RAJIV GANDHI INSTITUTE OF TECHNOLOGY

GOVERNMENT ENGINEERING COLLEGE

KOTTAYAM-686 501

DEPARTMENT OF COMPUTER APPLICATIONS

20MCA244 - SEMINAR REPORT

ENHANCING IDENTITY AND ACCESS MANAGEMENT USING HYPERLEDGER FABRIC AND OAUTH 2.0: A BLOCKCHAIN-BASED APPROACH FOR SECURITY AND SCALABILITY FOR HEALTHCARE INDUSTRY

Submitted By

GOPIKA KRISHNAN S

(KTE22MCA-2025)

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

THIRUVANANTHAPURAM

APRIL 2024

ACKNOWLEDGMENT

I want to express my gratitude to everyone who has supported me throughout the endeavor. First and foremost, I give thanks to God Almighty for His mercy and blessings, for without His unexpected direction, this would still be only a dream.

I sincerely thank **Dr. Prince A**, Principal, Rajiv Gandhi Institute of Technology, Government Engineering College, Kottayam, for providing the environment in which this seminar could be completed.

I owe a huge debt of gratitude to **Dr. Reena Murali**, Professor and HOD, Department of Computer Applications for granting permission and making available all of the facilities needed to complete the seminar properly.

I am profoundly honored and deeply grateful to express my sincere appreciation to my seminar guide and staff advisor **Prof. Jincy Kuriakose**, for her invaluable guidance and support, as well as to **Prof. Ancy Emmanuel**, co-staff advisor for providing constructive suggestions and inspiration throughout the seminar.

Finally, I would like to take this chance to express my gratitude to the entire teaching and technical staff members of the Department of Computer Applications.

GOPIKA KRISHNAN S

ABSTRACT

The seminar is based on the paper ”Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A blockchain based approach for security and scalability for the healthcare industry”, by S. Sutradhar et al, Internet of Things and Cyber-Physical Systems 4 (2024). The management of electronic health records (EHRs) presents significant issues in the rapidly changing healthcare industry. EHRs are vulnerable to problems such as unauthorized access, data tampering, or breaches, primarily due to their centralized storage structure. Therefore, a transformational solution is required. Blockchain technology offers a safer and better way to handle healthcare records. Unlike the traditional system, blockchain uses advanced methods to secure information, creating a secure and unchangeable ledger of all transactions. Not controlled by one central authority, blockchain is robust against failures and attacks. This not only keeps patient data safe and private but also allows for easy and secure sharing of information among healthcare providers. It can even help in stopping medical fraud and reducing administrative costs. Using special codes called cryptography ensures that the information on the blockchain cannot be messed with or changed, making it ideal for keeping critical data secure, like in financial transactions. In healthcare, Identity and Access Management (IAM) systems play a crucial role. IAM systems ensure that only authorized individuals can access sensitive health data using unique credentials and additional security measures. IAM systems not only control access but also ensure that data is used following rules and regulations, such as the General Data Protection Regulation (GDPR). Other technologies, like Privacy-Enhancing Technologies (PET), also help in making healthcare data more private and secure. For instance, data anonymization hides or changes identifying information in datasets, protecting sensitive details. Encryption is like putting a lock on sensitive data, making sure it stays safe during storage, transmission, and processing. Implementing cryptography, IAM systems, and PET categories helps protect sensitive health data when it’s stored, sent, or processed, making it less likely for unauthorized access or data compromise to happen. The proposed system utilizes blockchain, specifically Hyperledger Fabric and OAuth 2.0, to make a secure system for managing healthcare data access. Hyperledger Fabric keeps things private, secure, and scalable, while OAuth 2.0 ensures that only trusted applications can access specific data. This ensures transparency, security, and reduces the risk of fraud. So, system can work well with a large amount of data and different applications, making it a safe and easy way to control access within the network. Moreover, the secure record of actions provided by the system can help catch any

attempts to access or change things without permission, adding an extra layer of security. Role-based Access Control (RBAC) based on a patient's role ensures privacy and confidentiality. The solution can efficiently and securely manage patient identity and access. This could change how healthcare works, making data sharing better, reducing fraud and mistakes, and enhancing patient privacy and security. Importantly, the system follows health regulations such as HIPAA (Health Insurance Portability and Accountability Act) and GDPR (General Data Protection Regulation), meeting the required standards. This system, with extra-strong security, not only deals with current problems but also sets the stage for a safer, smoother, and patient-focused healthcare system. In changing healthcare, using such solutions is vital for patient safety and data protection.

Keywords: Block-chain, Hyper-ledger fabric network, OAuth2.0, Identity and Access Management (IAM)

Table of Contents

List of Figures

List of Tables

Chapter 1

INTRODUCTION

This chapter introduces a blockchain-based IAM system in healthcare, tackling EHR vulnerabilities. Leveraging decentralized blockchain, it ensures tamper-proof records, patient data control, enhanced security, fraud prevention, and cost reduction. The system promises transformative changes in healthcare practices aligned with emerging technological standards.

1.1 Need

The blockchain-based Identity and Access Management (IAM) system [1] addresses critical needs within the healthcare industry, primarily stemming from the vulnerabilities inherent in traditional electronic health record (EHR) systems. In conventional architectures, centralized EHR systems are susceptible to security breaches, data tampering, and unauthorized access. These weaknesses pose significant risks to the confidentiality and integrity of sensitive patient information. The blockchain-based IAM system responds to these challenges by leveraging advanced cryptographic techniques and decentralized technology. Blockchain's tamper-proof ledger ensures the security of all transactions, mitigating the risks associated with centralized control. Furthermore, the system introduces transparency and immutability, allowing patients to assert control over their data while enabling healthcare providers to securely and efficiently share information. Beyond safeguarding against security threats, the decentralized nature of blockchain technology contributes to the creation of a trustless system. By eliminating the need for a centralized authority or intermediary, the IAM system not only enhances security but also establishes a resilient framework capable of withstanding failures and attacks. Additionally, the system aims to address broader industry concerns, including the prevention of medical fraud, reduction of administrative costs, and facilitation of compliance with regulations such as the General Data Protection Regulations (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). Through these capabilities, the system seeks to transform the healthcare sector by fostering data interoperability, minimizing errors, and fortifying patient privacy and security.

1.2 Objective

The blockchain-based Identity and Access Management (IAM) system in healthcare has clear goals. Firstly, it wants to make sure patient records are super safe by using smart technology. It aims to share control among different parts of the healthcare system, making it stronger and better at handling problems. The system also wants to make it easy for patients to decide who gets to see their information while letting healthcare providers share data securely. Additionally, it's determined to stop fraud and save on administrative costs by using technology that keeps a super secure and unchangeable record of all transactions. The system is keen on following healthcare rules to protect patient data and aims to create a safer environment by removing the need for one central authority. Overall, it wants to make healthcare data easier to share, reduce mistakes, and keep patient information private and secure.

1.3 Scope

Aiming to revolutionize healthcare practices, the blockchain-driven Identity and Access Management (IAM) system has a comprehensive scope, touching on several crucial aspects to enhance the overall functionality of the healthcare industry. Its primary goal is to bolster the security of electronic health records (EHRs) by implementing advanced cryptographic techniques, fortifying defenses against unauthorized access and ensuring the integrity of data. Central to its scope is the establishment of a decentralized control framework, distributing authority across the blockchain network to enhance system resilience against potential failures and attacks, contributing to the creation of a more robust and trustworthy infrastructure. Furthermore, the system aspires to facilitate transparent and efficient management of patient data, empowering individuals to control access and enabling secure data sharing among healthcare providers. Its scope extends to fraud prevention and cost reduction, utilizing blockchain's tamper-proof characteristics to prevent medical fraud and reduce administrative expenses through secure transaction record-keeping. Compliance with healthcare regulations, including GDPR and HIPAA, is a pivotal consideration, ensuring the privacy and security of patient information. By eliminating the need for a centralized authority, the system seeks to establish a trustless environment, thereby enhancing overall security and resilience. Revolutionizing healthcare, enhancing data interoperability, reducing errors, and ensuring patient privacy. The system ensures scalability, flexibility, and transformative changes aligning with tech standards in healthcare.

Chapter 2

LITERATURE REVIEW

Diving into notable works, this chapter explores blockchain applications in data privacy, identity verification, industrial blockchains, electronic health records, and healthcare. These studies present diverse perspectives, addressing challenges and envisioning innovative solutions within the blockchain landscape.

2.1 System Study

G. Zyskind et al [2] present Decentralizing Privacy: Using Blockchain to Protect Personal Data. The paper proposes a decentralized personal data management system ensuring user ownership and control. The decentralized approach to personal data management is imperative amid escalating privacy concerns. Existing privacy-preserving methods like anonymization and encryption are limited, prompting exploration of blockchain's potential in addressing societal trusted computing issues. The protocol introduces blockchain for automated access control management, prioritizing data ownership, transparency, and fine-grained access control, particularly pertinent in mobile platforms where data collection occurs without user consent. By amalgamating blockchain and off-blockchain storage, a privacy-focused data management platform is envisaged, with detailed network protocol and security analysis. Future blockchain extensions, such as multi-party computation for secure data processing and dynamic trust measures for nodes, are proposed to enhance decision-making and bolster network resilience. This proposal advocates for decentralized personal data management systems, empowering users with ownership and control while addressing privacy concerns. It underscores the significance of blockchain integration, offering transparency, access control, and ownership, thereby enriching the discourse on data privacy and ownership and presenting a compelling case for decentralized solutions in contemporary data management practices.

Ben Cresitello-Dittmar [3] explores Application of the Blockchain for Authentication and Verification of Identity. The paper aims to overcome the limitations of traditional authentication methods by proposing blockchain's decentralized and secure nature. It discusses blockchain's

security attributes, including its trustless nature and proof of work, advocating for its application in authentication, identification, secure data transfers, and two-factor authentication. Challenges such as security, trust in third parties, and vulnerabilities in certification authorities and private key management are addressed, alongside potential misuse in voting systems. Proposed authentication flows and data minimization strategies offer technical insights and use case scenarios. Emphasizing the need for a nuanced understanding of blockchain's limitations despite its promise, the document urges cautious adoption, recognizing both its potential benefits and inherent complexities. It underscores the imminent need to revamp existing authentication systems and positions blockchain as a promising avenue for addressing these challenges. Offering a comprehensive examination of blockchain-based authentication, the document navigates technical, security, and practical considerations, laying groundwork for informed decision-making in adopting blockchain for identity verification and authentication.

W. Li et al [4] propose Towards Scalable and Private Industrial Blockchains. The paper addressing scalability, privacy, and governance challenges in industrial applications. The proposed solution introduces satellite chains, independent subchains interconnected within a single blockchain system, maintaining private ledgers and supporting diverse consensus protocols. It incorporates a "hands-off" regulator enforced via smart contracts. Integration with Hyperledger Fabric v0.6 is discussed, with insights on potential integration with v1.0 to address existing framework limitations. Emphasizing blockchain's significance in finance and retail, the document notes challenges like privacy and scalability, proposing satellite chains to tackle these issues. It details system model, cross-chain asset transfer, and integration with Hyperledger Fabric, highlighting agnostic architecture for seamless platform integration. Potential applications in trade finance, asset management, and supply chain are explored. Integration with Hyperledger Fabric v1.0 is discussed, underscoring enhancements for industrial use cases through support for satellite chains and asset transfers. Overall, the document offers a comprehensive view of blockchain limitations, proposed solutions, Hyperledger Fabric integration, and potential industrial impact.

A. Shahnaz et al [5] propose Using blockchain for electronic health records. The paper introduces a framework for implementing blockchain technology in healthcare, focusing on secure electronic record storage and granular access control. It tackles issues like data security, integrity, and management prevalent in Electronic Health Record (EHR) systems. Transitioning from paper-based to EHR systems, it addresses challenges like interoperability and data

breaches, advocating for a decentralized blockchain solution for patient-centric healthcare. The framework leverages blockchain and off-chain storage to enhance scalability, security, and data integrity. Architecturally, it comprises users, a blockchain layer, and a system implementation layer, utilizing Ethereum and IPFS with smart contracts defining user roles and access. Performance evaluation includes execution time, throughput, and latency assessments, showcasing efficiency and scalability. Data payload, transaction size, and fees are discussed, emphasizing secure and efficient patient record handling. Compared to related work, the framework ensures secure, authorized, and tamper-proof record storage, addressing traditional EHR system challenges comprehensively.

Sadia Ramzan et al [6] propose 'Healthcare Applications Using Blockchain Technology: Motivations and Challenges.' The topic provides a detailed analysis of blockchain technology, its types, and its impact on healthcare. It underscores secure and efficient data management's criticality in healthcare amidst challenges like population growth, treatment accessibility, and data security. It extols blockchain technology's potential to revolutionize healthcare by securing electronic health records (EHRs) and patient information. Providing a comprehensive overview, it elucidates blockchain's technical aspects, types, and motivations, highlighting applications in remote patient monitoring, supply chain management, and interoperability. Specific use cases are explored, including EHR management, global scientific data sharing, data storage, and security. Integration with the Internet of Medical Things (IoMT) is discussed to bolster data security and chronic condition monitoring. The paper also examines blockchain's application in pharmaceutical supply chain management, ensuring medicine authenticity, quality, and efficient claims and billing management. Overall, it emphasizes blockchain's transformative potential across various healthcare domains, addressing critical issues and enhancing patient care and industry efficiency.

Table 2.1: Literature Review

Sl No.	Title	Author	Objective	Features
1	Decentralizing Privacy: Using Blockchain to Protect Personal Data(2015) [2]	G. Zyskind et al	Address privacy concerns in personal data management. Give users control over their data for transparency, auditing, and specific access.	Decentralized Personal Data Management and Privacy Protection.
2	Application of the Blockchain For Authentication and Verification of Identity (2016) [3]	Ben Cresitello-Dittmar	Address limitations of current authentication methods. Explore blockchain applications for identity authentication and verification.	Secure data transfers and identity verification. Protects against identity theft.
3	Towards Scalable and Private Industrial Blockchains (2017) [4]	W.Li et al	Address limitations of current blockchain systems. Propose a new blockchain architecture that meets industrial needs.	Integration with Hyperledger Fabric. Privacy Assurance
4	Using blockchain for electronic health records(2019) [5]	A. Shahnaz et al	Address challenges in EHR systems. Define clear guidelines for access control	Decentralization and Data Transparency
5	Healthcare Applications Using Blockchain Technology: Motivations and Challenges(2022) [6]	Sadia Ramzan et al	Examine motivations and challenges in adopting blockchain for healthcare. Offer a detailed overview of blockchain, including its technicalities, types, and core principles.	Verify the integration of traditional healthcare with blockchain. Examine issues and propose improvements for ongoing studies.

The reviewed literature underscores the transformative potential of blockchain in various domains. From decentralized personal data management and authentication to healthcare applications and industrial blockchains, these studies explore blockchain's ability to address privacy concerns, enhance scalability, and overcome governance challenges. They collectively highlight the broad-reaching impact of blockchain across different sectors.

Chapter 3

PROPOSED SYSTEM

This chapter unveils key contributions, focusing on scalability, interoperability, and lowered administrative expenses. The detailed workflow and a thorough comparative analysis of authentication methods provide deeper insights into the system's functionality and effectiveness.

3.1 Key Contributions of the Proposed System

The key contributions of the proposed system are outlined as follows:

- **Integration of OAuth2.0 and Hyper-ledger Fabric:** OAuth 2.0 and Hyperledger Fabric work together to create a strong and adaptable system for controlling access to the Fabric network. OAuth 2.0 manages user authentication securely, allowing trusted third-party providers. Hyperledger Fabric adds privacy, security, and scalability, ensuring careful control over who accesses sensitive information. Together, they form a reliable foundation for efficiently handling access within the Fabric network.

- **Role-based Access Control:** The system applies role-based access control (RBAC) according to the patient's role. This guarantees privacy and confidentiality by providing access to specific data based on predefined roles, minimizing the risk of unauthorized exposure to data.

- **Mitigation of cyber risks and data breaches:** Addressing cyber risks and potential data breaches involves deploying cutting-edge technologies and frameworks like blockchain, cryptography, Identity and Access Management (IAM) systems, and Privacy-Enhancing Technologies (PET). Organizations can thereby mitigate the risks associated with cyber-attacks and unauthorized access, ensuring the protection of sensitive health data throughout storage, transmission, and processing.

- **Compliance with Regulatory Requirements:** Addressing regulatory compliance needs, the solution aligns with frameworks like HIPAA and GDPR. IAM systems govern access

to health data, while the incorporation of Privacy-Enhancing Technologies (PET), such as data anonymization and encryption, bolsters privacy and security, ensuring adherence to regulatory standards.

- **Statistical Analysis:** The study incorporates a statistical analysis showcasing the effectiveness and security of the approach in handling patient identity and access. This analysis offers proof of the system's potential to bring about significant changes in the healthcare sector, diminishing fraud and errors, advancing data interoperability, and fortifying patient privacy and security.

- **Scalability and Interoperability:** The system's architecture is crafted for managing substantial data volumes and accommodating various applications. Hyperledger Fabric's modular design ensures scalability, enabling the system to adapt to changing demands. Additionally, OAuth 2.0 enhances interoperability by permitting only trustworthy applications to access designated data on the Fabric network.

- **Reduced Administrative Costs:** The incorporation of blockchain technology can effectively decrease administrative expenses related to Electronic Health Records (EHRs). The streamlined processes, automation, and enhanced efficiency offered by blockchain systems eliminate intermediary roles and reduce paperwork, leading to significant cost savings for healthcare organizations.

3.2 Workflow of Proposed System

The step-by-step workflow is elucidated in Figure 3.1, detailing the process of accessing sensitive resources utilizing OAuth 2.0 authentication and authorization servers for user identity verification. Notably, all access and authorization transactions are recorded on the tamper-proof Hyperledger Fabric blockchain, guaranteeing transparency and security. The decentralized ledger technology provides an immutable record, enhancing system integrity. The workflow of the IAM system is outlined as follows

1. **Step1: User Access Attempt**

   The user initiates access to a sensitive resource, starting the interaction with the system's workflow.

2. **Step2: OAuth 2.0 Authentication**

   Users are directed to the OAuth 2.0 authentication server, where they input credentials or opt for a trusted provider. The OAuth 2.0 server validates the user's identity, issuing an access token upon confirmation. This token serves as proof of authentication throughout the user's interaction with the system, ensuring secure access to sensitive resources.

3. **Step3: Access Token Presentation**

   The user submits the access token to the resource server as a credential for authentication and authorization validation.

4. **Step4: OAuth 2.0 Authorization**

   The resource server validates the access token by consulting the OAuth 2.0 authorization server, ensuring its legitimacy and permissions. Based on this verification, the authorization server communicates approval or rejection to the resource server for granting or denying access to the requested resource.

5. **Step5: Resource Access**

   Upon approval, the resource server permits access to the sensitive resource. Every transaction, including access grants, is securely recorded on the Hyperledger Fabric blockchain. This ensures a transparent and tamper-proof record of all interactions, enhancing system integrity and providing a verifiable history of resource access within the blockchain ledger.

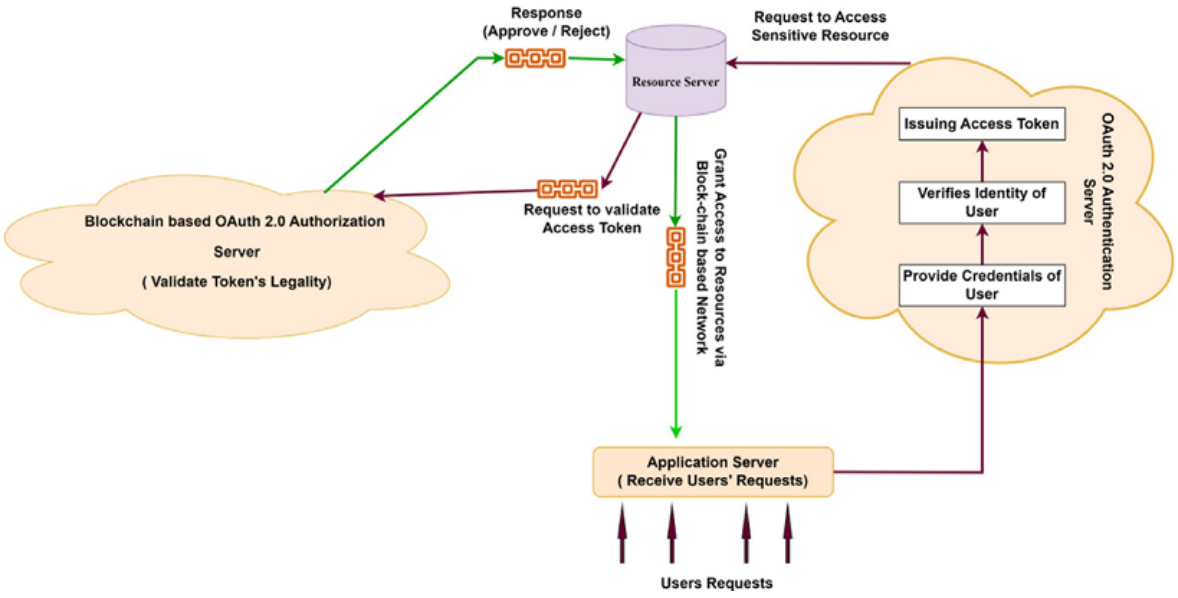

Figure 3.1: Detailed Transmission of Users' Requests Workflow of IAM

3.3 Comparative Analysis

Comparative analysis of the proposed system, considering three common authentication methods—biometric authentication, zero-trust architecture, and multi-factor authentication—where security, usability, scalability, and deployment complexity are the key factors.

- **Biometric Authentication:**

  The security aspect of the proposed system relies on the utilization of biometrics, such as fingerprints and iris scans, to ensure robust user authentication and potentially decrease the risk of unauthorized access. While this approach enhances security, it introduces considerations for usability, as implementation may necessitate specialized hardware and user enrollment processes, potentially impacting user convenience. Scalability becomes a relevant factor in managing large user populations, and the integration of diverse biometric systems can pose challenges. Additionally, the deployment complexity of the system is influenced by the intricate nature of setting up and maintaining the required biometric infrastructure. These factors collectively shape the efficacy and feasibility of incorporating biometric authentication within the proposed system, necessitating a balanced assessment of security benefits against usability, scalability, and deployment complexities.

- **Zero-Trust Architecture:**

  Zero-Trust Architecture, as a key component of the proposed system, emphasizes several important considerations. In terms of security, it implements continuous authentication and authorization, minimizing trust assumptions and access risks. This approach enhances the overall security posture by consistently verifying the legitimacy of users and their access permissions. However, this heightened security comes with potential challenges in usability, as the implementation and management of a Zero-Trust Architecture can be complex, potentially impacting the user experience. On the scalability front, this architecture is specifically designed for dynamic environments characterized by frequent user and device changes, ensuring adaptability to evolving scenarios. Nevertheless, the deployment complexity of a Zero-Trust Architecture should not be overlooked, as it necessitates significant infrastructure changes and demands expertise to be effectively implemented. Balancing the robust security features with considerations for usability, scalability, and deployment complexities is crucial in evaluating the overall suitability of Zero-Trust Architecture within the proposed system.

- **Multi-Factor Authentication (MFA):**

  Multi-Factor Authentication (MFA), a vital component in the proposed system, contributes to enhanced security by introducing an additional layer of authentication beyond passwords. This approach adds an extra level of protection against unauthorized access attempts. Notably, MFA is relatively user-friendly and widely adopted, minimizing disruption to existing workflows and ensuring a smoother user experience. In terms of scalability, MFA integrates seamlessly with existing systems and can be easily scaled to accommodate growth, making it adaptable to evolving user and organizational needs. While implementation requires integration with existing authentication systems, the overall deployment complexity is considered straightforward, adding to the practicality and feasibility of incorporating MFA within the proposed system. This makes MFA a promising choice, striking a balance between heightened security measures, user-friendliness, scalability, and deployment simplicity.

The analysis of three authentication methods within the proposed system highlights their unique trade-offs in terms of security, usability, scalability, and deployment complexity. The final choice for authentication will be determined by aligning these factors with the specific priorities and requirements of the proposed system in the context of the healthcare industry.

Chapter 4

MATERIALS AND METHODS

Detailing the methodology, this chapter systematically implements a secure, decentralized identity and access management system with OAuth 2.0 and Hyperledger Fabric. It covers programming languages, technologies, simulation setup, and comprehensive testing procedures.

4.1 System Design

The authentication and authorization system depicted in Fig. 4.1 is a conceptual representation of the proposed identity and access management system. The system comprises several key components:

- **Database (DB):** Stores and manages data related to user identities, permissions, and transactions.
- **Application Server (App-server):** Acts as an intermediary between the client application (App) and the authentication and authorization server (Auth-server). It is responsible for interacting with the App, retrieving information from the DB, and, if necessary, coordinating tasks with the Auth-server.
- **Authentication and Authorization Server (Auth-server):** Utilizes blockchain technology for validating transactions, ensuring security and transparency. It is responsible for authenticating users and authorizing their actions within the blockchain network.
- **Client Application (App):** The user-facing component that interacts with the system through various interfaces such as web, mobile, or standalone applications.

The distributed system architecture facilitates secure and decentralized communication between these components, emphasizing modularity and scalability. Users are required to undergo authentication and authorization processes handled by the Auth-server to access the system's functionality. The App-server plays a crucial role in connecting the blockchain network and the Auth-server, authenticating users, and granting access to the database.

The App-server communicates directly with the blockchain network, executing commands, altering the global state, and authenticating users. The system involves participating nodes (M1–M3) in the blockchain network, maintaining the ledger, and executing the consensus process. When Auth-server and App-server are separate, modularity allows multiple application servers to connect to the same Auth-server for authentication and authorization. An off-blockchain DB stores additional data, reducing the volume of data stored in the blockchain. The App-server requires permission confirmation in the blockchain before accessing the DB.

This architecture is designed to emphasize security, decentralization, and modularity, facilitating efficient data management and scalability.

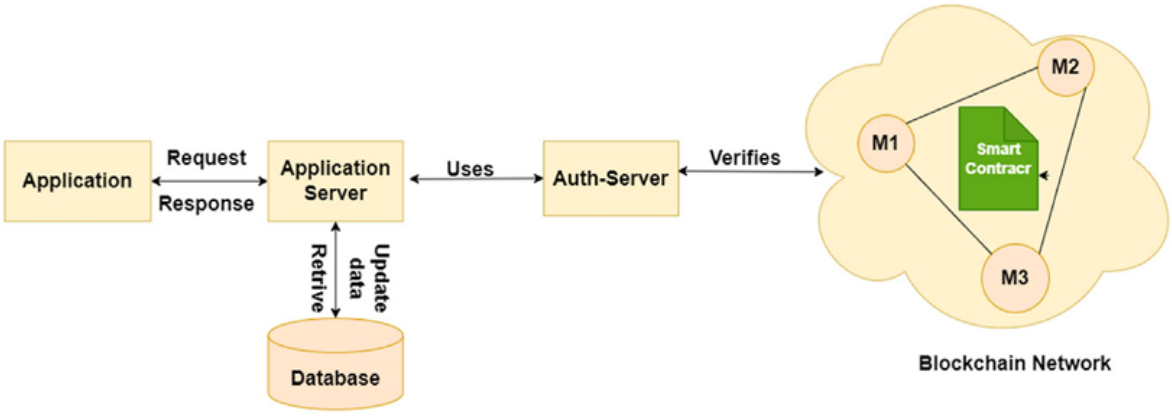

Figure 4.1: Architecture of the Blockchain Based Smart Contract Identification and Access Management System

4.2 Implementation

Implementing a secure and decentralized identity and access management system involves several steps.

1. **Initialize the OAuth 2.0 Server:**

   To initialize the OAuth 2.0 server, the first step involves selecting and installing appropriate OAuth 2.0 server software, such as OpenID Connect or a custom implementation. Once installed, each external application intending to access the system is assigned a unique OAuth 2.0 client ID and secret. These credentials serve as secure keys for communication between the applications and the OAuth 2.0 server. Additionally, OAuth 2.0

scopes are created to precisely define the level of data access permitted for each application. By specifying these scopes, the system ensures controlled and secure data access, enhancing overall security in user authentication and authorization processes.

2. **Implement the Hyperledger Fabric Network:**

   To implement the Hyperledger Fabric network, the first step involves selecting an appropriate Hyperledger Fabric implementation, such as IBM Blockchain Platform, AWS Managed Blockchain, or Azure Blockchain Service. Following this, the Fabric network is designed and deployed with a focus on privacy, security, and scalability considerations. The network setup includes the establishment of channels to manage access control and data segregation. Lastly, data access policies are defined, specifying which data can be accessed by authorized applications. This comprehensive approach ensures the creation of a secure and scalable Hyperledger Fabric network, emphasizing controlled data access and adherence to privacy and security measures.

3. **Define Data Access Policies:**

   To enhance the security of the Hyperledger Fabric network, specific data access policies are specified, detailing the permissions for accessing different types of data. Additionally, a role-based access control (RBAC) system is implemented. This RBAC system ensures that user access to data is governed by predefined roles, adding an extra layer of granularity to the access control mechanism. By incorporating RBAC, the Fabric network can efficiently manage and regulate user permissions, contributing to a robust and secure data access framework within the Hyperledger Fabric ecosystem.

4. **Authenticate Users Using OAuth 2.0:**

   To enhance user authentication within the system, users are provided with the flexibility to authenticate either through traditional user credentials or trusted third-party identity providers, such as Google, Facebook, or LinkedIn. This dual authentication approach broadens accessibility while maintaining security. Additionally, a two-factor authentication (2FA) mechanism is implemented to fortify security. 2FA adds an extra layer of protection by requiring users to verify their identity through a secondary method, such as a mobile app or SMS code. This combined authentication strategy ensures a robust and secure user authentication process within the system.

5. **Authorize Third-Party Applications:**

   To facilitate controlled access to data on the Hyperledger Fabric network, third-party applications are authorized through a systematic process. The OAuth 2.0 server plays a key role in this authorization, issuing access tokens exclusively to applications that have been authorized. These access tokens serve as secure credentials, allowing the authorized applications to interact with and retrieve specific data from the Fabric network. By employing OAuth 2.0, the system ensures that only trusted third-party applications receive the necessary permissions to access and utilize data on the Hyperledger Fabric network. This approach enhances security and maintains a structured framework for data access control.

6. **Separation of Authentication and Authorization Processes:**

   Strengthening security and scalability is achieved by segregating authentication and authorization processes, ensuring a more resilient system that efficiently manages user access while preserving data integrity and confidentiality.

7. **Use Blockchain Technology:**

   The system leverages blockchain technology to ensure transparency and tamper-proof transactions. This decentralized ledger records all interactions securely. Access policies and user permissions are stored directly on the Hyperledger Fabric network, enhancing security and providing a robust foundation for managing user access.

8. **Continuously Monitor and Update the System:**

   Continuous monitoring of the system is conducted to identify and address potential security vulnerabilities. Regular updates are performed to enhance both security measures and system scalability, ensuring a proactive approach to maintaining a secure and resilient system.

4.3 Technical Framework

- **Backend Technology:** Node.js with Express was selected for the backend due to its efficiency in handling core system functionalities. This combination offers a lightweight and event-driven architecture, allowing for fast and scalable development. Express, a web

application framework for Node.js, further streamlines the creation of robust and efficient backend services.

- **Blockchain Implementation:** Leveraging Node.js, we crafted chain code for the Hyperledger Fabric network, establishing a resilient and secure foundation for blockchain infrastructure. Node.js, known for its asynchronous capabilities, contributed to efficient code execution, while Hyperledger Fabric ensured tamper-resistant and transparent transactions, making the blockchain infrastructure robust and reliable.

- **Containerization and Orchestration:** Docker streamlined containerization, encapsulating components for efficient deployment. Simultaneously, Docker Swarm provided harmonious coordination among containers, optimizing system orchestration. This combination enhanced scalability, simplifying the management of distributed applications and ensuring seamless communication between containers for an effective and well-coordinated system.

- **Cloud Hosting:** AWS Cloud served as the dependable hosting platform for the Hyperledger Fabric network, guaranteeing both accessibility and stability. This choice of cloud infrastructure played a pivotal role in ensuring the reliability of our system, facilitating consistent and secure access to the network while maintaining its overall stability.

- **User Authentication:** JSON Web Tokens (JWT) play a pivotal role in defining and managing user roles and permissions, establishing a secure and controlled access mechanism. By employing JWT, the system ensures the integrity of user roles and permissions, contributing to a robust framework for secure access control.

- **Access Control:** Role-based access control (RBAC) libraries, like Casbin, were integrated to regulate user access across various system functionalities. This implementation ensures a structured and secure access management system, where users are granted permissions based on their roles, contributing to effective control and security within the system.

- **Federated Authentication:** Open ID Connect and OAuth 2.0 bolster security by implementing federated authentication processes. These mechanisms guarantee a robust and authenticated user interaction, enhancing the overall security posture of the system. By employing industry-standard protocols, the system ensures a trustworthy and secure environment for user authentication and authorization.

- **Two-Factor Authentication (2FA):** Security measures are fortified through the implementation of two-factor authentication (2FA) using libraries like Speakeasy. This additional layer of security enhances the protection of user accounts by requiring a second form of verification, ensuring a more resilient defense against unauthorized access and potential security threats.

- **OAuth 2.0 Client Authorization:** Passport.js ensures secure authorization of third-party applications through OAuth 2.0. This integration facilitates the secure and reliable authentication of external services, enabling seamless interaction with the system while adhering to established security protocols and standards.

- **API Gateway Integration:** Efficient streamlining of authentication and authorization processes was realized by integrating API Gateway solutions, such as Kong or Tyk. These tools serve as a centralized gateway, managing access controls and authentication tasks, ensuring a secure and organized flow of communication between the system and external entities.

- **Distributed Ledger Technology:** Chosen for its robust features, Hyperledger Fabric served as the distributed ledger technology, guaranteeing transparency and safeguarding transactions against tampering. This selection reinforced the integrity of the system by providing a secure and immutable foundation for recording and managing transactions.

- **Smart Contract Management:** The critical role of Node.js-based chain code was highlighted in managing data access policies and user permissions through the implementation of smart contracts. This component ensured a secure and efficient mechanism for governing how data is accessed and how user permissions are defined within the system.

- **DevOps Automation:** Jenkins automation played a pivotal role in optimizing continuous integration and deployment, contributing to the enhancement of development and release processes. This streamlined approach facilitated efficient and reliable integration of code changes, ensuring a smooth and effective deployment pipeline in the software development lifecycle.

- **System Monitoring:** Logging and monitoring tools conducted continuous health checks, ensuring the reliability of the system. These tools played a crucial role in tracking system performance, identifying potential issues, and maintaining overall system health for sustained operational effectiveness.

- **Updates Management:** Frequent updates were executed to uphold the system's security and scalability. This proactive approach involved implementing necessary patches, improvements, and modifications to ensure the system remained resilient and adaptable to evolving requirements.

4.4 Simulation Set-up

To simulate the system, follow these steps:

1. **Set up the Development Environment:**
   To prepare the development environment, install Node.js, Docker, and required libraries. Node.js facilitates server-side application execution, while Docker ensures consistent runtime environments. Create an AWS Cloud account and establish a Hyperledger Fabric network on AWS, configuring peer nodes and channels. This setup forms the basis for developing and deploying applications with Hyperledger Fabric in a cloud environment.

2. **Develop and Deploy the Backend Application:**
   Construct the backend application using Node.js and Express, creating a robust foundation. Integrate OAuth 2.0 and OpenID Connect to secure authentication and authorization processes. Implement two-factor authentication and Role-Based Access Control (RBAC) mechanisms, enhancing security measures. This comprehensive setup ensures a secure, efficient, and multifaceted backend system for applications, promoting user authentication and controlled access.

3. **Develop and Deploy the Chain Code:**
   Compose chain code using Node.js to govern the Hyperledger Fabric network. Establish data access policies through smart contracts, ensuring controlled data interactions. Deploy the crafted chain code by encapsulating it in Docker containers and orchestrating with Docker Swarm. This systematic approach enhances the reliability and security of the chain code, facilitating efficient execution within the distributed network environment.

4. **Integrate the API Gateway:**
   Leverage Kong or Tyk as the API Gateway to streamline external access to the system.

The API Gateway serves as a centralized control point, efficiently managing authentication and authorization processes. By utilizing these gateways, the system ensures secure and standardized interactions between external applications and the underlying infrastructure, contributing to enhanced overall performance and security.

5. **Monitor and Update the System:**

   Ensure the system's reliability by employing continuous monitoring tools and log analysis for proactive issue detection. This ongoing surveillance guarantees optimal performance and identifies potential vulnerabilities promptly. Regularly update the system to incorporate the latest security measures and scalable features, reinforcing its robustness against evolving threats and ensuring it aligns with the latest technological advancements.

This simulation set-up involves developing and deploying multiple components, integrating them to create a secure and decentralized identity and access management system. The use of specified programming languages and technologies ensures scalability and security in handling authentication, authorization, and data access policies.

Chapter 5

RESULT

The identity and access management (IAM) system, blending OAuth 2.0 and Hyperledger Fabric, offers a solid solution for handling patient records in healthcare. Built on blockchain technology, it ensures data security, transparency, and precise control over patient information. To understand its performance, the analysis delves into how the system responded when more entries were added to the blockchain.

As more information was added to the blockchain, the system's response time for answering questions and carrying out tasks was impacted. The system's speed depended on both the number of entries in the blockchain and the specific task at hand. Basic functions like logging in and updating data were relatively quick, aligning with the time it took to look up information in the blockchain. However, certain actions, such as registering or changing permissions, took a little more time. This interaction between different tasks and the load on the blockchain provides insights into how the system performs in various situations.

The system shows promise in practical applications, enhancing data integrity, transparency, and integrating OAuth 2.0 with Hyperledger Fabric for robust access controls. Additionally, the inclusion of role-based access control, customized to the specific roles of patients, provides precise control over data access. Importantly, the system ensures compliance with healthcare regulations such as HIPAA and GDPR by limiting access to sensitive information to authorized personnel only. This comprehensive approach not only secures patient data but also aligns with existing privacy and security standards. This iterative approach ensures that the IAM system continues to evolve into a resilient, scalable, and cutting-edge solution for healthcare data management, with the ultimate goal of transforming the healthcare industry's digital landscape.

Chapter 6

PERFORMANCE ANALYSIS

In this chapter, the focus is on the Performance Evaluation of the algorithm, highlighting crucial aspects such as authentication and authorization speed, access control efficiency, and system scalability. Strategic implementations like OAuth 2.0 and Hyperledger Fabric are explored to unveil the algorithm's effectiveness, with a particular emphasis on performance metrics and comprehensive testing for ongoing refinement.

6.1 Performance Evaluation

In evaluating the performance of the algorithm, key factors such as the speed of authentication and authorization, the efficiency of access control, and the scalability of the system must be considered.

1. **Speed of Authentication and Authorization:**

   The implementation of OAuth 2.0 as the authentication server ensures expeditious user authentication. This is achieved through the verification of user credentials or redirection to trusted providers for authentication. The utilization of access tokens further reduces the time required for authorization, focusing on checking token validity and permissions. Optimizing the configuration of the OAuth 2.0 server and ensuring swift communication between the server and the resource server can significantly enhance the speed of authentication and authorization processes.

2. **Efficiency of Access Control:**

   The implementation of OAuth 2.0 as the authentication server ensures expeditious user authentication. This is achieved through the verification of user credentials or redirection to trusted providers for authentication. The utilization of access tokens further reduces the time required for authorization, focusing on checking token validity and permissions. Optimizing the configuration of the OAuth 2.0 server and ensuring swift communication between the server and the resource server can significantly enhance the speed of authentication and authorization processes.

3. **Scalability of the System:**

   Ensuring the scalability of the proposed algorithm is reliant on the use of Hyperledger Fabric, known for its modular architecture that adapts seamlessly to the dynamic needs of the system. Additionally, the separation of authentication and authorization processes provides a scalable framework for managing user access to resources. By optimizing the system's architecture efficiency and its capability to handle diverse user loads and transaction volumes, the overall scalability of the system can be effectively increased.

4. **Performance Metrics and Benchmarks:**

   A comprehensive evaluation of the algorithm's performance necessitates the execution of benchmark tests and stress tests. These assessments should encompass diverse conditions, including varying user loads and network scenarios, to ensure the system's adaptability. Addressing any identified issues or bottlenecks during these tests is imperative for continual improvement and optimization of the system's overall performance.

This structured analysis provides a detailed exploration of specific performance aspects, offering a comprehensive understanding of the algorithm's effectiveness.

6.2 Performance Metrics for Block-chain Operations

Figure 6.1 illustrates the commendable overall performance of the blockchain system, notably revealing that the registration of new users consumes more time compared to other routine operations. The figure depicts the system's performance metrics, emphasizing vital operations such as Registration, Grant Permission, Revoke Permission, and Invoke. It visually presents the time needed for each operation, providing valuable insights into user registration speed, permission management duration, and transaction latency on the blockchain network. Granting, revoking, and invoking permissions all exhibit faster growth, with function invocation showing the most efficient performance. Despite the blockchain's secure and transparent nature, its distributed architecture inherently impacts speed and cost considerations.

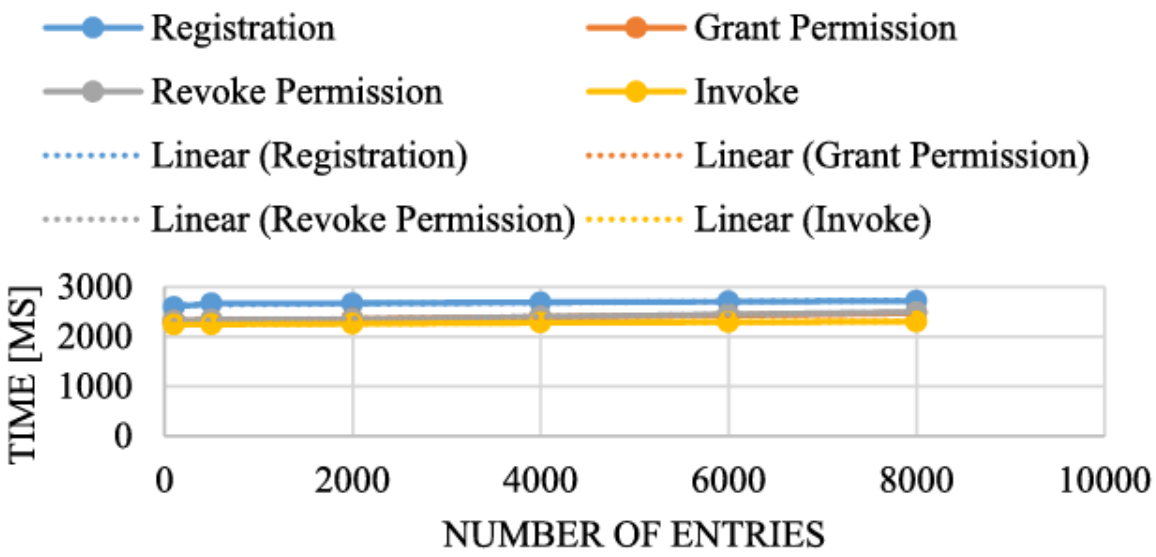

Figure 6.1: Measurements of the Performance of Blockchain Based on Registration, Grant Permission, Revoke Permission, and Invoke

The blockchain system exhibits efficient performance, with user registration taking more time. Granting, revoking, and invoking permissions demonstrate faster growth, emphasizing the system's distributed nature impacting speed and cost.

6.3 Performance Evaluation for Essential Operations

Analyzing diverse blockchain sizes on a local server revealed a correlation between blockchain size and entry numbers, as depicted in Figure 6.2. As entries increased, tasks such as querying and invoking the blockchain, along with system operations, saw a slight time increment. In a blockchain with a single entry, the average query time is 54 ms, and the average invoke time is 2272 ms. With a rising number of entries, operations like registration, permission granting, and login displayed prolonged durations, indicating potential challenges for the system's scalability and efficiency.

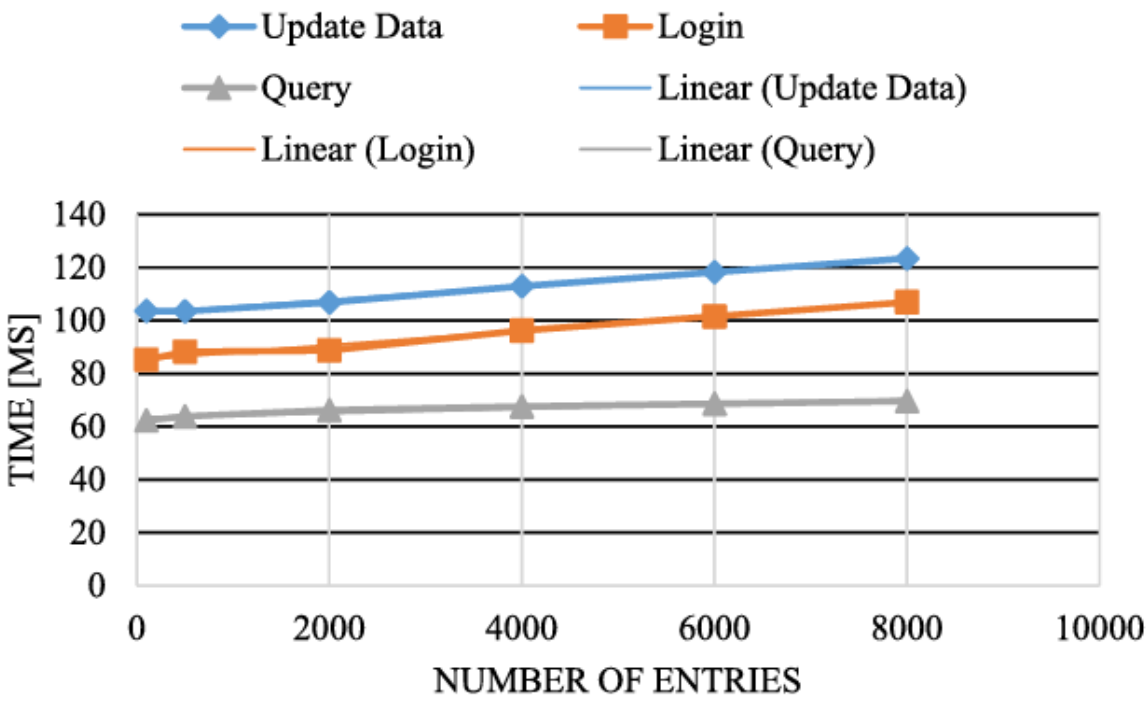

Figure 6.2: Measurements of the Performance of Blockchain Based on Update Data, Log-in, and Query

Examining diverse blockchain sizes on a local server reveals a correlation between size and entry numbers. As entries increase, querying, invoking, and system operations experience slight time increments, posing scalability and efficiency challenges.

Chapter 7

CONCLUSION

The blockchain-based framework outlined here addresses critical challenges in healthcare, focusing on identity management and access control for enhanced security and privacy in patient data sharing. This innovative framework leverages the inherent advantages of blockchain technology, including decentralization, immutability, and transparency, to establish a secure and finely-grained access control solution for managing sensitive patient information. The integration of OAuth 2.0 and Hyperledger Fabric ensures scalability and robust security, safeguarding the Fabric network against unauthorized access by permitting only approved applications. The algorithm outlined for constructing a secure and decentralized identity and access management system through the combination of OAuth 2.0 and Hyperledger Fabric provides a comprehensive guide for framework implementation. Key features such as the segregation of authentication and authorization processes, reliance on trusted authentication providers, and the issuance of access tokens to authorized applications by the OAuth 2.0 authorization server contribute to the algorithm's security and scalability. By empowering patients with control over their health data and ensuring exclusive access for authorized entities, this framework and algorithm possess the transformative potential to revolutionize the healthcare sector. Additionally, the tamper-proof audit trail embedded in the framework serves as a robust deterrent against unauthorized access or tampering attempts, augmenting the overall security posture of the system. In essence, the effort introduces a user-friendly and secure solution poised to revolutionize the management of healthcare data. Beyond safeguarding patient privacy, this framework offers a robust defense against unauthorized access or alterations. As the healthcare sector advances into the digital realm, the framework emerges as a beacon of security and control, empowering individuals to dictate who accesses their health information and preserving the trustworthiness of the entire healthcare ecosystem.

Chapter 8

FUTURE SCOPE

To advance the algorithm, future efforts can focus on key areas. Firstly, enhancing interoperability and broadening the system's reach could be achieved by integrating the algorithm with other blockchain platforms like Ethereum, Corda, and Quorum. This expansion would foster seamless collaboration across different blockchain ecosystems, promoting a more interconnected and versatile system. Prioritizing user experience by refining the user interface to be more intuitive and accessible, particularly for non-technical users, holds significant potential. A more user-friendly interface would contribute to the algorithm's usability, ensuring a smoother and more inclusive interaction for individuals with varying technical expertise. Streamlining system efficiency and minimizing errors can be achieved by implementing smart contracts to automate the application of permission criteria, enhancing the overall efficiency and contributing to error reduction in the application of permissions. Additionally, integrating machine learning algorithms to detect anomalies and potential security threats stands as a valuable avenue for enhancing the system's security and reliability. This proactive approach to security would empower the system to identify and respond to emerging threats, bolstering its resilience against potential risks. Lastly, developing mobile applications would significantly increase the system's accessibility, empowering users to conveniently utilize the system through their smartphones and aligning with the prevalent trend of mobile-centric interactions, providing flexibility in accessing the system. Addressing these areas of focus contributes to the algorithm's technical robustness and positions it for more effective and widespread application in real-world scenarios.

REFERENCE

[1] S. Sutradhar, S. Karforma, R. Bose, S. Roy, S. Djebali, and D. Bhattacharyya, "Enhancing identity and access management using Hyperledger Fabric and OAuth 2.0: A blockchain based approach for security and scalability for the healthcare industry," Internet of Things and Cyber-Physical Systems, vol. 4, pp. 49-67, 2024. ISSN 2667-3452.

[2] B. Cresitello-Dittmar, Application of the Blockchain for Authentication and Verification of Identity, Independent Paper, 2016, pp. 1–9, 2016.

[3] G. Zyskind, O. Nathan, Decentralizing privacy: using blockchain to protect personal data, in: IEEE Security and Privacy Workshops, IEEE, 2015, May, pp. 180–184, 2015.

[4] W. Li, A. Sforzin, S. Fedorov, G.O. Karame, Towards scalable and private industrial blockchains, in: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017, April, pp. 9–14.

[5] A. Shahnaz, U. Qamar, A. Khalid, Using blockchain for electronic health records, IEEE Access 7 (2019) 147782–147795.

[6] Ramzan, A. Aqdus, V. Ravi, D. Koundal, R. Amin and M. A. Al Ghamdi, "Health care Applications Using Blockchain Technology: Motivations and Challenges," in IEEE Transactions on Engineering Management, vol. 70, no. 8, pp. 2874-2890, Aug. 2023, doi: 10.1109/TEM.2022.3189734.

[7] D.H. Sharma, C.A. Dhote, M.M. Potey, Identity and access management as security as-a service from clouds, Procedia Comput. Sci. 79 (2016) 170–174.

[8] S.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, K.S. Kwak, The internet of things for health care: a comprehensive survey, IEEE Access 3 (2015) 678–708.