International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

e-DRBAC-HC: Extended Decentralized Role-Based Access Control for Healthcare System using Blockchain

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

Submitted: 29/01/2024 **Revised**: 07/03/2024 **Accepted**: 15/03/2024

Abstract*:* Recent advancements in the Internet of Things have made a significant impact on health informatics. Healthcare services are increasingly incorporating information and communications technology (ICT) as a response to the rising volume of patient data. This surge in data has prompted a shift from traditional methods of storing patient records in physical files to digital alternatives, with Electronic Health Records (EHRs) leading the way. However, Patient tamper-proof data, storage and retrieval of health records, and avoidance of the centralized record-keeping mechanism are crucial requirements in any healthcare system. Blockchain, being a distributed ledger technology, offers a secure and transparent way to store every record within the healthcare system. The proposed e-DRBAC-HC framework leverages the principles of Role-Based Access Control (RBAC) and Blockchain's distributed ledger to establish secure, transparent, and interoperable EHR management. By implementing this framework, the healthcare sector can strengthen its access control mechanisms, ensuring timely and secure access to EHR while maintaining Security and confidentiality. The performance of this proposed framework is measured in terms of the efficiency and throughput of the system. It is observed that the proposed framework performs better concerning EHR encryption-decryption, token generation, verification, response, and RBAC policy execution.

Keywords: *Internet of Things, Role-Based Access Control, Healthcare System, Blockchain Technology, Security*

1. Introduction

Internet of Things (IoT) is a disruptive technology that is revolutionizing the global economy and society by permeating all areas of life. The global healthcare IoT market size is estimated to grow 110.6 billion USD in 2025, representing a compound yearly growth rate of 7.4% between 2020 and 2025 [1]. IoT is particularly important in healthcare, where it is being used to improve patient's care through wearable and mobile devices. Wearable devices and other patient monitoring devices produce large amount of data about patients and can be used as a source for various healthcare services [2]. This data could integrate with Electronic health records (EHRs) to provide accurate diagnosis and treatment for students. EHRs, which traditionally store patient's medical histories, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results, can be immensely enriched with the real-time, continuous data from IoT devices. The Internet of Things (IoT) presents numerous advantages, yet it is not without its drawbacks. One of the fundamental challenges is ensuring secure and granular access to health data [3].

The current centralized systems used for privacy, security, and data handling rely on third-party organizations that users must trust to manage their data securely. The current healthcare system faces various issues in handling patient data. Healthcare data contains sensitive patient information that should be accessible only to the authorized individuals. So it also raises concerns about the security and privacy of patient's health records. Unauthorized access to this information can lead to serious

Consequences include financial fraud, identity theft, and breach of privacy [4]. Therefore, a secure access control system is required to maintain the privacy and confidentiality of patient's records. Blockchain technology was developed to address some limitations and challenges of traditional centralized systems, particularly in trust, transparency, immutability and security. Blockchain is a distributed ledger technology that provides peer-to-peer networks for every transaction. Blockchain enables users to send digital transactions to all the nodes within the network through a secure and verifiable method. Users send requests as transactions within the network, and requests are verified and recorded by all the nodes making it very difficult for any single entity to manipulate the data and increase trust and efficiency in a variety of applications. Blockchain provides a decentralized infrastructure that ensures data interoperability, security, authentication, integrity, and is immune to single-point failures and communication bottlenecks unlike centralized systems. Blockchain technology provides a high level of security through cryptography and distributed consensus.

1.1. Motivation

The Internet of Things (IoT) has the potential to transform

[1] *LDRP-ITR, KSV, Sarva Vidyalaya Kelavani Mandal, Gujarat, Gandhinagar- 382015, India*
[2] *VS-ITR, KSV,Sarva Vidyalaya Kelavani Mandal, Kadi, 382715, India*
** Corresponding Author Email: avani26.22@gmail.com*

healthcare systems for the users by providing digitization. Access control is a critical requirement for timely & secure access to patient information in order to receive better treatment and other services from the IoT-based healthcare system. It defines the rules and policies to access the patient's personal and medical records. However, the healthcare sector faces several issues when it comes to access control. Healthcare organizations have a wide range of users, including doctors, nurses, administrators, Pharmacy, Laboratory and patients. Each of these groups may require different levels of access to different types of data. Healthcare system uses various devices and technologies that may not be compatible with each other. Ensuring seamless interoperability among this system for achieving robust access control can be a challenge. As healthcare organizations expand and adapt, so does the demand for enhanced data access. It is difficult to provide an effective access control system with smooth interoperability among various systems. In centralized storage architecture, all the data is stored in a single server or location where a single entity controls and administers the entire system, including the hardware, software, and data. As the system grows, it can become more difficult to maintain and manage large amount of data. Hence, it becomes more vulnerable to security risks because they have a single point of entry that can be targeted by attackers. If that point is compromised, the entire system can be at risk. Blockchain technology was developed to address some limitations and challenges of traditional centralized systems, particularly in trust, transparency, immutability and security. Blockchain is a distributed ledger technology that provides peer-to-peer networks for every transaction. Blockchain enables users to send digital transactions to all the nodes within the network through a secure and verifiable method. Blockchain provides a decentralized infrastructure that ensures data interoperability, security, authentication, integrity, and is immune to single-point failures and communication bottlenecks unlike centralized systems. In summary, the implementation of strong security measures, including robust data encryption and fine grained access control, plays a pivotal role in fortifying the IoT-Based Healthcare system against potential vulnerabilities and risks. To address aforementioned challenges, Decentralized Role-Based Access Control (DRBAC-HC) framework with Blockchain Technology is proposed.

The main contribution and novelty of this research is as follows:

Decentralized Role-Based Access Control (DRBAC-HC) Framework: Ethereum based smart contract implementation for a decentralized and tamper-resistant access control framework

Elliptical Curve Cryptography (ECC) for EHR Encryption and Decryption: ECC based public and private key pairs enhance security, allowing only authorized parties with the corresponding private keys to decrypt and access the sensitive health information.

Electronic Health Record Storage and Retrieval from Distributed IPFS: IPFS (InterPlanetary File System) is used to store health records in a decentralized and distributed manner. This guarantees data availability and resilience in the face of single points of failure.

Role-Based Access Control Framework with Customized Token Generation: The DRBAC-HC framework defines roles and their associated permissions within the smart contract. Customized RBAC policies determine access levels for different users based on their roles. These tokens serve as access credentials and are required for interacting with the EHR smart contract and IPFS storage.

The rest of the paper is structured as follows: Section 2 discuss the existing work done by different authors. section 3 explain the proposed architecture and different algorithm for access control. Experimentation results of proposed system presents in section4. In section 5 we conclude the paper.

2. Literature Survey

Researchers have been exploring various methods of access control mechanisms for addressing security and privacy concerns involved in integrating IoT devices to the healthcare systems. Traditional access control methods like mandatory access control, access control list, and discretionary access control, have been widely used in the healthcare system. However, these methods face various challenges due to limitations of scalability and interoperability among IoT devices. Therefore, the integration of Blockchain with access control mechanisms in the healthcare system has been proposed. Blockchain with access control offers decentralization, immutability, and transparency, which enhance security and privacy in IoT-based healthcare environments. Some of the researchers have proposed a smart contract-based solution to enforce access rights and permissions in IoT based healthcare systems. These solutions give the decentralization and temper-proof data access mechanism but also raise the security, privacy, scalability and computational overhead concern. In this section, we present the literature survey of Blockchain-based access control systems for the Healthcare system. In [5] The author proposes attribute-based access control for Globalized Healthcare Provisioning Ecosystem (GHPE) using Next Generation access control (NGAC) and Blockchain. Different smart contracts are developed to store attributes, and access policies in a decentralized way, where the Policy Enforcement Point (PEP) intercepts the request sent by the subject, which then sends to the Policy

Decision point (PDP). After evaluating the request by PDP, Policy Administration Point (PAP) with the attribute from Policy Information point (PIP) takes the decision. That decision is sent to PEP .The authors propose a Blockchain-based electronic health record (EHR) sharing system using the Key search and Proxy re-encryption technique to achieve the privacy and security of the health system. The author implemented the ECDH algorithm with a conjunctive keyword search for evaluating the performance of the proposed system in terms of integrity, privacy, and search operation [6]. Author of [7] proposed and implemented an Electronic Health record (EHR) sharing scheme to achieve the security and privacy of patients' data where EHR are stored on the IPFS storage and their address is encrypted with public key cryptography. In [8], the authors developed a cipher text attribute-based encryption algorithm in the Cloud storage to achieve access control and revocation rights. The data owner encrypts the data and shares it with the attribute authority for re-encryption so that revoked users do not get access to the records. The proposed architecture claims to achieve data protection, collusion tolerance, and Backward and forward security features. In [9] the authors implement the biometric-based EHR management prototype using Blockchain that overcomes the public key infrastructure requirement. BBEHR architecture is divided into different layers such as the user interface layer, Middleware layer, Blockchain layer, and Cloud storage layer to ensure access control, privacy, and confidentiality. In [10], the authors implemented signature and encryption methods using attributes for Cloud storage data. The authors developed an access control tree structure for access right policy development that achieves access control, and confidentiality. Authors of [11], proposed a health record storage and retrieval model with modification in Merkle tree data storage. Cryptographic hash functions provide security and integrity of data. The system measured the performance in terms of latency, throughput, resource utilization, and number of transactions. Author in [12] developed a disease management system to enhance the security, scalability, and privacy of patient information. In [13] the authors proposed a Blockchain-based access control system. Attribute-based access control policies are developed using chain codes. The model is also tested with the Hyperledger Caliper tool and shows the performance of the comparison proposed system with Fabric-IoT for latency and throughput evaluation. In [14], the authors proposed a multi-authority attribute-based encryption scheme to encrypt and decrypt personal data for data sharing and access control. The authors developed a dynamic access control scheme for Cloud-based e-health care services. The authors developed a Cloud-based web application and hosted and tested it on Amazon Web Services (AWS).The authors propose the architecture called BlockMedCare to integrate IoT, Blockchain, and IPFS for remote patient monitoring with a re-encryption proxy for the security of the data. Different nodes are responsible for data collection, data sharing, and data storage. The proposed system provides data integrity and privacy and access control to the users [15]. In [16], the authors proposed an Oath based Authorization framework for IoT access control using Blockchain Technology for addressing the issues with centralized server storage. This is accomplish with the help of authorization delegation using decentralized identity (DID) and secure token generation called POP token. In [17], the authors proposed a lightweight authentication framework to overcome the data storage and overhead issues. It provides storage optimization for trust aware security and privacy services. In [18], the authors proposed an access control framework using attribute based search encryption for storage and retrieval of Personal health records from IPFS using smart contract for achieving security. In [19], the authors proposed an architecture that provides device authentication and ring structure-based access control for achieving security and privacy.

3. Preliminaries

Table 1. Notations and their Description

Notations	Description
P_{ID}	Patient ID
D_{ID}	Doctor ID
PR_{User}	Private Key of Users
PU_{User}	Public Key of Users
Ts	Time Stamp
TRS	Transaction Status
T	Token
EHRs	Electronic Health Records
OP	Operative Prescription
MP	Medication Prescription
LP	Laboratory Prescription
LR	Laboratory Reports
LR_h	Laboratory Report Hash
MI	Medication Invoice
Ns	Nurse
Ph	Pharmacy
Lb	Laboratory

3.1. Bilinear Mapping[20]:

Bilinear groups G:=(p, G1, G2, GT, g1, g2, e) are made up of a prime p, cyclic groups G1, G2, GT of order p, generators g1 and g2 of G1 and G2, and a bilinear map e : G1 × G2 → GT that satisfy two properties.

- (Bilinearity): $\forall h_1 \in G_1$, $h_2 \in G_2$, a, b ∈ Zp, $e(h1^a , h2^b) = e(h^1, h^2)^{ab}$.
- (Non-degeneracy): For g_1 and g_2, $g_T := e(g_1, g_2)$ is a generator of G_T .

3.2. Notations

3.2.1 Users: U $\supseteq \bigcup_{i=0}^{\infty} Ui$, U is a set of all users in the system that send the access request for a health document. Usr = {Hospital Desk, Patient, Doctor, Nurses, Laboratory, Pharmacy}

3.2.2 Roles: R $\supseteq \bigcup_{j=0}^{\infty} Ri$, R is a Set of all roles defined in the

Ri,system. Roles (R) ={HospitalDesk, HospitalAdmin, PatientOPD, PatientAdmitted, DoctorSurgen, DoctorPhysician, DoctorSurgen, Patient,Nurses, Laboratory, Pharmacy}

3.2.3 Permissions: P $\supseteq \bigcup_{j=0}^{\infty} Pn$, P is a set of all Permissions available in the system. Permission p_n is nth number of permissions of (DOC, PRM), where DOC is a document and PRM is permission. Permissions (PRM) = {Read, Write}

3.2.4 Rights: RGT is a set of all possible rights which can be issued over a document to a user.

Rights (RGT) = {Grant, Revoke, Deny}

3.2.5 Electronic Health Record (EHRs): Documents is a set of all health records in the system that is requested by all users. Electronic Health Records (EHRs) = {Registration Slip, Medication Prescription, Laboratory Prescription, Operative Prescription, Laboratory Reports, Medication Invoice, Discharge Summary, Insurance Related, Hospital Invoice}

3.2.6. Token: Set of all capability tokens generated in the system. Token (T): <Token ID, Document ID, User ID, Role ID, Can Delegate?, Permission, Rights, Time-from, Time-to>

Transaction Status (TRS)= Success, Fail, NoUpdate

3.3 e-DRBAC-HC Model and design goals

The overview of the proposed architecture was presented in the earlier paper [20]. This work shows the implementation of the proposed work with Decentralized Role-Based access control. The proposed architecture presents a novel Role-based access control framework designed specifically for healthcare systems using Blockchain Technology. This architecture leverages the decentralized and immutable nature of Blockchain technology to establish a secure and transparent access control mechanism, ensuring authorized entities to access EHRs. Fig.1 shows the proposed e-DRBAC-HC Framework. The architecture comprises several key components and their interactions, as outlined below

3.3.1 Users: Users are the different stakeholders such as doctor, nurse, Patients, laboratory, pharmacy and hospital desk, who will send the access request for EHRs.

3.3.2 Key Generation Center: Key generation center is a trusted third party that is responsible for generating system public parameter and public key-private key pair.

3.3.3 User Interface: A user-friendly interface is provided to healthcare providers and administrators, enabling them to interact with the RBAC smart contracts. Through this interface, they can manage access control configurations, such as creating and assigning roles, defining permissions, and granting/revoking access privileges. The user interface abstracts the complexity of interacting with smart contracts, making it easier for authorized users to manage access control.

3.3.4 Role-Based Access Control Model: The framework adopts a RBAC model to manage access control. The model defines roles, permissions, and user assignments. Roles represent different job functions or responsibilities within the healthcare system, and permissions define the actions that can be performed by users with specific roles. User assignments link individual users to specific roles, allowing them to exercise the associated permissions. The Framework supports a hierarchical role structure, enabling flexible management of access control policies in complex healthcare systems

3.3.5. Access Control Enforcement: The RBAC smart contracts enforce access control policies by validating user requests against predefined permissions. When a user attempts to access patient records, the smart contracts verify their assigned role and permissions. If the user is authorized, the access request is granted, and the relevant data is provided. Otherwise, the request is denied, preventing unauthorized access. The access control enforcement mechanism also includes auditing and logging capabilities to maintain an immutable record of access activities for transparency and accountability purposes.

3.3.6. Smart Contract Layer: The core of the framework is the RBAC smart contracts deployed on a blockchain network. These smart contracts enforce access control policies and manage user roles and permissions. They provide a tamper-resistant and immutable framework for access control, ensuring that access decisions are transparent and cannot be altered or manipulated.

3.3.7. Smart Contract Implementation: The RBAC smart contract in the framework is designed to manage roles, permissions, and user assignments efficiently. They include data structures, functions, and events that facilitate role creation, permission assignment, and user management. The smart contracts also handle access control enforcement, ensuring that only authorized users can perform specific actions on patient records.

3.3.8. Blockchain Network: The framework leverages a blockchain network to store and validate access control policies and audit logs. The blockchain ensures the integrity and immutability of the access control data, making it tamper-resistant. By using a distributed ledger, the architecture eliminates the need for a central authority, enhancing the security and resilience of the system.

3.4 Design Details of e-DRBAC-HC Scheme

System Initialization (1^{λ})→(PP): System Initialization is done by Administrator. Administrator takes security parameter 1^{λ} as input and generates the public parameter to execute all the transaction within system

User Registration: User registration is performed by the Hospital

Desk.Users such as Doctor, patient, Nurse, Pharmacy and Laboratory submit their identity documents, and Hospital Desk will verify their identity and registered all the users within the system. Each user's public key (PU_{User}), private key (PR_{User}) pair are generated.

Role Based Access Control Structure:

Role Assignment: After the key generation for each entity, a user role is assigned within the system. User-role assignment function is defined as f: $U \rightarrow 2^{R}$ Where 2^{R} is the power set of R. This means each user can be assigned multiple roles.

User-to-Role assignment relation: $UA \subseteq U \times R$

Permission Assignment: Permissions define what actions a role can perform on a specific set of data. After role assignment, a

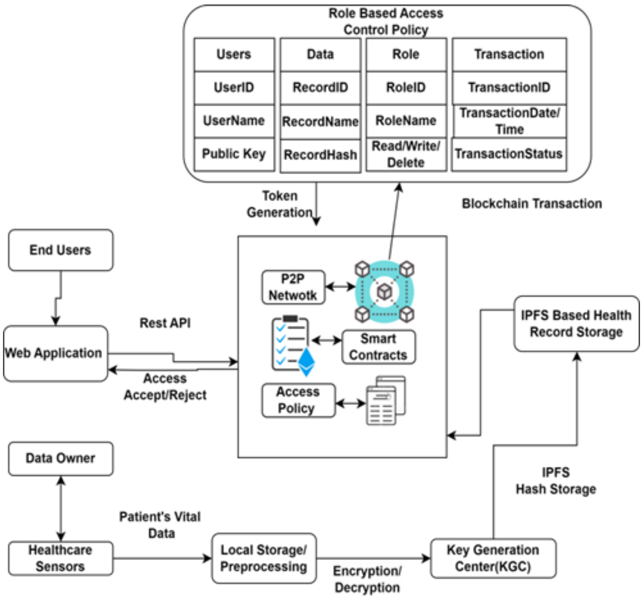


Fig.1. e-DRBAC-HC Framework

role-permission assignment function is defined as g:$R \rightarrow 2^{P}$. This means each role can have multiple permissions.

Role-to-permission assignment relation: $PA \subseteq R \times P$

Access Control Structure: Let a: $U \times P \rightarrow \{true, false\}$ be an access control function. Where U is the set of all users and P is the set of all permissions in the system. a (u, p) returns true if user u has permission p, and false otherwise. This can be defined in terms of the previous functions as: $a(u, p) = true \Leftrightarrow \exists\ r \in f(u)$ such that $p \in g(r)$.This means that a user has a permission if and only if there exists some role assigned to that user which has that permission.

Token Generation and Delegation: When a user send a request for EHR access, token is generated. A token generation function for a user with specific role and permission is defined as GenerateToken T:$U \times R \times P \times exp \times del \rightarrow T$ which generates a unique token for a user to execute a permission under a role that map users, roles, permission, expiration time, delegation depth from the access control list.

Token Delegation: When user wants to give access rights to other user, rights will be given to other user and new token will be generated and that token will be delegated to other user.

Token Verification:

A token verification function is v: $T \times P \rightarrow \{true, false\}$. This verifies if a token grants permission to a specific action. It ensures the token is valid, not expired, and corresponds to the claimed permission.

DelegateToken DT: $T \times U \rightarrow T$: Delegates a token from one user to another, decrementing the delegation depth by Token can only be delegated if del > 0 and tokens can only be used if the current time is less than exp.

Token-to-Permission Relation:

$TP \subseteq T \times P$ For token t and permission p, $(t, p) \in TP$ indicates that token t grants permission p.

EHR Encryption (EHR, PU_{User})→ (EHR_{enc}, nonce, authtag , Secretkey) : The AES GCM encryption algorithm takes EHR and public key PR_{User} as input parameter and outputs encrypted Electronic Health Record EHR_{enc}, Nonce N and authentication tag authtag and secret key.

EHR Decryption {EHR_{enc}, nonce, authTag, Secretkey}, PR_{User})→(EHR): In the decryption process, the encrypted EHR, along with other cryptographic parameters, is decrypted to reveal the original Electronic Health Record(EHR).

As Shown in the algorithm 1 patient request for the registration and after checking all credentials of the patient, admin register the patient in the system and system generate patient ID (P_{ID}). Patient request for the Appointment with particular Doctor for a given time, if doctor is available then Appointment ID is generated with $< P_{ID}, D_{ID}, T>$ and A_{ID} is sent to the patient and A_{ID} details are stored in the Blockchain. If doctor is not available, appointment is rescheduled. After that Doctor visits the patient PID and generates the Operative prescription, Laboratory Prescription and Medication Prescription. Patient submits their Laboratory report to the Doctor. Laboratory report will also store on the IPFS storage and their hash values will be stored on blockchain. Doctor will get the token to access the reports. After using token as input to the system, doctor will download the encrypted EHRs. Encrypted EHRs can decrypt with their own private key and now doctor verifies the patient's report.

Algorithm1: Patient Registration and Appointment

```
Patient Request for Registration
Hospital Registers Patient (PID)
Patient (PID) requests for appointment with Doctor (DID) for time T
if Doctor (DID) == AVAILABLE then
   Appointment AID : <DID,PID,T> of Doctor (DID) is given to Patient (PID) for time T
   Appointment AID : <DID,PID,T> is conveyed to Patient and Blockchain
   Appointment AID : <DID,PID,T> = TRUE
else
   Appointment is rescheduled OR cancelled.
   Appointment AID : <DID,PID,T> = FALSE
end if

if Appointment AID : <DID,PID,T> == TRUE AND Time ∈ T then
   Doctor DID visits Patient PID
   Doctor DID issues Prescriptions Operative (OP), Medication (MP), Laboratory (LP) to  Patient PID and Blockchain
   Patient PID submits Operative Prescription (OP) to Nurse (N)
   Patient PID submits Medication Prescription (MP) to Pharmacy (P)
   Patient PID submits Laboratory Prescription (LP) to Laboratory (L)
   Pharmacy (P) provided Medication Invoice (MI) to Patient PID
   Laboratory (L) provides Laboratory Report (LR) to Patient PID
   Patient PID Laboratory Report (LR) to Doctor DID and Blockchain
end if
```

As shown in the algorithm-2, Access Control List is generated which takes Users u, Roles r, Permissions p, Rights rt, Electronic Health Record hr, Token t as an input and outputs status s with updated permission list PL. If role r exists is in the list of roles (Roles), the status is set to "NoUpdate". If the role does not exist and User is admin, the role r is added to the list of roles (role).Initialize the counter to 0. System will check the mapping between the user (U) and role (rl). If true, iterate through all EHRs (ehr) owned by the user. Create a tuple (t) containing user (u), role (rl), Electronic Health records (ehr), permission (p), and rights (rt). Add the tuple (t) to the Permission List (PL).Increment the counter (count). If false, do nothing. If count is greater than 0, Electronic Health Records are added to Permission List otherwise no Electronic Health Records will add to Permission List.

Algorithm-2 Create an Access Control List

```
Input: Users u, Roles rl, Permissions p, Rights rt, Electronic Health Record hr, Token t
Output: Status s
Updated: Permission List PL
if r is in Roles then
   Status ← NoUpdate
else
   if u is Admin then
         Add r in Roles
   else
         prompt ← "Permission Denied to Add a Role"
         s ← Fail
   end if
end if

count ← 0
for all u in Users do
   for all rl in Roles do
         if mapping(u,rl) == TRUE then
               for all hr in Electronic Health Redords do
                     if u is owner of hr then
                           create a tuple t <u, rl, ehr, p, rt>
                           add the tuple t into the Permission List PL
                           increment count
                     end if
               end for
         else
         end if
   end for
end for
if count > 0 then
   prompt ← count + "Electronic Health records added to Permission List"
   status ← Success
else
   prompt ← "No Electronic Health records added to Permission List"
   status ← Fail
end if
return status
```

As shown in the algorithm-3, Access Control List is generated which takes Users u, Roles r, EHRowner (eo), EHRrequester (er), Permissions p, Rights rt, Electronic Health Record hr, TimeStamp (ts), Rights (rt),Token t as an input and outputs status s with updated permission list PL.System will Verify if both the EHR Owner (eo) and EHRrequester (er) exist in the defined Roles (rl). If not, return an error indicating that the role of either the owner or requester does not exist. If rights are defined in the permission list then Role-based Access Permission granted with no indent.

Algorithm-3 Role Based HealthRecord Access Control

```
Input: Users u, Roles rl, EHROwner eo, EHRrequester er, PermissionList PL, Permission p, TimeStamp ts, EHR ehr, Rights rt
Output: Status s
if do is not in Roles OR dr is not in Roles then
   prompt ← "The Role of either owner or requester does not exist"
   s ← Fail
   return s
end if
if p is not in Permission then
   prompt ← "Requested Permission does not exist"
   s ← Fail
   return s
end if
if ehr is not in Electronic Health Records then
   prompt ← "Requested Document does not exist"
   s ← Fail
   return s
end if
if do is NOT owner OR do does not have delegation rights then
   prompt ← "Electronic Health Record Owner does not have rights to delegate to others"
   s Fail
else
   if rt is Grant AND ts is within permitted time stamp then
          prompt ←"Role-based Access Control Permitted"
          s ←Success
   else
   prompt ← "Enter the right is NOT Grant OR Time stamp has expired"
end if
return s
```

4. Experimentation and Result

The proposed framework provides decentralized secure access of EHRs using Blockchain and IPFS storage. Raspberry Pi 4 8GB RAM and Healthcare sensor is connected with Blockchain and patient's data are collected. Public key cryptography for different key generation and Electronic Health records encryption/decryption are done with python. We have generated ECC brainpoolP256r1 curve and point X and Y on the axis on ECC curve over the field defined by $y^2 = x^3 + x$. Each users public key-private key pair is generated and EHR is encrypted and decrypted using shared secret key with Python's Cryptography library. The experiments were conducted on the host system Windows 10 with Intel(R) Core (TM) i3-5005U CPU @ 2.00GHz, 4 GB RAM.The proposed framework is tested with Ganache Blockchain platform. All the smart contracts are deployed in the solidity programming language with the Remix platform. It uses Truffle Suit for the local Blockchain environment.Web3.js provides a collection of libraries that interact with a local or remote Ethereum node using HTTP or web socket to connect with the front-system. Metalmark wallet is used to interact with the Blockchain. Figure 2 shows the overall implementation flow of the proposed framework. Figure 3 shows the user's role assignment and their access permissions for EHRs.

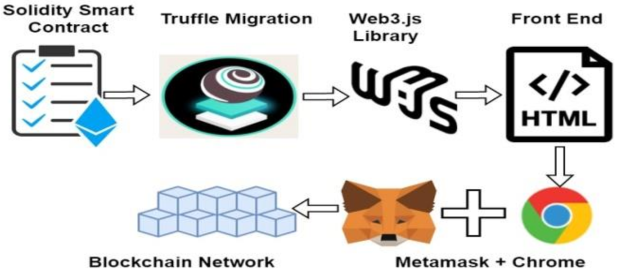
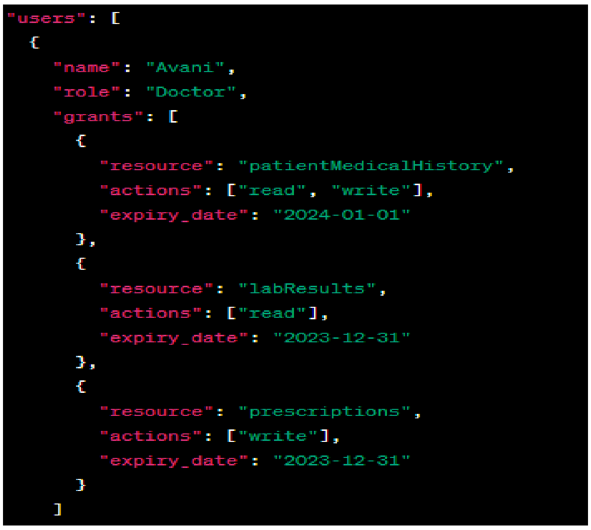


Fig.2. Process Flow of Framework



```
"users": [
  {
    "name": "Avani",
    "role": "Doctor",
    "grants": [
      {
        "resource": "patientMedicalHistory",
        "actions": ["read", "write"],
        "expiry_date": "2024-01-01"
      },
      {
        "resource": "labResults",
        "actions": ["read"],
        "expiry_date": "2023-12-31"
      },
      {
        "resource": "prescriptions",
        "actions": ["write"],
        "expiry_date": "2023-12-31"
      }
    ]
```

Fig.3. Role Assignment and access permissions to different users

4.1 Performance Analysis

In this section, we evaluate the performance of our proposed system based on the different smart contract execution, RBAC policy execution, Health Record encryption and decryption and IPFS-based EHR storage and retrieval. Fig.4 shows the average time to deploy and execute the different smart contracts. We can see that, HealthRecordStorage contract contains all the EHRs of each registered patient.

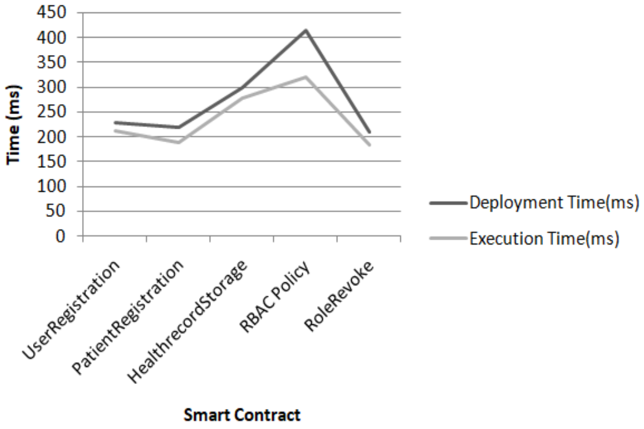


Fig.4. Computational Cost of Smart Contract

4.1.1. Efficiency

We evaluated the efficiency analysis of time required to encrypt and decrypt electronic health records (EHR) against the size of the EHRs. It involves assessing how the computational time scales as the size of the health records increases. Fig.5 shows average processing time per EHR size category.

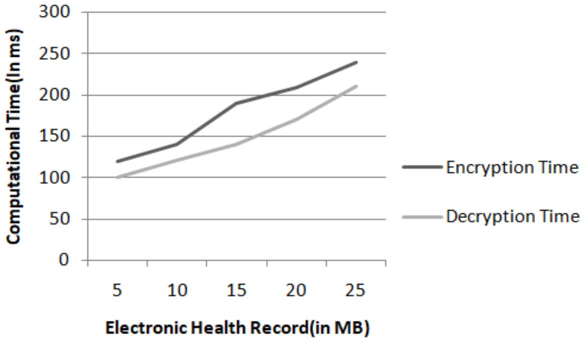


Fig.5. Computational Cost of EHR Encryption and Decryption

In Fig 6 we evaluated the latency during EHR storage and retrieval against different EHR sizes in KB. As a result, it shows computational latency of EHR storage is higher than retrieval.

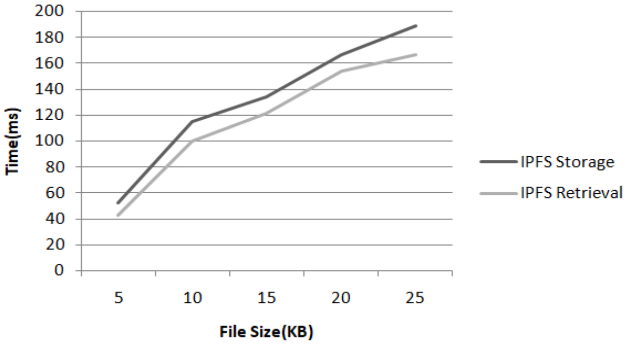


Fig.6. Computational Cost of IPFS Storage and Retrieval

4.1.2. Throughput

In this section we evaluate the performance of our proposed system with different numbers of user's request and their response time in milliseconds. Fig 7 shows how computational time varies with the number of transaction increases for the RBAC policy. Fig 7 shows, the different number of access request and their response time are evaluated for RBAC policy by the proposed system while we measure the scalability. As result shows that when number of access request increase from 10 to 50, performance of the RBHAC policy execution is stable and access are evaluated between 140 to 250ms.

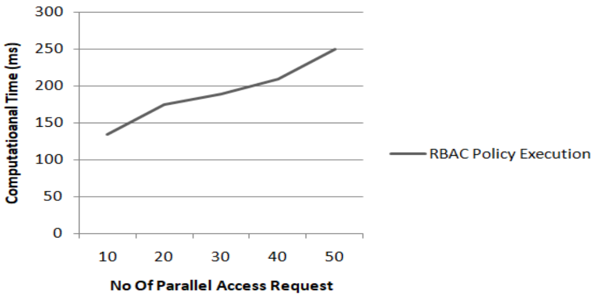


Fig.7. Computational Cost RBAC Policy Execution

We evaluate and tested the performance of token generation, verification and response process. As no of parallel access request increases, it required to record the time taken to generate token for each parallel access request. As fig.8 shows that token generation and response time scales with the increasing number of parallel access requests. We have calculated the overall throughput by considering the number of access requests handled per unit of time for both token generation and response.

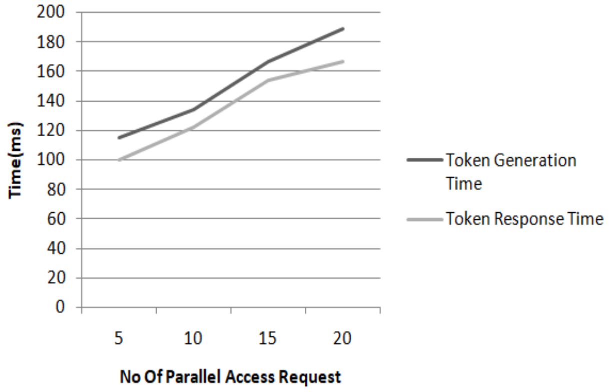


Fig.8. Computational Cost of Token Execution

5. Conclusion and Future Work

In this paper, e-DRBAC-HC, a Decentralized Role-Based Access Control for EHRs was implemented with Blockchain technology. The adoption of Blockchain technology to facilitate a decentralized role-based access control (RBAC) system represents a paradigm shift in the growing environment of healthcare data management. This study has highlighted the inherent benefits of such a decentralized system, including solid security measures, more transparency, reduced susceptibility from single points of failure, and the facilitation of a faster auditing process. Furthermore, in this study, we have proposed a

Extended Decentralized Role Based Access Control Framework to ensure Electronic Health Record access, data storage and retrieval from IPFS Storage. The presented e-DRBAC-HC Framework has made a few contributions: (i) secure encrypted EHRs exchange storage using Elliptical Curve Cryptography.(ii) Role-based Access Control policy execution for EHRs access to maintain security of records.(iii) Customized Token Generation and delegation for every users based on Role Based Access Control policy. Decentralized RBAC can lead to significant improvements in data access times, a reduction in unauthorized access incidents, and an overall enhancement in the system's trustworthiness from the perspective of both healthcare professionals and patients. Moreover, the prospective convergence of other advanced technologies, like artificial intelligence, with Blockchain can further amplify the capabilities of RBAC systems.

Author contributions

Avani Dadhania: Role of Primary Author (a) Conceptualization b) Feasibility Study (c) Requirement Analysis from Health Stakeholder (d) Writing-Original draft preparation Implementation/Coding [Python, Solidity] (e) Testing/Validation

Dr. Hiren Patel: Guidance about research problem, Documentations, Deadline Maintenance.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] A. Rejeb, K. Rejeb, S. Zailani, and Y. Kayikci, “Knowledge diffusion of halal food research: a main path analysis,” *J. Islam. Mark.*, vol. 14, no. 7, pp. 1715–1743, 2023, doi: 10.1108/JIMA-07-2021-0229.

[2] J. Y. Lee *et al.*, “Blockchain-Based Data Access Control and Key Agreement System in IoT Environment,” *Sensors*, vol. 23, no. 11, 2023, doi: 10.3390/s23115173. doi: 10.3390/s23115173. 3

[3] J. Y. Lee *et al.*, “Blockchain-Based Data Access Control and Key Agreement System in IoT Environment,” *Sensors*, vol. 23, no. 11, 2023, doi: 10.3390/s23115173. ,doi: 10.1109/MCC.2015.2.

[4] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, Healthcom 2016, 2016, doi: 10.1109/HealthCom.2016.7749510.

[5] S. Salonikias, M. Khair, T. Mastoras, and I. Mavridis, “Blockchain-Based Access Control in a Globalized Healthcare Provisioning Ecosystem,” *Electron.*, vol. 11, no. 17, 2022, doi: 10.3390/electronics11172652. doi: 10.3390/electronics11172652.

[6] M. Alsayegh, T. Moulahi, A. Alabdulatif, and P. Lorenz, “Towards Secure Searchable Electronic Health Records Using Consortium Blockchain,” *Network*, vol. 2, no. 2, pp. 239–256, 2022, doi: 10.3390/network2020016

[7] H. Li, X. Yang, H. Wang, W. Wei, and W. Xue, “A Controllable Secure Blockchain-Based Electronic Healthcare Records Sharing Scheme,” *J. Healthc. Eng.*, vol. 2022, 2022, doi: 10.1155/2022/2058497

[8] P. Sharma, R. Jindal, and M. D. Borah, “Blockchain-based cloud storage system with CP-ABE-based access control and revocation process,” *J. Supercomput.*, vol. 78, no. 6, pp. 7700–7728, 2022, doi: 10.1007/s11227-021-04179-4.

[9] E. Barka, M. Al Baqari, C. A. Kerrache, and J. Herrera-Tapia, “Implementation of a Biometric-Based Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records,” J. Sens. Actuator Networks, vol. 11, no. 4, 2022,doi: 10.3390/jsan11040085.

[10] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, “A blockchain-based attribute-based signcryption scheme to secure data sharing in the Cloud,” J. Syst. Archit., vol. 102, 2020, doi: 10.1016/j.sysarc.2019.101653.

[11] U. Chelladurai and S. Pandian, “A novel blockchain based electronic health record automation system for healthcare,” J.Ambient Intell. Humaniz. Comput., vol. 13, no. 1, pp. 693–703, 2022, doi: 10.1007/s12652-021-03163-3.

[12] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, “Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management,” IEEE Trans. Comput. Soc. Syst., 2022, doi: 10.1109/TCSS.2022.3186945.

[13] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, “An Attribute-Based Access Control Model for Internet of Things Using Hyperledger Fabric Blockchain,” *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022, doi: 10.1155/2022/6926408.

[14] L. Hong, K. Zhang, J. Gong, and H. Qian, “A Practical and Efficient Blockchain-Assisted Attribute-Based Encryption Scheme for Access Control and Data Sharing,” *Secur. Commun. Networks*, vol. 2022, 2022, doi: 10.1155/2022/4978802.

[15] K. Azbeg, O. Ouchetto, and S. Jai Andaloussi, “BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security,” *Egypt. Informatics J.*, vol. 23, no. 2, pp. 329–343, 2022, doi: 10.1016/j.eij.2022.02.004.

[16] J. H. Kang and M. Seo, “Enhanced Authentication for Decentralized IoT Access Control Architecture,” *Cryptography*, vol. 7, no. 3, 2023, doi: 10.3390/cryptography7030042.

[17] H. M. Hussien, S. M. Yasin, N. I. Udzir, and M. I. H. Ninggal, “Blockchain-based access control scheme for secure shared personal health records over decentralised storage,” *Sensors*, vol. 21, no. 7, 2021, doi: 10.3390/s21072462.

[18] A. K. Al Hwaitat *et al.*, “A New Blockchain-Based Authentication Framework for Secure IoT Networks,” *Electron.*, vol. 12, no. 17, 2023, doi: 10.3390/electronics12173618.

[19] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, “Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control,” *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, 2021, doi: 10.1109/JIOT.2021.3058946.

[20] A. Dadhania, H. Patel, “DRBAC-Healthchain (DRBAC-HC): Decentralized Role Based Access Control Framework For Achieving Security And Privacy Using Blockchain In Healthcare System,” *J. Pharm. Negat. Results*, pp. 2931–2942, 2023, doi: 10.47750/pnr.2023.14.03.368.