Privacy-Preserving eHealth Records: A Blockchain-Driven Role-Based Access Control Frame Work

Abida Khanam
Computer Application, Integral University, Lucknow, India
abidakhan@iul.ac.in

Kashif Asad
Computer Application, Integral University, Lucknow, India
kasad@iul.ac.in

Abstract: In contemporary healthcare systems, electronic medical records are often scattered across multiple hospitals and managed by centralized cloud service providers. This structure creates a significant vulnerability, as it introduces a single point of failure and limits patients' direct control over their own sensitive and confidential electronic health records (EHRs). Consequently, a major challenge in healthcare is developing a secure and efficient mechanism for accessing eHealth records while ensuring patient privacy remains a top priority. Access control, a critical aspect of computer security, is responsible for regulating access to system resources. However, existing access control mechanisms face multiple issues, such as reliance on third parties, inefficiencies, and inadequate privacy protection. Blockchain technology, which has recently gained substantial attention and holds great promise for the future, can address these challenges effectively. This paper presents an innovative authentication method that integrates blockchain-based smart contracts within a Role-Based Access Control (RBAC) framework. The proposed approach ensures decentralized and reliable access control for cloud-based medical services by leveraging multiple access control contracts. By utilizing blockchain's tamper-resistant nature and the automation capabilities of smart contracts, the system enhances the authentication process while safeguarding the confidentiality and anonymity of eHealth data. Under this model, EHRs are encrypted using Elliptic Curve Cryptography (ECC) before being stored in a cloud environment, while their corresponding hashes are recorded on the blockchain. This design takes into account the size constraints of blockchain ledgers and the vast amount of patient data. The study explores the design, implementation, and evaluation of this authentication framework, highlighting its potential to transform how healthcare institutions manage access to sensitive patient information.

***Keywords*—eHealth Records, User Authentication, Blockchain, Smart Contracts, Role-Based Access Control, Security, Privacy**

INTRODUCTION

The adoption of electronic health records (EHRs) has revolutionized data management in the healthcare sector, significantly improving patient care. These digital records have facilitated the integration of diverse clinical information, streamlined healthcare processes, and minimized errors associated with manual documentation. However, as healthcare organizations increasingly rely on EHRs to deliver patient care, concerns regarding the confidentiality and security of digital health information have become more prominent. In the eHealth domain, patient EHRs are generated from multiple sources, including wearable devices, smart sensors, and medical imaging technologies. By 2020, the volume of EHR data was projected to reach approximately 2,354 billion bytes, with an annual growth rate of 49%. The increasing adoption of EHRs in eHealth highlights their importance as a fundamental component of digital healthcare

applications, containing crucial patient-related information. These records, often classified as legal documents in hospital settings, serve as primary sources of medical data. Despite their widespread use in hospitals, medical professionals do not fully trust digital medical record systems.

Research literature has explored security risks associated with technological advancements, particularly the storage of medical records on remote servers managed by third-party cloud service providers. Health information technology encompasses all digital tools that support healthcare service delivery and system management, including patient test results, diagnoses, treatments, and medical histories. However, between 2010 and 2018, more than 2,150 healthcare data breaches occurred, exposing approximately 180,709,305 medical records, as reported by the U.S. Agency for Health and Human Services (HHS).

Privacy, security, and anonymity are critical issues in EHR systems. Although these concepts are closely related, they differ in key aspects. Security refers to the extent to which access to personal data is restricted to authorized individuals, while privacy pertains to an individual's right to control when, how, and to what extent their personal information is shared. Unauthorized access or transmission of sensitive health data can result in breaches, and systemic identification within electronic health infrastructures, along with centralized monitoring by healthcare entities, can lead to privacy violations in various scenarios.

Consequently, ensuring the security of EHR data has become a major concern in eHealth. While encryption addresses some security and privacy challenges, implementing effective access control remains difficult due to the highly distributed nature of EHR data and the complex relationships between data owners and users. Therefore, developing a flexible and regulated access control mechanism for EHR data is essential. eHealth records have transformed healthcare by improving information accessibility and service delivery, but secure and authorized access to confidential medical data must be ensured. This research introduces an innovative authentication approach that employs blockchain-based smart contracts within a role-based access control (RBAC) framework, offering a secure and efficient solution for managing access to EHRs.

A. Security and Confidentiality Concerns in Electronic Health Records (EHRs)

Electronic health records (EHRs) have significantly transformed the healthcare sector by improving patient care, streamlining administrative processes, and enabling data-driven decision-making. However, despite these advantages, serious concerns exist regarding the security and confidentiality of EHRs. This article explores the major challenges associated with EHR safety, their potential consequences, and possible solutions.

1) Unauthorized Access

One of the primary concerns with EHRs is unauthorized access. When individuals without proper authorization gain access to patient records, it can lead to identity theft and privacy violations. Healthcare professionals, employees, and external parties may attempt to access records for various reasons, including curiosity or malicious intent. Preventing unauthorized access is crucial to maintaining patient confidentiality and trust.

2) Data Breaches

EHR data breaches can occur due to cyberattacks or negligence. Hackers often target EHR systems to steal sensitive patient information, which can then be used for fraud or sold on illegal markets. Insufficient security measures, such as weak authentication protocols and poor network security, increase the risk of breaches. These incidents can have severe legal and financial consequences for healthcare providers.

3) Insider Threats

Insider threats arise when individuals within a healthcare organization misuse their access privileges. Employees may manipulate records, sell patient data, or deliberately disclose sensitive information to unauthorized parties. Such incidents pose a significant challenge as they involve trusted personnel who already have legitimate access to the system. Strengthening access controls and monitoring user activity can help mitigate insider threats.

4) Data Interoperability

Interoperability—the seamless exchange of data between different EHR systems—is essential for efficient patient care. However, it also introduces security risks, as sensitive information may be mishandled or exposed during transmission. Poorly designed interoperability mechanisms can lead to data leaks or mismanagement, compromising patient confidentiality. Secure data exchange protocols are necessary to ensure safe interoperability.

5) Consent and Control

Patients often have limited control over who can access their EHRs. A lack of transparency regarding how their data is used and shared can create concerns. Patients should have the ability to grant or revoke consent and manage data access permissions. Implementing a patient-centric access control system would empower individuals to make informed decisions about their health information.

6) Data Encryption

Encryption is a critical security measure for protecting EHRs during storage and transmission. Unencrypted data is highly vulnerable to interception and unauthorized access. Strong encryption techniques ensure that even if data is accessed by an unauthorized party, it remains unreadable and secure.

Addressing these security and confidentiality challenges is essential for maintaining trust in EHR systems and ensuring the protection of sensitive patient data. By implementing strict access controls, enhancing encryption, and improving patient consent mechanisms, healthcare providers can strengthen the security of EHRs and mitigate potential risks.

B. Traditional access control system issues

This section examines the challenges associated with existing access control mechanisms and explores how blockchain technology can provide effective solutions. Several studies have highlighted issues in centralized access management systems, particularly the risk of privacy breaches due to third-party access to sensitive personal information. Furthermore, since a single entity controls access, there is an inherent risk of a single point of failure. To mitigate these concerns, this study proposes a temporal access control mechanism and incorporates a blockchain-based permissioned verification system.

The Attribute-Based Authentication mechanism also presents several challenges, including the possibility of a single point of failure and the risk of privacy breaches stemming from private key generation. Some research suggests using decentralized storage to address these issues by implementing an architecture for secure information sharing and access management. However, existing solutions for access control across multiple administrative domains remain ineffective. Public Key Infrastructure (PKI)-based systems are difficult to manage, traditional static techniques lack scalability, and many access control methods fail to provide fine-grained authorization. A proposed alternative involves distributing and storing access policies on a blockchain with permission controls. Additionally, Conifer, a blockchain-based PKI approach, has been introduced to achieve security without relying on trusted third parties.

From a user confidentiality perspective, data sharing among multiple organizations within a cloud federation poses significant challenges. The primary concern is ensuring that user identities and personal information remain protected while still allowing authorized access to shared data. Some previous research proposes an attribute-based access management system that employs symmetric key encryption. This system grants access rights to data within a federal organization by matching users' attributes with predefined access control policies while ensuring that users’ attributes remain hidden from the organization itself. To enhance the integrity of the policy evaluation process, this study suggests leveraging blockchain technology along with a trusted operational environment.

I. THEORETICAL BACKGROUND

A. Electronic Health Records (EHRs)

Electronic health records (EHRs) serve as digital versions of patients' paper-based medical histories, providing comprehensive details about their

healthcare journey. These records include crucial information such as diagnoses, prescribed medications, treatment plans, and laboratory test results. A healthcare provider can maintain a permanent record of a patient's medical history within an EHR system, encompassing progress reports, existing medical conditions, prescribed treatments, physical symptoms, immunization records, laboratory test findings, and radiology reports. Additionally, EHRs store details on medications, vital signs, medical issues, and updates on a patient's progress.

Designed to offer a holistic view of an individual's health status, EHR systems facilitate the storage and management of medical history and treatment-related information. Access to this data is granted to authorized entities, including healthcare providers, pharmacists, laboratories, insurance companies, and other relevant services. The adoption of EHRs has significantly transformed the healthcare industry in various ways, improving efficiency, accuracy, and accessibility in patient care.

1) **Data Accessibility**

EHRs provide authorized healthcare professionals with instant and remote access to patient information, enabling them to make timely and well-informed medical decisions. Unlike traditional paper records, which may be difficult to retrieve and share, digital records ensure that patient data is available whenever needed. This accessibility is particularly beneficial in emergency situations where rapid access to a patient's medical history can significantly impact treatment outcomes.

2) **Reduced Errors**

The digitization of medical records has significantly minimized errors associated with handwritten prescriptions and manual data entry. Paper-based records are prone to misinterpretation, misplacement, and illegibility, leading to potential medical mistakes. By using EHRs, healthcare providers can rely on standardized, legible, and structured data, reducing the likelihood of errors in medication, treatment plans, and diagnostic information.

3) **Interoperability**

EHRs facilitate seamless integration of data from various healthcare sources, including hospitals, clinics, laboratories, and pharmacies. This interoperability ensures that healthcare providers have a comprehensive view of a patient's medical history, improving coordination between different medical professionals. As a result, redundant tests and unnecessary procedures can be minimized, leading to more efficient and cost-effective healthcare delivery.

4) **Patient Engagement**

By granting patients access to their own medical records, EHRs empower individuals to take an active role in managing their health. Patients can review their medical history, monitor test results, and track treatment progress, fostering greater engagement with their healthcare providers. This transparency encourages adherence to prescribed treatments and enhances communication between patients and medical professionals, ultimately leading to improved health outcomes.

Overall, EHRs revolutionize healthcare by enhancing accessibility, reducing errors, improving coordination, and encouraging patient participation, making them an essential component of modern medical systems.

B. Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is an access management model that grants user permissions based on their designated roles within an organization. In a healthcare environment, RBAC categorizes users into roles such as nurses, physicians, administrative staff, and patients, assigning specific privileges to each role. As one of the most significant advancements in access control since mandatory and discretionary access control models, RBAC plays a crucial role in regulating system access. The National Institute of Standards and Technology (NIST) formally defined RBAC in 1992.

Within the RBAC framework, users are assigned roles, and each role is linked to a set of predefined permissions. For instance, medical professionals, nurses, and pharmacists are assigned specific access

rights according to their responsibilities in a hospital setting. Organizational administrators are responsible for assigning and revoking roles as needed. The fundamental principle of RBAC is to ensure that users receive authorization based on their job functions, enabling system administrators to efficiently manage access rights in alignment with assigned tasks. This structured approach enhances security and simplifies access management within healthcare institutions.

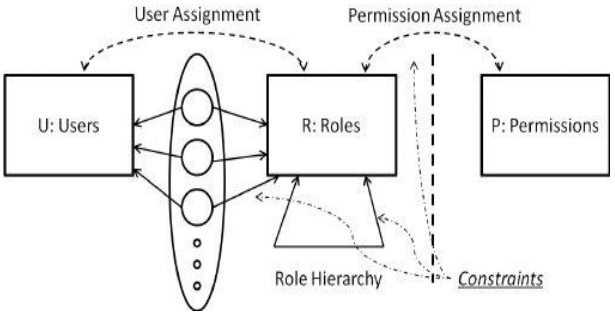

Fig. 1. Process of Role-Based Access Control[13]

Key aspects of RBAC include:

Roles: Roles are described in terms of duties or job functions. Every role is linked to a set of permissions.

Permissions: What operations people with a specific function are permitted to carry out within the system is determined by permissions. Doctors, for instance, might be allowed to read and update patient records, whereas administrative employees might only be allowed to maintain records[14].

Simplicity: By offering a structured approach where access rights are provided based on roles, RBAC streamlines access control.

In healthcare systems, RBAC acts as a core access control framework, although it may have issues managing dynamic access instances and providing fine-grained access to data.

C. Blockchain Technology

Blockchain is a distributed ledger technology that ensures secure, transparent, and tamper-resistant data storage and transactions. Initially introduced to the world through Bitcoin, a decentralized cryptocurrency created by an anonymous entity in 2008, blockchain enables a secure, decentralized peer-to-peer network without a central authority. In Bitcoin's case, blockchain facilitates a trustless digital currency system where transactions are publicly recorded, and all participants acknowledge a single historical record. Transactions are grouped into blocks, time-stamped, and added to the ledger, making them resistant to modifications. Each block contains a cryptographic hash linking it to the previous one, forming an immutable chain.

1) Key Features of Blockchain:

Decentralization: Instead of relying on a central authority, blockchain distributes data across a network of nodes, minimizing the risk of a single point of failure. This decentralized approach allows users to manage their assets without dependence on intermediaries such as organizations or financial institutions. Owners retain full control over their accounts and can transfer assets using cryptographic keys. Blockchain has the potential to revolutionize the internet by promoting decentralization and enhancing data security.

Immutability: One of blockchain's most significant advantages is its ability to create an unalterable ledger. Unlike centralized databases that rely on intermediaries for security and are susceptible to hacking, blockchain ensures that once a transaction is recorded, it cannot be modified or deleted. This guarantees data integrity, as no participant in the network can alter past records.

Enhanced Security: Compared to traditional systems, blockchain offers a higher level of security by eliminating single points of failure. Since data is distributed across multiple nodes, even if one node is compromised, the original information remains intact, ensuring that the network's integrity is not jeopardized.

Transparency: Blockchain enhances trust by making every transaction visible to network participants. This level of transparency fosters accountability and reduces the likelihood of fraud.

Beyond cryptocurrencies, blockchain technology has gained widespread recognition for its applications in data privacy, access control, and

other domains, positioning it as a transformative solution for various industries.

D. Smart Contract

Smart contracts are self-executing agreements in which the terms are written directly into code, enabling automatic fulfillment of obligations when predefined conditions are met. These contracts operate on blockchain technology, ensuring reliability and security without requiring intermediaries.

1) **Advantages of Blockchain-Based Smart Contracts:**

Automation: Smart contracts simplify processes by eliminating the need for third-party intermediaries, reducing the chances of errors and delays. Once conditions are met, the contract executes itself, enhancing efficiency.

Transparency: The execution of smart contracts is visible to all involved parties, fostering trust and ensuring that all transactions occur as agreed upon.

Security: Due to blockchain's tamper-resistant nature, smart contracts are highly secure and resistant to manipulation, ensuring that the terms remain unchanged once deployed.

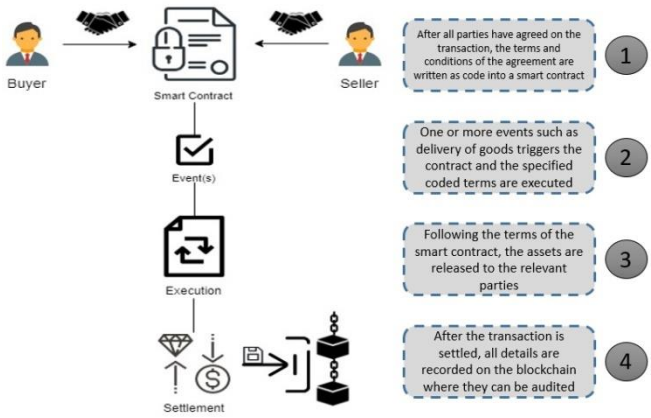

Fig.2. Process of Smart Contract [6]

Smart contracts enable the automation of various operations, including access management and authentication. This study establishes the groundwork for exploring an innovative authentication system that leverages blockchain-based smart contracts within the framework of electronic health records (EHRs) and role-based access control (RBAC). By providing a detailed explanation of these foundational concepts, the research highlights their significance and the novelty of the proposed approach. These principles form the essential framework for understanding the impact and advancements introduced by this study.

II. ROLE-BASED ACCESS CONTROL APPLYING A SMART CONTRACT BUILT ON THE BLOCKCHAIN

In this part, we provide a novel RBAC paradigm to safely and reliably validate users and their roles in the EHR system. By implementing the technology of blockchain with smart contracts, we created an RBAC paradigm for achieving user authentication. In this example, we took into account three separate entities: the role-issuer, the resource owner, and the users. The very first is the role-issuer, who gives roles to the user. The following individual is the data owner, who authorizes users based on their position and credentials inside the organization[21]. The user that accesses the resource and has access to managing their computer's network address is the last one. The suggested approach uses a Smart Contract (SC) to assign user roles and associated role permissions before publishing the information on the Ethereum blockchain[22]. The SC's key attributes are:

i) permit the organization's role-issuer to award roles to users who are members of the organization (by verifying their credentials),
ii) enabling the role-issuer to preserve the SC data,
iii) enabling the role issuer to add or remove users from SC
iv) allow the data owner to provide access to people according to their related roles and credentials, and
v) Permit the data owner to grant or revoke access to the user as necessary.

Therefore to facilitate user-role assignments quickly, efficiently, and securely, SC implements various features.

A. Role-assigning smart contract

In RBAC-SC, we consider that a role-issuer (a) in the organization creates an Ethereum's smart contract (SC). The organization will first create an account of the role-issuer SC. The creation of SC generates a pair of a private key and its externally

owned account (EOA also known as the hash of the public key). The role-issuer will use this account to deploy the role-issuing SC. These keys will execute and create different functions of SC as shown in Fig. 1. There are several options for keypair creation such as Ethereum Wallets, address generators, MetaMask [23]. We represent a.pvkey and a.pbkey for the private key and public key respectively for the role-issuer. Public key infrastructures (PKIs) manages the keys in public key cryptographic systems. They store the key pairs, digital certificates, digital signatures, and hash values. The digital signature establishes the validation of data using the cryptographic algorithm. The digital signature validates the authentication of a message (or data) by applying PKI. The user uses the digital signature and signs a message using the private key. The recipient (role-issuer) of the message uses the user's public key to determine the validity of a message. The proposed scheme adopts Elliptic Curve Digital Signature Algorithm (ECDSA) as a digital signature algorithm for signing the transaction and for the generation of public and private keys . The ECDSA algorithm requires less power as compared to other security algorithms. The Ethereum uses the Keccak-256 cryptographic hash function. After the formation of SC, the role-issuer deploys it on the blockchain. The information regarding smart contract can be seen at blockchain by using address SCr.address. The smart contract "interface" (SCr.interface) is created using Javascript Object Notation (JSON) interface. Thereafter, the role-issuer publishes the a.pbkey, SCr.address, and SC. Interface on public databases or website to make them accessible to the public. This information thus published provides proof that the owner creates and manages the SC using a.pbkey and SCr.address.

Additionally, the user (u) also has a keypair of a private key and an Externally Owned Account represented as u.pvkey and u.pbkey respectively.

The different functions that are executed by role-issuer owner SC are represented as follows:

add_User(u.pbkey, u.role, u.credentials) - The function is invoked by the owner of SC i.e., role-issuer to add individuals or users in university and assign them the corresponding roles. It takes input as the user's public key (u.pbkey), and assigns the role to the concerned user (u.role). It also takes user credentials (u.credentials) that are other necessary information regarding the user such as name, department, etc. rem_User(u.pbkey) - The function can be created and invoked through the role-issuer owner of SC to remove the users and revoke the corresponding roles from the SC. The function takes the input as a user's public key (u.pbkey). After its successful execution, remove the users, SC gets updated. addMACaddress(u.MACaddress) - The users execute the function to add their MAC Address in the SC. It takes as input the string value of the MAC address of the device which the user requires to register with the university. The corresponding function fetches the "public key" of the user. Thus, the individual (or user) can use the resources using MAC addresses registered by the organization.

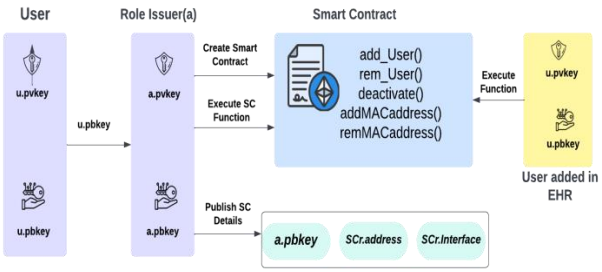

Fig.3. Role assigning smart contract flow diagram.

remMACaddress(u.MACaddress) - This function is invoked only by the user added
to the university to remove their MAC address from the SC. The function fetches the public key of the user executing the function. The function takes the input as the MAC address (u.MAC address) and removes the MAC address after it gets successfully executed. Consequently, the smart contract is amended.

deactivate() - The particular function is invoked by the owner/creator of the SC. After the execution of this function, the smart contract is inactive and no longer in use.

B. Data owner smart contract

According to RBAC-SC, a data owner (o) generates smart contracts (SC). The resource access provisioning SC is deployed by each data owner for their specific resource. We display the data owner's private key & public key as o.pvkey and o.pbkey, accordingly. This keypair creates and carries out the many SC operations. Similar to how SC is created,

Scr.address is generated when the data owner deploys SC on the chain of Ethereum. Additionally, the data owner makes this public key (o.pbkey), SCr.address, and Interface available to the public by publishing them on a website that is accessible to everyone. The following functions are provided by the data owner SC: grantResourceAccess(u.pbkey) - The EHR data owner uses this specific function to grant access to the resource. The user's public key is the input for the aforementioned function.

rmvResourceAccess(u.pbkey) - The SC data owner will be used to call the function. Once more, this method accepts the user's public key as input to revoke the user's privileges to access resources. The smart contract is altered as a result.

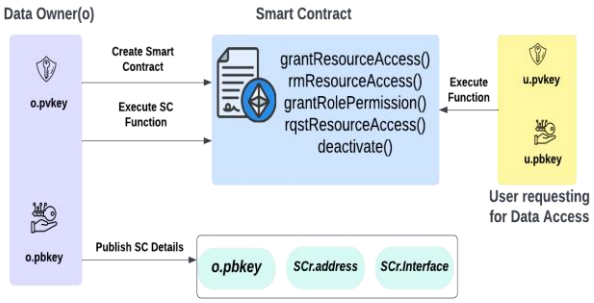

Fig. 4. Data Owner smart contract flow diagram.

grantRolePermission(u.role, o.permission) - The owner of the SC performs this role. The function accepts parameters for the user's role and associates the role's authorization (o.permission) with the arguments. When the function is called, it outputs to SC a record of all the data. The smart contract gets updated as a result.

rqstResourceAccess() - When a user asks permission to a data from its owner, this function is carried out by that user. The user's address is retrieved by this method when they request information.

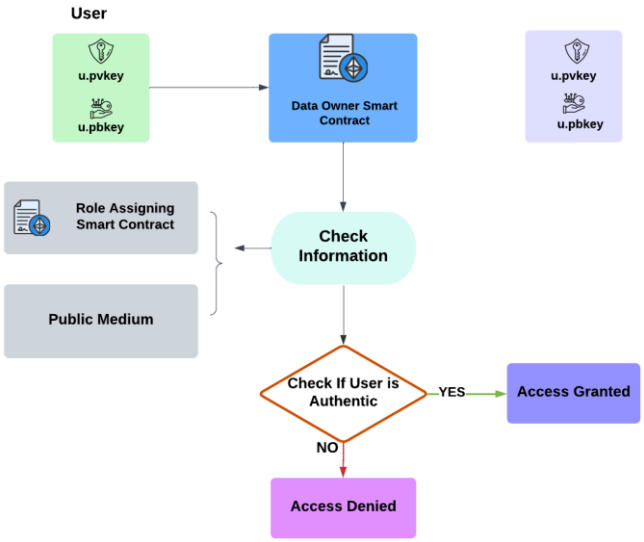

Fig. 5. Role-Based Access Control model using smart contract.

The data owner SC is to provide access to the records, as shown in Fig. 3. The data owner reviews the records posted by the role-assigning SC on a public media, like an internet site or a database, when requests are made. The owner of the data confirms the allocated permissions and the role's authorization with the user. The role-assigning SC's data is used for authenticating the user's credentials. If a user establishes their authenticity, they are given access to the records[24]. However, no privilege is granted to the user if they cannot be discovered in the role-assigning SC or do not match the requirements. The owner of the resource has the ability to revoke user access as well as the permission that was given to the role.

To establish the right to use the public address, a fresh user in the organization employs a digital signature. The role-issuer uses the add_User() method to add an individual to the SC when the user's legitimacy has been verified. The user can add or delete MAC addresses from the SC by using the addMACaddress() or remMACaddress() functions, respectively. The resource owner then installs the SC and calls the procedure grantRolePermission() to save the information. By utilizing the reqResourceAccess() method, the user asks the resource owner to allow access to the resource. The resource owner retrieves the user's information from the role-assigning SC after receiving the user demand[25].

III. Discussion

The performance of the role-based access control (RBAC) model utilizing blockchain technology was assessed to determine its efficiency and security. The primary objective is to leverage blockchain, specifically Ethereum, to develop a secure, cost-effective, efficient, and adaptable RBAC framework. This section highlights the benefits of blockchain over traditional centralized RBAC models and evaluates its key features.

1) Verification

The framework implements a verification mechanism using public keys and digital signatures. In this process, a user generates a digital signature on a message using their private key. This signature is then verified using the corresponding public key to confirm the authenticity of the user. This cryptographic method ensures strong identity verification, preventing unauthorized access.

2) Running Time

The performance analysis indicates that the proposed blockchain-based RBAC system requires less processing time compared to the RBAC-SC model. The evaluation was conducted by varying the number of users in an organization. Unlike RBAC-SC, which employs a challenge-response protocol, the proposed system demonstrates superior time efficiency, particularly as the user base grows. This advantage makes it scalable for large organizations.

3) Security

Blockchain technology significantly enhances security by addressing multiple concerns, including authorization, data integrity, and non-repudiation. Solidity, the programming language used for Ethereum smart contracts, includes built-in modifiers that authenticate users, further strengthening access control. Additionally, the immutability of blockchain ensures that once data is recorded, it cannot be altered, thereby protecting against unauthorized modifications and fraudulent activities.

This evaluation demonstrates that integrating blockchain into RBAC systems offers substantial improvements in security, efficiency, and scalability compared to conventional centralized access control models.

Conclusion

Due to the centralized nature of access control systems, businesses often encounter challenges related to authentication and security management. To address these issues, this study introduces a role-based access control (RBAC) model leveraging Ethereum blockchain and smart contract functionalities. The proposed approach provides a fast, secure, and efficient method for managing user-role assignments within an organization. The system architecture includes two Ethereum-based smart contracts: one responsible for assigning or revoking user roles and permissions, and the other for granting or restricting access based on the assigned roles. Digital signatures are employed to authenticate users and verify their role ownership. By utilizing blockchain's decentralized framework, this solution enhances user identity management, verification, security, and customization. Additionally, the distributed nature of blockchain technology ensures improved authentication, privacy protection, and system adaptability.

Reference

[1] Z. Ying, L. Wei, Q. Li, X. Liu, and J. Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud," *IEEE Access*, vol. 6, pp. 53698–53708, 2018, doi: 10.1109/ACCESS.2018.2871170.

[2] A. Haddad, M. H. Habaebi, F. E. M. Suliman, E. A. A. Elsheikh, M. R. Islam, and S. A. Zabidi, "Generic Patient-Centered Blockchain-Based EHR Management System," *Appl. Sci.*, vol. 13, no. 3, 2023, doi: 10.3390/app13031761.

[3] E. K. Christiansen, E. Skipenes, M. F. Hausken, S. Skeie, T. Østbye, and M. M. Iversen, "Shared Electronic Health Record Systems: Key Legal and Security Challenges," *J. Diabetes Sci. Technol.*, vol. 11, no. 6, pp. 1234–1239, 2017, doi: 10.1177/1932296817709797.

[4] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egypt. Informatics J.*, vol. 22, no. 2, pp. 177–183, 2021, doi: 10.1016/j.eij.2020.07.003.

[5] J. B. D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "Generalized Temporal Role Based Access Control Model (GTRBAC) Part I 1 Introduction," 2002.

[6] G. I. Microgrid, "Applications of the Blockchain Technology in the Energy Sector : The Case of MSc . in Energy : Strategy , Law and Economics Master ' s Thesis Applications of the Blockchain Technology in the Energy Sector : The Case of Greek Islands ' Microgrid Supervisin," no. May, 2020, doi: 10.13140/RG.2.2.30697.93289.

[7] H. Guo, W. Li, M. Nejad, and C. C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 44–51, 2019, doi: 10.1109/Blockchain.2019.00015.

[8] M. M. Madine *et al.*, "Blockchain for Giving Patients Control over Their Medical Records," *IEEE Access*, vol. 8, no. October, pp. 193102–193115, 2020, doi: 10.1109/ACCESS.2020.3032553.

[9] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5914–5925, 2021, doi: 10.1109/JIOT.2020.3032997.

[10] N. Jamshed, F. Ozair, A. Sharma, and P. Aggarwal, "Ethical issues in electronic health records: A general overview," *Perspect. Clin. Res.*, vol. 6, no. 2, p. 73, 2015, doi: 10.4103/2229-3485.153997.

[11] A. Gharat, P. Aher, P. Chaudhari, and B. Alte, "A Framework for Secure Storage and Sharing of Electronic Health Records using Blockchain Technology," *ITM Web Conf.*, vol. 40, p. 03037, 2021, doi: 10.1051/itmconf/20214003037.

[12] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, 2019, doi: 10.1109/JIOT.2018.2847705.

[13] S. Raje, C. Davuluri, M. Freitas, R. Ramnath, and J. Ramanathan, "Using ontology-based methods for implementing role-based access control in cooperative systems," *Proc. ACM Symp. Appl. Comput.*, no. March, pp. 763–764, 2012, doi: 10.1145/2245276.2245421.

[14] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-based access control using smart contract," *IEEE Access*, vol. 6, pp. 12240–12251, 2018, doi: 10.1109/ACCESS.2018.2812844.

[15] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, Sep. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[16] N. Al Asad, M. T. Elahi, A. Al Hasan, and M. A. Yousuf, "Permission-based blockchain with proof of authority for secured healthcare data sharing," *2020 2nd Int. Conf. Adv. Inf. Commun. Technol. ICAICT 2020*, no. November, pp. 35–40, 2020, doi: 10.1109/ICAICT51780.2020.9333488.

[17] R. Kumar, "Scalable Inter-operable and Secure Healthcare Framework For Sharing Patient Medical Report using Blockchain and IPFS Technology," 2022, doi: 10.21203/rs.3.rs-2115239/v1.

[18] R. Charanya, R. A. K. Saravanaguru, and M. Aramudhan, "Sefra: A secure framework to manage ehealth records using blockchain technology," *Int. J. E-Health Med. Commun.*, vol. 11, no. 1, pp. 1–16, Jan. 2020, doi: 10.4018/IJEHMC.2020010101.

[19] P. Kamboj, S. Khare, and S. Pal, "User authentication using Blockchain based smart contract in role-based access control," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2961–2976, 2021, doi: 10.1007/s12083-021-01150-1.

[20] H. S. Jennath, V. S. Anoop, and S. Asharaf, "Blockchain for Healthcare: Securing Patient Data and Enabling Trusted Artificial Intelligence," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 6, no. 3, p. 15, 2020, doi: 10.9781/ijimai.2020.07.002.

[21] 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.

[22] I. Saenko and I. Kotenko, "Administrating role-based access control by genetic algorithms," *GECCO 2017 - Proc. Genet. Evol. Comput. Conf. Companion*, pp. 1463–1470, 2017, doi: 10.1145/3067695.3082509.

[23] C. Gan, A. Saini, Q. Zhu, Y. Xiang, and Z. Zhang, "Blockchain-based access control scheme with incentive mechanism for eHealth systems: patient as supervisor," *Multimed. Tools Appl.*, vol. 80, no. 20, pp. 30605–30621, 2021, doi: 10.1007/s11042-020-09322-6.

[24] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, Feb. 2018, vol. 2017-October, pp. 1–5, doi: 10.1109/PIMRC.2017.8292361.

[25] F. Ghaffari, E. Bertin, J. Hatin, and N. Crespi, "Authentication and Access Control based on Distributed Ledger Technology: A survey," *2020 2nd Conf. Blockchain Res. Appl. Innov. Networks Serv. BRAINS 2020*, pp. 79–86, 2020, doi: 10.1109/BRAINS49436.2020.9223297.

[26] P. Barnaghi, Association for Computing Machinery, Institute of Electrical and Electronics Engineers, and Web Intelligence Consortium, "Proceedings, 2019 IEEE/WIC/ACM International Conference on Web Intelligence (WI 2019) : Thessaloniki, Greece, 13-17 October 2019," *2Proceedings, 019 IEEE/WIC/ACM Int. Conf. Web Intell. (WI 2019) Thessaloniki, Greece, 13-17 Oct. 2019*, p. 511.

[27] A. H. Kashmar, "Encryption key Generation Protocol Based on Elliptic Curve and PSO." [Online]. Available: https://www.researchgate.net/publication/366095384.

[28] A. I. Mendoza Arvizo, L. Avelar Sosa, J. L. García Alcaraz, and O. Cruz-Mejía, "Beneficiary Contracts on a Lightweight Blockchain Architecture Using Smart Contracts: A Smart Healthcare System for Medical Records," *Appl. Sci.*, vol. 13, no. 11, 2023, doi: 10.3390/app13116694.