactions are traceable and irreversible, and the programming regulates their execution.

IV. PROPOSED ARCHITECTURE

The Proposed model's layered architecture is depicted in Figure 2, which includes healthcare sensors, local storage, end-users, and local bridges all connected by a peer-to-peer blockchain network. The physical layer has Healthcare sensors for perceiving and receiving information from the human body. The routing layer manages to send packages from origin to destination, whereas the encapsulation layer is in charge of producing packets. Data storage and distribution are made possible through the peer-to-peer network and distributed file system protocol known as the Interplanetary File System (IPFS). IPFS uses content addressing to uniquely identify each file in a global namespace that integrates all computing devices.In the IoT Blockchain network, all the modules integrate common services to enable various functionalities of blockchain technology, such as identity management, consensus, and peer-to-peer (P2P) communication. Distributed Ledger Technology can be used by blockchain to record, confirm, and process transactions, enhancing the network's security, transparency, and efficiency. Web services run on top of existing software systems like application servers and the Content Server as a layer. Web services can provide a link between operating systems or programming languages. The

application layer is the link between the network and the end devices. A specialized program is used to implement this layer.

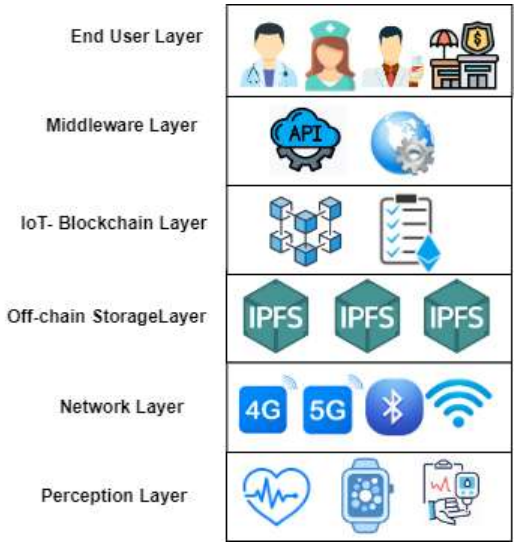

Figure 2: Architecture of IoT- Blockchain Network

V. PRELIMINARIES

Table 1: Symbols Table

Notations	**Description**
DO	Data Owner
DU	Data User
Λ	Security Parameter
E	Elliptical curve of prime order p
G, G_N	Two cyclic multiplicative group
SS_k	System secret key
Pub_{AM}	Public key of AM(Authorization Manager)
E_{Add}	Ethereum Address of User
IF	IPFS storage
Pub_{DO}	Public key of Data Owner
Pr_{DO}	Private key of Data Owner
Pub_{EU}	Public key of End User
Pr_{EU}	Private key of End User
T_K	Access Token
PKI	Public key infrastructure
ENC_{HCR}	Encrypted healthcare records
HCR	Healthcare records
SC	Smart Contract

5.1 BILINEAR MAPPING [18]:

Let G and G_N be two multiplicative cyclic group of prime order p, and Let g be a generator of G. The construction of a bilinear pairing procedure e= G*G→ if pairing relation satisfy the following properties.

1) Bilinearity: For all m, n∈ G, a, b∈ Z_p, $e(m^a, n^b)=e(m, n)^{ab}$
2) Non-degeneracy: $(g, g) \neq 1$.
3) Computability: For all m, n∈ G, computing e(m, n) is efficient.

5.2 CRYPTOGRAPHIC SCHEME:

In this Proposed Scheme, asymmetric encryption using the elliptical curve cryptography is used. Elliptical Curve Cryptography (ECC) is a data encryption technique that uses a mathematical approach based on the algebraic structures of elliptical curves over a finite field, as well as its generator to encrypt and decrypt data. A 160-bit ECC key can give the

same level of security as a 1024-bit RSA key, but it is smaller and more efficient. The elliptical curve is the curve that has an elliptic shape. E is concisely describes by the equation $y^2 \pmod p = x^3 + ax + b \pmod p$, where p is a large prime number. Furthermore, in order to exclude the singular elliptical curve $4a^3 + 27b^2 \neq 0 \pmod p$ must be satisfied. ECC encryption algorithm and advanced encryption standard (AES) scheme provide the hybrid encryption-decryption scheme. As shown in fig.1 the proposed architecture of a Blockchain-based healthcare system consists of five entities. Authorization Manager (AM), End Users (EU), Data Owner (DO) and IPFS Storage, Ethereum Blockchain.

5.3 SYSTEM MODEL

As shown in figure-3,the proposed model includes different entities: Data Owner, End User, Authorization Manager, Public key infrastructure, Healthcare Sensors, and IPFS Storage.

The functions of the entities are as follows.

System Initialization: The authorization manager will initialize the system.

Data Owner: Data Owner owns and manages the healthcare record.

Public key Infrastructure: Public-key Infrastructure is responsible for generating the public key and private key of the end-users and data owner.

End Users: End Users will send the request for accessing the data. When access requests satisfy the access policy defined in the smart contract end-user gets the access token to get the healthcare records.

Local Storage: Local Storage is responsible for storing the data owner's records collected from the healthcare device.

IPFS Storage: IPFS Storage is responsible for storing encrypted healthcare records.

Authorization Manager: The system initialization, Data owner, and user authorization are handled by the Authorization Manager. The authorization Manager is a trusted authority. The authorization manager is responsible for uploading the encrypted healthcare records to the IPFS storage and defining the access policies for the end-users. It also gives EUs fine-grained access rights based on their roles.

Healthcare Sensors: Healthcare sensors monitor the data owner's health and collect the data either periodically or continually.

5.4 ARCHITECTURE OVERVIEW:

5.4.1 *System Initialization* $(1^{\lambda}) \rightarrow (\ Pub_{AM}, SS_k)$: The system setup algorithm is run by the Authorization Manager which takes the security parameter λ as an input and outputs the public key (Pub_{AM})and system secret key SS_k.

The public key is stored in the blockchain through smart contract.

5.4.2 Key Generation $(EC, G) \rightarrow : (Pub_{DO}, Pr_{DO}), (Pub_{EU}, Pr_{EU})$

Here the ECC curve from the python cryptographic libraries and security standards named brailpool256r1 from the registry, and 256-bit field size is defined. Let us assume that we have an elliptical curve over a finite field along with its generator G. In this phase, the algorithm generates the public key/private key pair for the end-user and data owner, where the private key is a random integer number and a public key is a point on the elliptical curve (EC point) and then derive the shared secret key(SSk).

5.4.3 User Registration **(**EAdd) → ($Pub_{EU,}$ Pr_{EU}**)**: In this phase, the user will send his/her Ethereum account public key as an identity to the Authorization Manager. It authenticates the user's identity and stores it in the set of authorized user details. Public key/Private key pair of the user will be generated from the public key Infrastructure. Then, Authorization Manager sends $Pub_{EU,}$ Pr_{EU} to the End Users. The end user's public key is stored in the blockchain via smart contract.

5.4.4 Healthcare Record Encryption **(**SSk, HCR**)→** ENC_{HCR}: The encryption algorithm is run through the public key infrastructure. It takes healthcare records (HCR) and system secret key (SSk) as input and outputs the encrypted health records (ENC_{HCR}). All the encrypted healthcare records are stored in the IPFS storage(IF) and generate the hash of the record and store it in the blockchain network.

5.4.5 Token Generation ($Pub_{DO,}$ Pub_{EU}, HCR)→Tk: When the User sends the request for a particular healthcare record to the authorization manager, the access control smart contract will be executed, and based on the policy defined in the contract, the authorization manager will send the access token to the user.

5.4.6 Healthcare Record Decryption (SSk, ENC_{HCR})→HCR**:** When the User will get the token, He/She uses the token to get the encrypted healthcare record. After applying the secret key, a record will be decrypted.

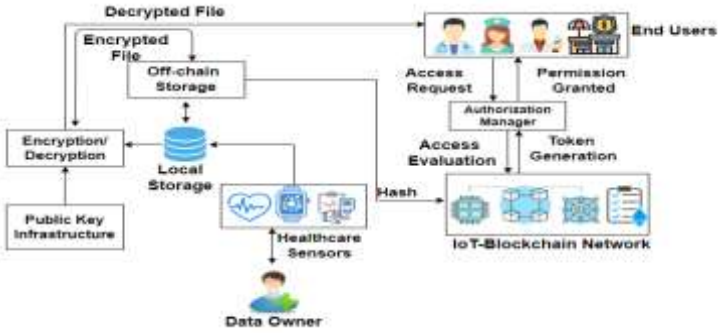

Figure 3: Proposed Decentralized Role Based Access Control System for Healthcare System

Algorithm-1 User Registration SC	
Required Field:	User name, unique ID and blockchain address of entity, method Name, contract Name, Address of contract owner, contract deployer, contract abi.
Input:	User credentials

Output:	Registration Confirmation
	function Userregistration(bool, address, string)
	public{require(keccak256(abi.encodePacked
	(_name)) != keccak256(""))
	if (!(user.User_Id> address(0x0)) then
	UserInfo[_userId] ←User(state, userId, name)
	Else
	Revert();
	emit UserDetailsAdded()
	end function

Algorithm-2 HealthRecord storage SC	
Required Field:	User name, unique ID and blockchain address of entity and Data Owner, method Name, contract Name, Address of contract owner, Health Record, contract deployer, contract abi.
Input:	User credentials, Health Records
Output:	Confirmation of HealthRecord Storage function setHealthRecordsDetails(string,address) public { emit HealthRecordsAdded(); } End function function getHealthRecords(address) public view returns(string, address, string[]) {} End function

Algorithm-3 Role Based Access Control SC	
Required Field:	User name, unique ID and blockchain address of entity, method Name, contract Name,Address of contract owner, contract deployer, contract abi.
Input:	User credentials, Role ID
Output:	Role Assignment Confirmation

```
function addRootRole(string)public
 returns(uint256){
 roles[role].Users[msg.sender] = true;
 emit addroot();}
end function
function addRole(string, uint256)
public returns(uint256)
{ require(_admin <= roles.length, "Admin role  doesn't
exist.");
 uint256 role = roles.push(Role()) ;
emit RoleCreated();
return role;}
End function
function addUser(address , uint256)
public {
roles[_role]s[_account] = true;
emit UserAdded(_account, _role);}
End function
function removeUser(address , uint256)
 public{
delete roles[_role].users[_account];
emit UserRemoved(_account, _role);}
End function
function grantaccesstouser (address, uint) public {
patientToUser[msg.sender][User_id] = access;
emit GrantAccessToUser();}
End function
```

As shown in algorithm 1, this contract allows users to register their address and a name by calling the register function. The registered user information is stored in a mapping, where the user's address is used as the key and the name is the value. The getName function can be used to retrieve the name of a registered user by providing the user's address. The contract also emits a NewUser event each time a new user is registered. In algorithm-2 The setHealthRecordsDetails function takes in a user's credentials and health records, and emits a HealthRecordsAdded event upon successful storage of the records. The getHealthRecords function allows for the retrieval of the stored health records, and returns the user name, the address of the data owner, and an array of strings representing the health records. As shown in algorithm-3 contract has several functions that allow an entity with the correct permissions to manage the roles and permissions of users on the blockchain.

VI. EXPERIMENTATION SETUP

Ethereum is a decentralized blockchain technology that creates a peer-to-peer network for securely executing and authenticating smart contracts. Ethereum accounts are used for sending and receiving transactions. As a cost of processing transactions on the network, a sender must sign and spend Ether, Ethereum's native coin. Solidity is an object-oriented programming language for enforcing smart contracts on different blockchain platforms, similar to Ethereum. Remix-IDE is used for smart contract creation and deployment. Ganache is an ethereum simulator used for setting up a personal ethereum Blockchain for testing your solidity contracts. Web3.js is the official Ethereum JavaScript API used it to interact with the Ethereum smart contracts using Ganache Client on the machine. Python is a high-level, general-purpose programming language. Python version 3.9 is used for the implementation of Public-key cryptography. A host system is a machine with Intel(R) Core (TM) i3-5005U CPU @ 2.00GHz, 4 GB RAM, running Windows 10.Table 2 shows the development environment for the proposed healthcare system using Blockchain Platform. Figure 4 shows the role has been created and assigned to the legitimate doctor. Figure 5 illustrates how authorized users can access health records.

Table 2: Development Component

Components	Description
CPU	Intel(R) Core (TM) i3-5005U CPU
Memory	4 GB

Operating System	Windows10
Ganache Truffle	v5.0.5 (core: 5.0.5)
On-chain	System Storage
Off-chain Database	IPFS
Solidity	v0.5.0 (solc-js)
Python	v 3.8
Node	v13.8.0

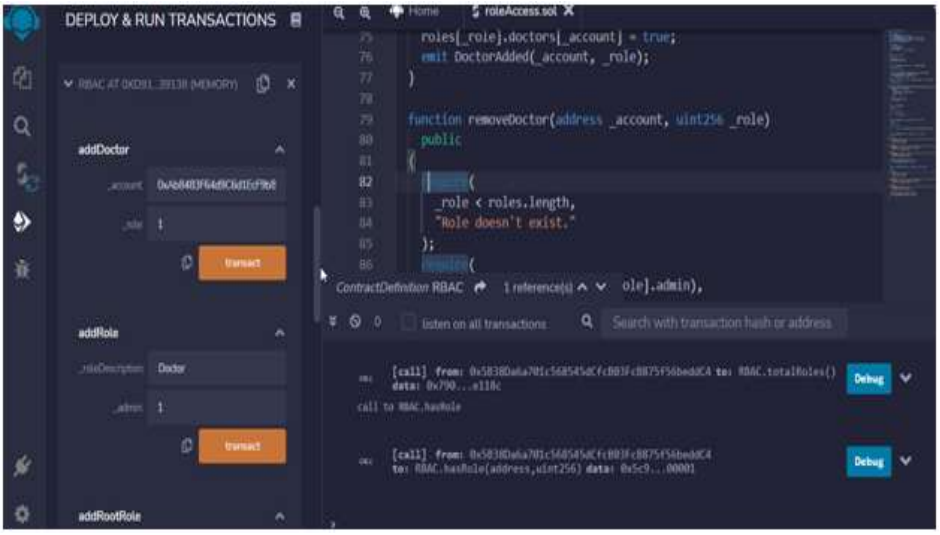

Figure 4: Role Assignment

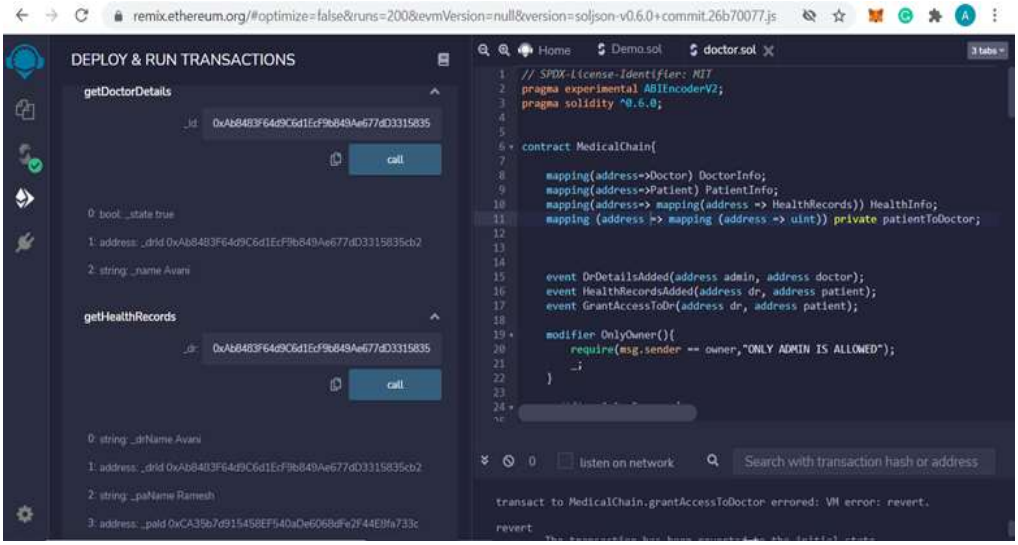

Figure 5: Health record access

VII.PERFORMANCE ANALYSIS

The transaction costs paid to miners on a blockchain network in order to include a user's transaction in the block are known as gas fees. Gas units consumed by smart contracts are used to compute the system cost consumption. The miners set the gas price at the beginning of the transaction, and it is measured in Gwei. Gas units are transformed into ether value, in the Ethereum blockchain. The performance of the proposed system is measured. Table 3 shows the execution costs of various the smart contract, with the highest cost healthrecord smart contracts worth 0:004 ETH. All of the remaining contracts have relatively low fees. Additionally, we tried to reduce the costs of the functions during the testing phase using RemixID by optimising the code. Table 4 shows the gas cost and transaction cost of various functions of smart contract.

Table 3: Proposed smart contract's gas usage for deployment.

(1 Gas = 20 gwei, 1 Eth=109 gwei).

Contract Name	Gas Used	Ether	Transaction Cost	Ether
UserRegistration SC	741461	0.00148	644748	0.0012894
PatientRegistration SC	834243	0.00166	725428	0.001450
HealthRecord SC	2273740	0.00454	1977165	0.003954
RoleBased SC	1021909	0.00204	888616	0.001777

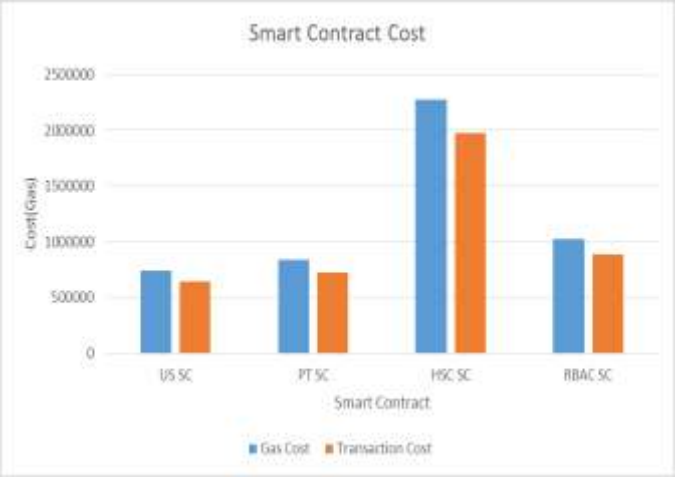

Figure 6: Smart Contract Cost

Table 4: Proposed smart contract's function execution cost
(1 Gas = 20 gwei, 1 Eth = 109 gwei).

Function	Gas Used	Ether	Transaction Cost	Ether
Userregistration()	88426	0.001768	76892	0.001537
Getuserdetail()	29551	0.000591	29551	0.000591
SetPatientdetail()	112082	0.002241	97462	0.001942
GetPatientdetail()	30715	0.000614	30715	0.000614
AddRootRole()	112058	0.002241	97441	0.001948
AddRole()	84428	0.001688	73415	0.001468
AddUser()	61392	0.001227	53384	0.001067
RemoveUser()	41670	0.000833	31434	0.000628
GrantAccesstoUser()	74532	0.001490	62345	0.001246
SetHealthRecord()	207388	0.004147	180337	0.003606
GetHealthRecord()	36131	0.000722	36131	0.000722

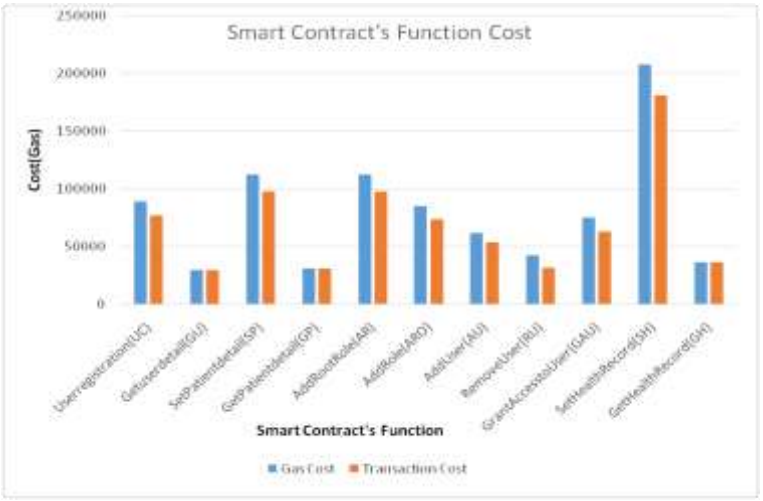

Figure 7: Smart Contract's Function Cost

VIII.SECURITY ANALYSIS

Mythril is an Ethereum smart contract security analysis tool debuted at the 2018 HITBSecConf. Mythril diagnoses a variety of security vulnerabilities in smart contract. As shown in figure 8, all the smart contract are tested against security vulnerabilities with mythrill and shows no vulnerabilities founds for all the smart contract.

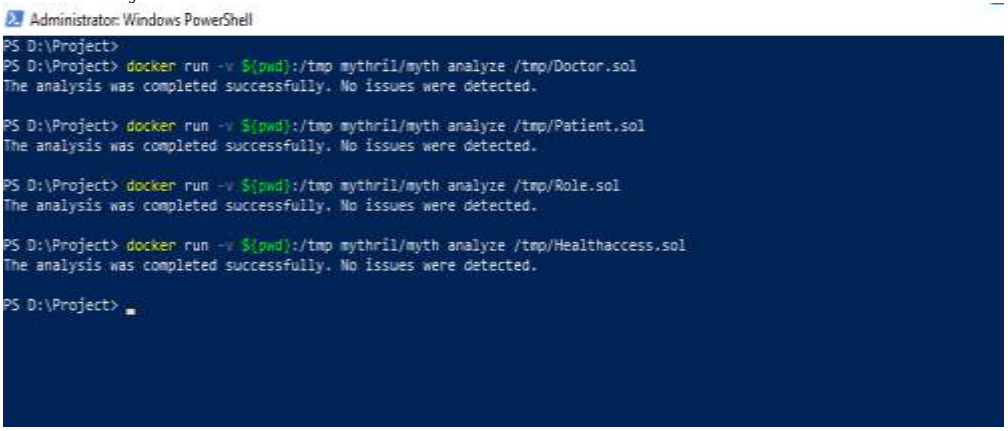

Figure 8: Smart Contract Security Analysis

IX. CONCLUSION

In this paper, a decentralized role based access control for healthcare data was proposed with blockchain technology. The framework is developed in a decentralized way to provide security and privacy of healthcare records. Access control policies are developed using smart contracts for user authorization. Performance analysis is measured with security against vulnerabilities.

REFERENCES

1. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.
2. S. M. Hasani and N. Modiri, "Criteria Specifications for the Comparison and Evaluation of Access Control Models," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 5, pp. 19–29, 2013, doi: 10.5815/ijcnis.2013.05.03.
3. I. Riabi, H. K. Ben Ayed, and L. A. Saidane, "A survey on blockchain based access control for internet of things," *2019 15th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2019*, pp. 502–507, 2019, doi: 10.1109/IWCMC.2019.8766453.
4. S. Rouhani, R. Belchior, R. S. Cruz, and R. Deters, "Distributed attribute-based access control system using permissioned blockchain," *World Wide Web*, vol. 24, no. 5, pp. 1617–1644, 2021, doi: 10.1007/s11280-021-00874-7.
5. A. Solanas, F. Casino, E. Batista, and R. Rallo, "Trends and challenges in smart healthcare research: A journey from data to wisdom," *RTSI 2017 - IEEE 3rd Int. Forum Res. Technol. Soc. Ind. Conf. Proc.*, 2017, doi: 10.1109/RTSI.2017.8065986.
6. O. P. Badve, B. B. Gupta, S. Yamaguchi, and Z. Gou, "DDoS detection and filtering technique in cloud environment using GARCH model," in *2015 IEEE 4th Global Conference on Consumer Electronics, GCCE 2015*, 2016, pp. 584–586, doi: 10.1109/GCCE.2015.7398603.
7. M. A. Alsmirat, Y. Jararweh, I. Obaidat, and B. B. Gupta, "Internet of surveillance: a cloud supported large-scale wireless surveillance system," *J. Supercomput.*, vol. 73, no. 3, pp. 973–992, 2017, doi:10.1007/s11227-016-1857x.
8. F. Liu, P. Shu, H. Jin, L. Ding, J. Yu, D. Niu, B. Li, Gearing resource pool mobile devices with powerful clouds: architectures, challenges, and

applications. IEEE Wireless communications 20 (3) (2013) 14–22
9. R. Akkaoui, X. Hei, and W. Cheng, “EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange,” *IEEE Access*, vol. 8, pp. 113467–113486, 2020, doi: 10.1109/ACCESS.2020.3003575.
10. G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, “Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology,” *Sustain. Cities Soc.*, vol. 39, pp. 283–297, 2018, doi: 10.1016/j.scs.2018.02.014.
11. R. Ammar and S. Salam, “Internet of Things From Hype to Reality, Internet of Things Security and Privacy,” pp. 195–223, 2017.doi: 10.1007/978-3-319-44860-2_8
12. S. Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, “Policy-Based Access Control for Constrained Healthcare Resources,” *19th IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM 2018*, 2018, doi: 10.1109/WoWMoM.2018.8449813.
13. N. Shi *et al.*, “BacS: A blockchain-based access control scheme in distributed internet of things,” *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2585–2599, 2021, doi: 10.1007/s12083-020-00930-5.
14. S. Pal, T. Rabehaja, A. Hill, M. Hitchens, and V. Varadharajan, “On the Integration of Blockchain to the Internet of Things for Enabling Access Right Delegation,” *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2630–2639, 2020, doi: 10.1109/JIOT.2019.2952141.
15. J. P. Dias, H. Sereno Ferreira, and Â. Martins, “A Blockchain-Based Scheme for Access Control in e-Health Scenarios,” in *Advances in Intelligent Systems and Computing*, 2020, vol. 942, pp. 238–247, doi: 10.1007/978-3-030-17065-3_24.
16. G. Tripathi, M. A. Ahad, and S. Paiva, “S2HS- A blockchain based approach for smart healthcare system,” *Healthcare*, vol. 8, no. 1, 2020, doi: 10.1016/j.hjdsi.2019.100391.
17. R. Kumar and R. Tripathi, “Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model,” *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 2, pp. 2321–2338, 2021, doi: 10.1007/s12652-020-02346-8.
18. S. Nakamoto and A. P. E. C. System, “Bitcoin: A Peer-to-Peer Electronic Cash System” 2008, [Online]. Available: https://bitcoin.org/bitcoin.pdf
19. T. M. Fernández-Caramés and P. Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things,” *IEEE Access*, vol. 6, pp. 32979–33001, 2018, doi: 10.1109/ACCESS.2018.2842685.
20. S.D.Levi, A.B.Lipton,“An Introduction to Smart Contracts and their Potential and Inherent Limitations”. Harvard Law School Forum on Corporate GovernanceAnd Financial Regulation, pp. 1–10,2018.
21. A. Hayes, “The Socio-Technological Lives of Bitcoin,” *Theory, Cult. Soc.*, vol. 36, no. 4, pp. 49–72, 2019, doi: 10.1177/0263276419826218.