ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

Enhancing Healthcare Identity and Access Management using Hyper ledger Fabric and OAuth 2.0: A Block chain-Powered Solution for Enhanced Security and Scalability

Debnath Bhattacharyya

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation (KLEF), Vaddeswaram 522302, Andhra Pradesh, India

Abstract

A block chain-driven framework for managing identity and access emerges as a promising remedy to the privacy and security concerns in sharing patient data within the healthcare sector. This innovative technology guarantees the safeguarding of sensitive information's confidentiality and integrity by establishing a decentralized and immutable ledger. Our study introduces an identity and access management system leveraging the capabilities of Hyperledger Fabric and OAuth 2.0, thereby augmenting security and scalability. The amalgamation of these technologies ensures the transparency and immutability of user transactions, substantially mitigating the risks of fraudulent activities and unauthorized entries.Furthermore, Hyperledger Fabric's prowess in privacy, security, and scalability empowers the implementation of meticulous access control mechanisms for sensitive data. Simultaneously, OAuth 2.0 validates solely trustworthy third-party applications' access to specific data within the Fabric network. This novel approach seamlessly handles voluminous data loads and supports diverse applications, thus constituting a secure and scalable solution for administering access within the Fabric network. In addition to these attributes, our solution incorporates a Role-based Access Control model, aligning access privileges with a patient's designated role to uphold their privacy and confidentiality. Our rigorous statistical analysis validates the effectiveness and security of the proposed strategy in competently managing patient identity and access. Furthermore, the proposed solution seamlessly aids compliance with regulatory mandates like HIPAA and GDPR.

Keywords: Identity & access management Block-chain Hyper-ledger fabric network OAuth2.0 Role-based access control system

Introduction:

In the realm of modern healthcare, the secure exchange of patient information is a critical imperative. However, as data sharing becomes increasingly digital and interconnected, it brings forth profound

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

challenges in terms of privacy, security, and scalability [1]. The inherent sensitivity of healthcare data necessitates robust mechanisms to ensure that patient information remains confidential, unaltered, and accessible only to authorized entities [2]. In response to these challenges, blockchain technology has emerged as a promising solution, offering the potential to revolutionize the way identity and access management are approached within the healthcare industry. Blockchain's decentralized and immutable nature addresses the vulnerabilities present in traditional data sharing systems, thereby offering a framework for establishing trust and security in digital interactions. Hyperledger Fabric, a prominent blockchain platform, is recognized for its capabilities in enhancing privacy, security, and scalability. In tandem with OAuth 2.0, a well-established authorization protocol, a formidable synergy emerges that could redefine how identity and access management are executed within the healthcare landscape.In this context, our research seeks to present a groundbreaking approach that leverages the strengths of Hyperledger Fabric and OAuth 2.0 to forge an advanced identity and access management system. This system is specifically tailored to address the unique security and scalability requirements of the healthcare industry [3]. By melding blockchain's immutable ledger with OAuth 2.0's authentication and authorization capabilities, we aim to create an environment that not only safeguards patient data but also enables seamless data sharing across trusted parties [4]. This paper delves into the intricacies of our proposed blockchain-based identity and access management framework. It explores the fundamental challenges faced by the healthcare sector in terms of data security and scalability. Moreover, it elucidates the theoretical underpinnings of Hyperledger Fabric and OAuth 2.0, detailing how their integration can yield a robust, adaptable solution [5]. By fostering transparency, traceability, and granular access control, we envision our approach as a stepping stone towards achieving enhanced patient privacy, streamlined data sharing, and compliance with regulatory standards.Through rigorous analysis and empirical evidence, we aim to demonstrate the feasibility and effectiveness of our proposed approach. The subsequent sections of this paper will elucidate the core components of our blockchain-based identity and access management system, the methodology employed, the results obtained, and the broader implications of our findings [6]. Ultimately, we endeavor to contribute to the ongoing discourse surrounding secure and scalable healthcare data management by presenting a novel paradigm that harnesses the synergies of blockchain and established authorization protocols [7].

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

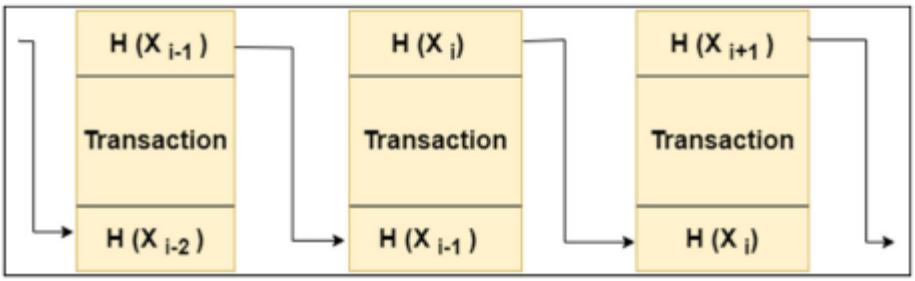

Fig. 1. Partial architecture of block-chain.

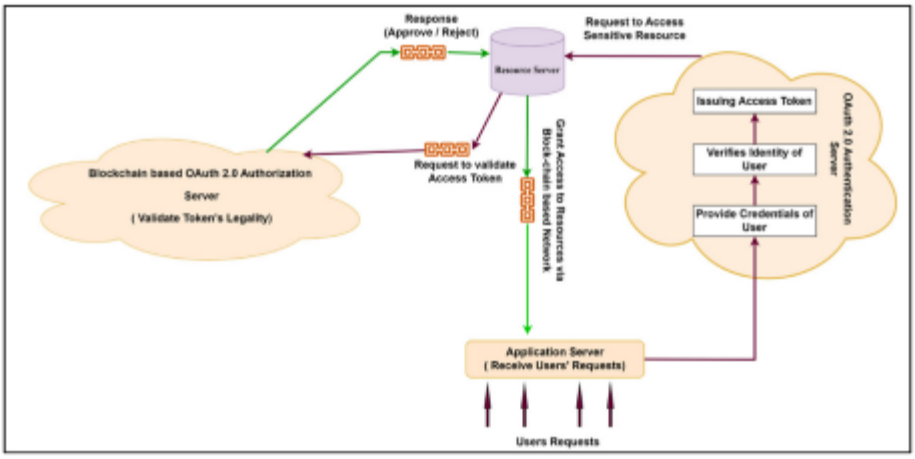

Fig. 2. Detailed transmission of Users Request & workflow of IAM.

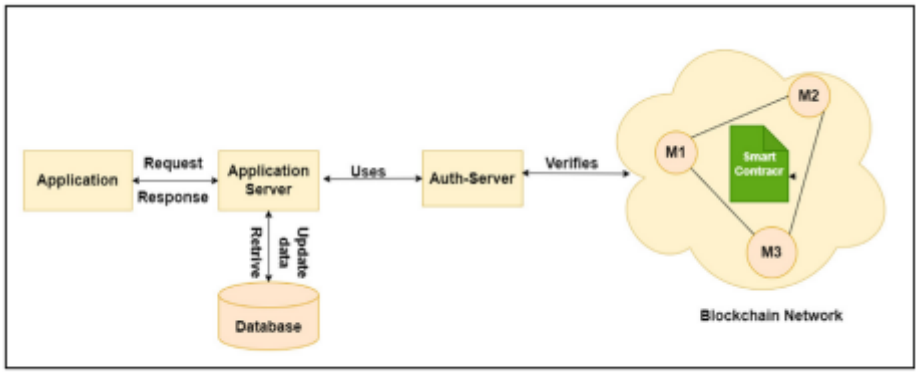

Fig. 3. Architecture of the block-chain-based smart contract identification and access management system.

Methodology

The proposed blockchain-based identity and access management system using Hyperledger Fabric and OAuth 2.0 offers several key contributions that address critical challenges in the healthcare industry.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

These contributions significantly enhance security, scalability, and overall data management. The primary contributions of the system are [8]:

1. **Decentralized Identity Management:** The system establishes a decentralized identity management framework using Hyperledger Fabric's blockchain technology. This ensures that patient identities are securely stored, authenticated, and managed across various healthcare entities, reducing the risk of data breaches and unauthorized access [9].
2. **Immutable Audit Trail:** The blockchain ledger created by Hyperledger Fabric records all transactions and access requests, establishing an immutable audit trail. This feature enhances transparency and accountability, facilitating regulatory compliance and forensic analysis in case of security incidents.
3. **Granular Access Control:** The combination of Hyperledger Fabric's permissioned network and OAuth 2.0's access control mechanisms enables fine-grained access control. It empowers healthcare institutions to grant specific levels of access to different users based on roles and responsibilities [10].
4. **Enhanced Data Privacy:** Hyperledger Fabric's privacy features and smart contracts ensure that patient data is shared only with authorized entities. This prevents unauthorized parties from accessing sensitive information, thereby enhancing patient privacy and complying with data protection regulations.
5. **Interoperability and Data Sharing:** The proposed system supports secure and controlled data sharing between healthcare providers, insurers, and other relevant stakeholders. Interoperability is achieved while maintaining data integrity and patient consent through OAuth 2.0's authorization protocols.
6. **Scalability and Performance:** Hyperledger Fabric's modular architecture allows for scalability, ensuring that the system can accommodate a growing number of users and transactions without compromising performance. This is crucial in a healthcare ecosystem with diverse entities and large volumes of data.
7. **Fraud Prevention and Security:** By leveraging blockchain's immutability and consensus mechanisms, the system reduces the risk of fraud and unauthorized access. Each transaction is validated and approved by network participants, enhancing security and trust.
8. **Regulatory Compliance:** The proposed system assists healthcare organizations in complying with regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). It provides a secure and auditable environment for managing patient data.
9. **Resilience and Reliability:** Hyperledger Fabric's distributed and fault-tolerant architecture ensures high availability and reliability. This prevents single points of failure and contributes to maintaining data integrity and system uptime.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

10. **Research Impact:** The proposed system contributes to academic and practical research by showcasing the potential of blockchain technology in solving real-world challenges in the healthcare domain. It presents a viable approach for other industries seeking to enhance their identity and access management practices.

The integration of Hyperledger Fabric and OAuth 2.0 in a blockchain-based identity and access management system presents a transformative solution for the healthcare industry. The system's contributions encompass improved security, scalability, interoperability, and compliance, laying the foundation for a more secure and efficient healthcare ecosystem.

Table 1
Comparative analysis of the proposed system with biometric authentication, zero-trust architecture, and multi-factor authentication.

Factor	Proposed Method	Biometric Authentication	Zero-Trust Architecture	Multi-Factor Authentication
Security	High	High	High	High
Usability	The use of block-chain technology ensures transparency, tamper- proof transactions, and reduces the risk of fraud and unauthorized access. Moderate Integration of OAuth2.0 and Hyperledger Fabric may require additional technical expertise and training for users.	Biometric data is unique and difficult to replicate, providing strong authentication factor. High Biometric authentication methods can be seamless and convenient for users.	Implements strong authentication mechanisms and enforces the principle of least privilege and zero trust principles. Moderate Requires a significant architectural changes and deployment complexity.	Combines multiple authentication factors to enhance security by requiring multiple credentials or factors for authentication. Moderate Requires users to provide multiple credentials or factors during authentication, which can be cumbersome for some users.
Scalability	High Hyperledger Fabric provides a modular architecture that can handle a significant number of users and transactions.	High Biometric authentication systems can scale to accommodate a large number of users and transactions.	High Zero-trust architecture can scale to accommodate growing user base.	Moderate Multi-factor authentication systems can scale to accommodate a large number of users and transactions.
Deployment Complexity	Moderate Integration of OAuth 2.0 and Hyperledger Fabric requires knowledge of block-chain and deployment considerations.	Moderate Biometric authentication may require specialized hardware or sensors, software integration, and database updates.	High Zero-trust architecture requires significant changes in the network architecture and careful implementation planning.	Moderate Integration of multiple authentication factors may require additional infrastructure and configuration, leading to increased complexity.
References		[51,52]	[53,54]	

Table 2
Comparative deduction of Size of Block-chain & Number of Entries.

Block-chain Functions	Mean values ± one standard deviation [ms]					
	N = 100	N = 500	N = 2000	N = 4000	N = 6000	N = 8000
Registration	2525 ± 73.8	2580 ± 89.4	2615 ± 58	2630 ± 61	2645 ± 61.3	2660 ± 61.7
Grant Permission	2300 ± 15.2	2315 ± 16.2	2340 ± 17.2	2380 ± 14.2	2420 ± 14.4	2460 ± 14.7
Revoke Permission	2300 ± 19.4	2325 ± 20.5	2329 ± 21.6	2375 ± 27.8	2420 ± 28.3	2465 ± 28.8
Update Data	99 ± 4.6	99 ± 4.5	102 ± 4.8	107 ± 5.9	112 ± 6.2	117 ± 6.4
Login	80 ± 5.2	83 ± 5.2	83 ± 5.7	90 ± 6.2	95 ± 6.5	100 ± 6.9
Invoke	2230 ± 16.2	2234 ± 14.2	2250 ± 12.2	2260 ± 23.3	2270 ± 23.4	2280 ± 23.5
Query	60 ± 2.3	62 ± 1.8	64 ± 2.2	65 ± 2.53	66 ± 2.6	67 ± 2.6
Block-chain size[kb]	39	115	400	780	1160	1540

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

Results

The conducted tests encompassed a thorough evaluation of diverse blockchain sizes on a local server configured in a specific manner [48]. The resultant outcomes were succinctly presented in Table 2 and visually depicted through Figures 4 and 5. In Table 2, each entry 'N' corresponds to the blockchain size. The analysis drew the inference that the augmentation of entries within the blockchain directly influences its size. Notably, the investigation revealed a direct relationship between the surge in blockchain entries and the consequential expansion of the blockchain's dimensions.Upon meticulous analysis, it was discerned that as the blockchain entries grew, a marginal increase in the time required for querying or invoking the blockchain was observed. Concurrently, activities such as system operations—registration, permission allocation, and login—also showcased a slight elongation in response times. Interestingly, with a solitary entry in the blockchain, the average query time registered at 54 ms, and the average invoke time was 2272 ms. These findings highlighted that functions such as system login and data updates exhibited response times akin to the blockchain's query intervals.Furthermore, the experiment shed light on the intrinsic correlation between invocation time and pertinent operations, including registration, permission bestowal, and permission revocation. It was evident that as the blockchain's entries proliferated, a modest temporal extension occurred in querying, invoking, and executing system functions. Notably, while the findings furnished valuable insights into the prototype's performance and usability [49,50], it is prudent to acknowledge the potential benefits of conducting future experiments on more robust hardware configurations, equipped with elevated memory resources. This prospect may provide an opportunity to explore the ramifications of larger blockchain sizes with greater precision.As the experimental data was encapsulated in Figures 4 and 5, a graphical representation of the mathematical outcomes was effectively achieved. These visualizations adeptly conveyed the linear progression of the blockchain in relation to the escalating number of entries. While the present study has been instrumental in unveiling performance trends, future endeavors could delve into scalability exploration and pinpointing potential constraints or bottlenecks.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

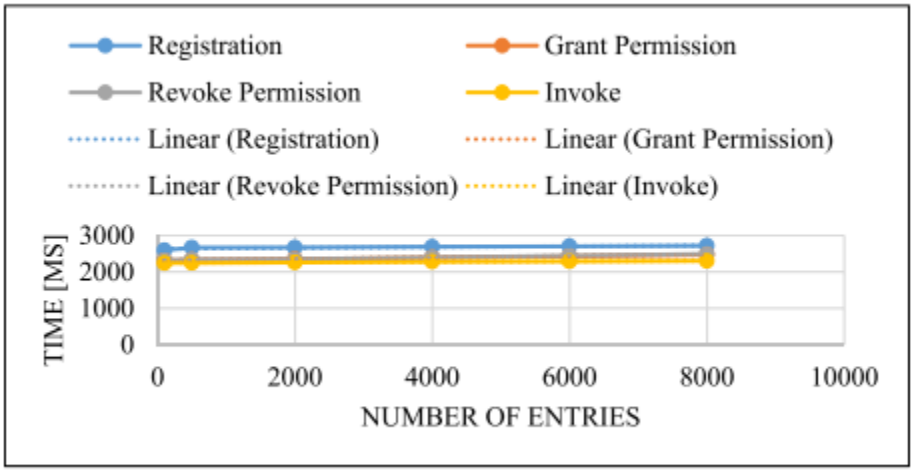

Fig. 4. Measurements of the performance of Block-chain based on Registration, Grant Permission, Revoke Permission, and Invoke.

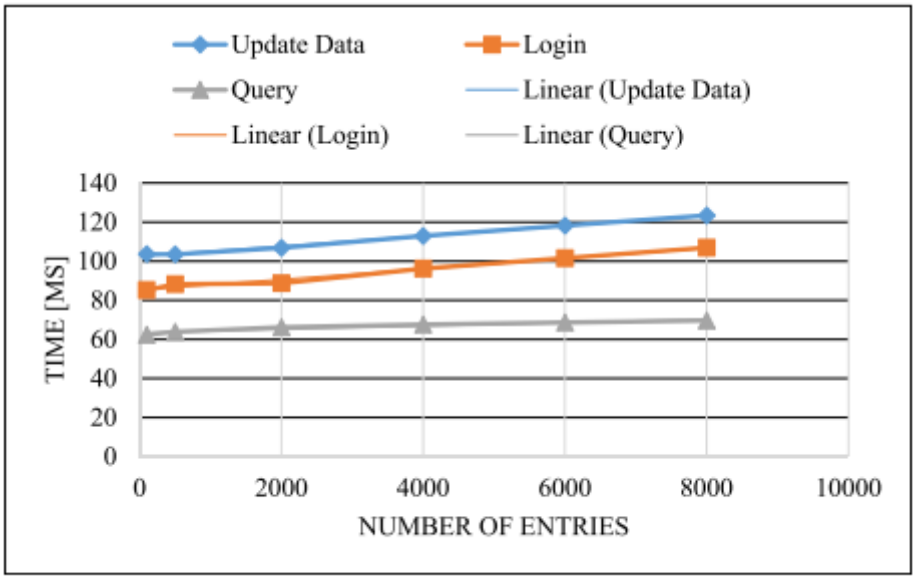

Fig. 5. Measurements of the performance of Block-chain based on Update Data, log in, and Query.

Conclusion

In summary, the presented research initiative introduces a blockchain-driven framework designed to revolutionize identity management and access control within the healthcare domain, effectively addressing the pressing challenges associated with the secure sharing of patient data. This innovative framework provides a robust and meticulous access control solution for the handling of sensitive patient information, capitalizing on the intrinsic benefits of blockchain technology, including decentralization, immutability, and transparency.By skillfully integrating OAuth 2.0 and Hyperledger Fabric, the framework establishes a scalable and impregnable approach to managing user access within the Fabric

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

network. This integration ensures that data accessibility is confined solely to authorized applications, further cementing security measures. The algorithm proposed for crafting a secure and decentralized identity and access management system, anchored by OAuth 2.0 and Hyperledger Fabric, furnishes a comprehensive blueprint outlining the sequential steps required for successful framework implementation.The algorithm's standout features include the segregation of authentication and authorization processes, the employment of trusted authentication providers, and the issuance of access tokens to vetted applications through the OAuth 2.0 authorization server. This amalgamation of traits renders the proposed algorithm a secure and scalable resolution for effectively overseeing access to sensitive information. Moreover, the framework's tamper-resistant audit trail augments security measures by promptly detecting unauthorized access or any tampering attempts.In essence, the amalgamation of cutting-edge technologies and innovative algorithms not only bolsters patient data security but also fuels a paradigm shift in healthcare operations. The proposed framework is poised to usher in a new era of patient data control and accessibility, underpinned by enhanced security and the assurance of data integrity.

Refernces

[1] J. Garay, A. Kiayias, N. Leonardos, April). The bitcoin backbone protocol: analysis and applications, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015, pp. 281–310.

[2] A. Ouaddah, H. Mousannif, A. Abou Elkalam, A.A. Ouahman, Access control in the Internet of Things: big challenges and new opportunities, Comput. Network. 112 (2017) 237–262.

[3] 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.

[4] S.C. Cha, T.Y. Hsu, Y. Xiang, K.H. Yeh, Privacy enhancing technologies in the internet of things: perspectives and challenges, IEEE Internet Things J. 6 (2) (2018) 2159–2187.

[5] I. Indu, P.R. Anand, V. Bhaskar, Identity and access management in cloud environment: mechanisms and challenges, Engineering science and technology, an international journal 21 (4) (2018) 574–588.

[6] X. Zhu, Y. Badr, Identity management systems for the internet of things: a survey towards blockchain solutions, Sensors 18 (12) (2018) 4215.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 10, Spl Iss 2, 2021

[7] W.L. Sim, H.N. Chua, M. Tahir, Blockchain for identity management: the implications to personal data protection, in: 2019 IEEE Conference on Application, Information and Network Security (AINS),

[8] R. Bose, S. Chakraborty, S. Roy, Explaining the workings principle of cloud-based multi-factor authentication architecture on banking sectors, in: Amity International Conference on Artificial Intelligence (AICAI), IEEE, 2019, February, pp. 764–768, 2019.

[9] P.J. Taylor, T. Dargahi, A. Dehghantanha, R.M. Parizi, K.K.R. Choo, A systematic literature review of blockchain cyber security, Digital Communications and Networks 6 (2) (2020) 147–156.

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