hChain 4.0: A Permissioned Blockchain Framework for Secure, Privacy-Preserving, and Scalable EHR Management

Musharraf N. Alruwaill
Dept. of Computer Science and Engineering
University of North Texas
Denton, USA
MusharrafAlruwaill@my.unt.edu

Saraju P. Mohanty
Dept. of Computer Science and Engineering
University of North Texas
Denton, USA
saraju.mohanty@unt.edu

Elias Kougianos
Dept. of Electrical Engineering
University of North Texas
Denton, USA
elias.kougianos@unt.edu

***Abstract*—The growing utilization of IoMT devices, including smartwatches and wearable medical devices, has facilitated real-time health monitoring and data analysis to enhance healthcare outcomes. These gadgets necessitate improved security measures to safeguard sensitive health data while tackling scalability issues in real-time settings. The proposed system, hChain 4.0, employs a permissioned blockchain to provide a secure and scalable data infrastructure designed to fulfill these needs. In contrast to conventional systems susceptible to security flaws or public blockchains constrained by scalability and expense. The proposed approach hChain 4.0 introduce a high-privacy method which health data is encrypted utilizing the Advanced Encryption Standard (AES) for time effective encryption. Moreover, it utilizes private channels enable isolated communication and ledger between stakeholders which ensure robust privacy while supporting collabrative operations. The proposed framework enables anonymized health data sharing for medical research by pseudonymize patient identity. Additionally, hChain 4.0 incorporates role-based access control (RBAC) to provide secure electronic health record (EHR) sharing among authorized parties. Experimental assessments indicate that the proposed approach achieves higher scalability, cost-effectiveness, and validated security.**

***Index Terms*—Smart Healthcare, Blockchain, Internet of Medical Things, Electronic Health Record, Smart Contract, Healthcare Cyber-Physical Systems.**

I. Introduction

The rapid advancement of smart healthcare technologies, has led to a significant increase in the use of devices such as smartwatches and wearable medical devices. These devices are beneficial for patient health monitoring, data analysis, aiding in the prediction and prevention of health risks [1]. However, these devices have limited capabilities and low computational power, thus they are more vulnerable to security issues [2]. Moreover, traditional healthcare systems use centralized infrastructure for EHR management and storage, which required enhanced security while handling sensitive information regarding a patient's health. Furthermore, traditional systems are inefficient in handling the lengthy processes of data transfer and EHR management [3].

Transitioning from centralized to decentralized data infrastructures addresses the limitations of data availability and reliability, as well as security in a centralized manner, toward patient-centric healthcare as presented at Figure 1. Blockchain, as a distributed ledger technology, ensures data security with its robust security mechanisms. Smart contract is self-executing code that enables secure agreements and automates processes between parties. Blockchain and smart contracts enhances the security and reliability of EHR management while reducing human intervention by automatized operations [4]. Blockchain and Smart Contract: A Transformational Approach to address Traditional Health Challenges. The proposed permissioned blockchain framework

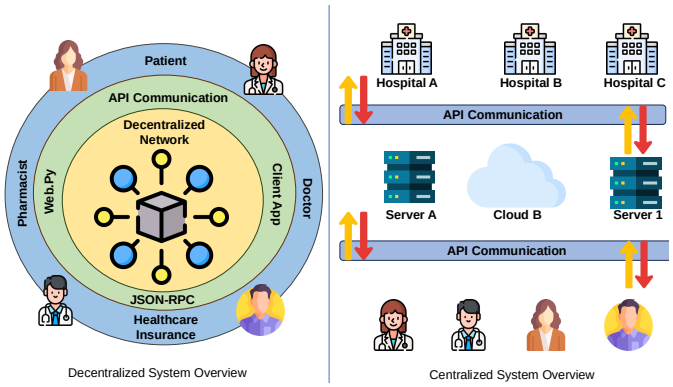

Fig. 1. Centralized And Decentralized System Overview.

utilizes blockchain for EHR and participant management, employing smart contracts to facilitate automated interactions between entities securely. The proposed approach, hChain 4.0, employs RBAC for enabling secure sharing of EHRs to all authorized participants within the network via a smart contract, fully controlled by the patient. Due the sensitive nature of patient data, a permissioned blockchain is utilized to facilitate restricted access strictly for authorized stakeholders, hence assuring enhanced privacy and security in contrast to a public blockchain, which enables potential access by any individual.

In addition to permissioned blockchain security and privacy, hChain 4.0 employs AES encryption to provide another level

of privacy for participants. Moreover, public blockchains are associated with higher fees and scalability limitations, whereas hChain 4.0 provides higher scalability and feeless. Additionally, channels are utilized to enhance privacy among participating entities by ensuring data confidentiality and isolation from other participants, enabling more efficient data management.

The rest of this paper is organized as follows. The novel contributions of the proposed hChain 4.0 framework are presented in Section II. Related prior research is discussed in Section III. A detailed architectural overview of hChain 4.0 is provided in Section IV. The proposed algorithms for hChain 4.0 are explained in Section IV-A. Experimental results validating the system are presented in Section V, and finally, the conclusion and future research directions are discussed in Section VI.

II. Novel Contributions

This section outlines the challenges addressed by hChain 4.0 and its innovative contributions in enhancing permissioned blockchain EHR management, focusing on improved privacy, scalability, and reliability.

A. Problems Addressed

- **Limitations of Centralized Systems:** Centralized systems are prone to single points of failure and lack robustness in terms of data availability and reliability.
- **Inefficient Data Ownership and Transfer:** Effective data ownership is critical in smart healthcare to prevent delays caused by lengthy data transfer processes.
- **Security Challenges in IoMT Devices:** IoMT devices face security vulnerabilities due to their limited computational and storage capabilities.
- **Scalability and Privacy Concerns in Public Blockchains:** Public blockchains encounter scalability and privacy challenges inherent to their consensus mechanisms.
- **High Costs:** Public blockchains incur significant transaction costs, making them less practical for large-scale applications.
- **Latency Issues:** Public blockchains experience delays in transaction processing due to the computational overhead of consensus algorithms.
- **Access Control Limitations:** Traditional systems face difficulties in managing access control as data is siloed across different stakeholders, limiting collaboration.
- **Challenges in Collaborative Research:** Ensuring data integrity is essential for collaborative research. However, traditional systems struggle to provide reliable mechanisms for data sharing and validation.

B. Novelty of the Proposed Solution hChain 4.0

- **Permissioned Blockchain for EHR Management:** Leverages a permissioned blockchain to enhance scalability within the system.
- **Advanced Encryption with AES:** Integrates AES encryption to provide an additional layer of privacy and security across the network.
- **Private Blockchain Channels:** Utilizes channels to facilitate isolated communication and collaboration among stakeholders, ensuring data confidentiality and effective management.
- **Role-Based Access Control (RBAC):** Employs RBAC via smart contracts to enable secure access to EHRs, granting patients greater control over data sharing.
- **Smart Contract Automation:** Implements smart contracts to streamline stakeholder interactions, minimize manual intervention, and ensure secure data handling.
- **Cost Efficiency:** Reduces the high costs associated with public blockchains, thereby enhancing overall cost-effectiveness.
- **Anonymized Data Sharing:** Supports the anonymized sharing of EHRs for medical research, protecting patient identities.
- **Patient-Centric Approach:** Promotes patient-centricity by avoiding lengthy data transfer processes and allowing patients full control over their data.
- **Interoperability:** Ensures that all authorized stakeholders within the network can access necessary data, effectively addressing interoperability challenges.

III. Related Prior Research

Various approaches have been implemented in the healthcare sector to enhance traditional centralized EHR management, focusing on optimizing efficiency, strengthening security, and implementing robust access control mechanisms [5]–[9]. In additon, many studies presented decentrealized and scalable EHR management cloud-based approaches to address the security and access control management issues in centralized system. Table I illustrates the features and technical comparison of state-of-the-art works and the proposed approach. Table II presents the scalability optimization, cost efficiency, and technical blockchain type comparisons between prior studies and hChain 4.0.

In [10], a private permissioned system emphasizes basic role-based methods for sharing EHRs, while [11] adopts a patient-centric Ethereum framework that leverages IPFS for off-chain storage. Another study, [12], showcases a cloud-based architecture that uses steganography-driven encryption and compares throughput against existing blockchain solutions. Meanwhile, [14] integrates Ethereum with IPFS and employs an attribute-based access control mechanism to fine-tune permission settings, whereas [13] applies Hyperledger Fabric with PBFT consensus to enhance performance and lower latency without detailing private channels.

In [15], a public blockchain is proposed that employs location-based authentication to enhance security, while [16] expands upon this by integrating IPFS off-chain storage to optimize scalability and cost-efficiency, and utilizes Long Short-Term Memory (LSTM) for fall detection to mitigate

TABLE I
COMPARATIVE TABLE FOR STATE-OF-THE-ART WORKS

Parameter	[10]	[11]	[12]	[13]	[14]	hChain 4.0 (Proposed)
1. Blockchain Type	**Private**	**Permissioned Infrastructure**	**Cloud-Based**	**Permissioned**	**Public**	**Permissioned**
2. Encryption Scheme	AES-256	Session Keys for Viewing (IPFS)	AES-128 + Steganography	NA	AES-128	AES-256
3. Isolation / Private Channels	✗	✗	✗	✗	✗	Secured Channels (Data Segmentation)
4. Access Control Management	RBAC	RBAC	Cloud Access Module	NA	ABAC	RBAC
5. ID Eliminated for Researchers	✗	✗	✗	✗	✗	Pseudonymization (**Patient IDs removed**)
6. Scalability	Moderate	Moderate	High	High	Moderate	High
7. Transaction / Operational Cost	Moderate	Moderate	Moderate	Low	Moderate	Low

health risks. In [17], the integration of blockchain with cloud-based EHR management is proposed to enhance scalability by storing the entire EHR in the cloud while the hash value remains stored on the blockchain. It employs RBAC with multi-layer authentication and authorization using smart contracts and cloud.

However, hChain 4.0 implements a permissioned blockchain architecture with the Raft consensus mechanism, thereby enhancing throughput, scalability, and cost efficiency. It employs AES-256 encryption to minimize encryption time while multiple chaincodes for omits patient identifiers to facilitate medical research under robust data privacy constraints and for encrypted EHR management. Furthermore, secure channels and separate ledgers across participating organizations reinforce confidentiality by isolating sensitive EHR operations among diverse stakeholders.

TABLE II
COMPARATIVE TABLE FOR HCHAIN RESEARCH

Parameter	hChain [15]	hChain 2.0 [16]	hChain 3.0 [17]	hChain 4.0
Blockchain Type	Public	Public	Public	Permissioned
Encryption Scheme	Symmetric	Asymmetric	Symmetric	Symmetric
Isolation & Anonymization	✗	✗	✗,	Proposed
Scalability	Low	Moderate	Moderate	Highest
Cost	High	Moderate	Moderate	Low

IV. ARCHITECTURAL OVERVIEW OF HCHAIN 4.0

The hChain 4 architecture comprises three primary layers as depicted in Figure 2, each performing a distinct function to ensure secure, reliable, and efficient data management. The first layer, referred to as the sensing layer, continuously gathers real-time data from wearable devices and forwards these data to the edge layer.

Within the sensing layer, smart devices such as wearables generate physiological data in real time. Each device connects to an edge device (e.g., a smartphone), which holds the necessary credentials and configuration details to interact with the blockchain network. Since these sensing devices typically possess limited computational and security capabilities, the data they produce are initially vulnerable. Consequently, the edge layer ensures the confidentiality of these data by applying AES-256 encryption, thus enhancing data privacy in local environments. It also standardizes the data format to facilitate advanced analytics. Once these processes are complete, the edge layer submits the resultant encrypted data to the blockchain network through a dedicated client application.

The client application serves as a communication bridge between the edge layer and the blockchain, submitting transactional proposals and awaiting endorsements from designated peers. Upon receiving sufficient endorsements, the blockchain commits the transactions to its distributed ledger. At the blockchain layer, multiple organizations maintain a shared public ledger while retaining operational independence. Moreover, It establishes separate ledgers and multiple chaincodes are doployed for specialized collaboration. A dedicated research organization is additionally instituted to enable the secure exchange of EHRs with patient identifiers removed, alleviating the need for any extra actions on the part of the patients. The second chaincode utilizes for encrypted EHR management. In addition to real-time data management, the chaincode are able to maintain the patient history and ciritical operation management with multiple signature approval from different stakeholder to ensure different stakeholder such as healthcare providers to approve the operation before comitted and considered to be approved. LevelDB is employed for optimizating and fast read and write operation and query simiplizity and provide a simple data structure.

The Raft consensus algorithm is employed to optimize network scalability. Moreover, a transaction is deemed approved only after receiving endorsements from multiple peers across different organizations, thereby ensuring robust validation within the network. To optimize performance, LevelDB is utilized, enabling rapid read and write operations, simplified query mechanisms, and a streamlined data structure for efficient storage and usage.

A. Proposed Algorithms for hChain 4.0

Algorithm 1 describes the complete hChain 4.0 data flow, from the generation of sensor-derived data to the commitment or rejection of transactions within the blockchain network. In the initial phase, IoMT devices sense data and transmit it in plain text to an edge device. The edge device then preprocesses, reformats, and encrypts the data, forwarding

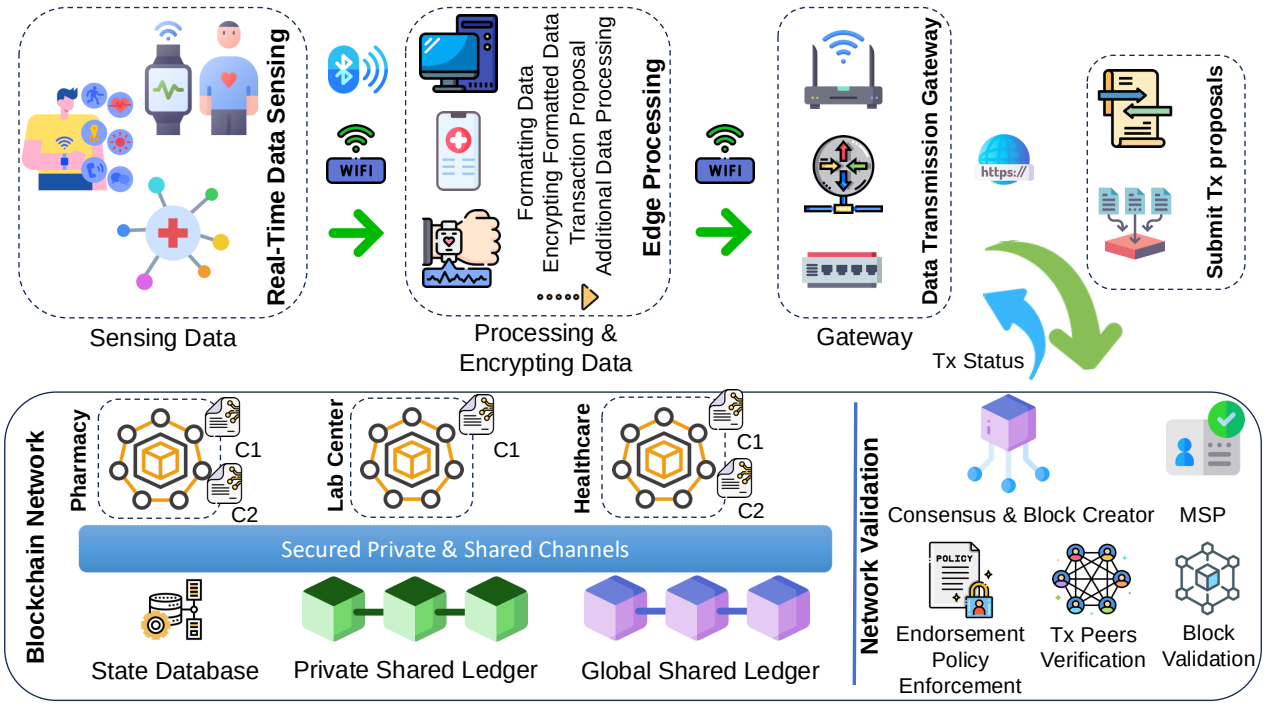

Fig. 2. hChain 4.0 Framework Architecture.

it to the blockchain network through a client application. Subsequently, the client application constructs a transaction proposal, which is evaluated by endorsing peers from multiple organizations to verify transaction validity. If the transaction is approved, it is committed to the blockchain; otherwise, it is rejected.

V. Implementation And Validation

A. Implementation

Hyperledger fabric 2.5 is utilized as permssioned blockchain and Caliper for testing the network performance. In addition, python and javascript is used to make a test code and interact with up network. The deployment and test are performed uses Mac OS Monterey with 2.2 GHz Quad-Core Intel Core i7 processor and 16 GB 1600 MHz DDR3 memory. Chaincode is written in the Go programming language, as Hyperledger Fabric supports Go for chaincode development.

B. Validation

1) Time Analysis And Cost Analysis: The Ethereum public blockchain utilized in hChain, hChain 2.0, and Chain 3.0 presents latency concerns and is less scalable compared to permissioned blockchains. The estimated transaction rate for the Ethereum blockchain is approximately 25 transactions per second (TPS) [18]. During the testing instance utilizing a caliper, it demonstrated 717 TPS, which is an increase of 28 times. Furthermore, hChain 4.0 shows improved cost efficiency than [15]–[17].

2) Data Privacy: hChain 4.0 introduces a multi-layered privacy framework by encrypting sensitive data locally before committing it to the distributed ledger under distinct identities, thereby avoiding plaintext exposure on-chain. Unlike a conventional public blockchain—where all transactions reside on a single ledger—each organization in hChain 4.0 maintains a secure, isolated environment that supports selective collaboration and communication, thereby upholding stricter confidentiality requirements across orgnizations boundaries. In addition, the patient identity is eliminated when it is shared with research centers to ensure higher privacy for clients and make it easier for research medical centers to access the data within the network.

3) Data Security And Access Control Management: The proposed approach enhances data security by leveraging a blockchain-based framework in conjunction with contemporary encryption algorithms, thereby preserving confidentiality even in untrusted environments. Moreover, transactional integrity is achieved by requiring endorsement from peers across multiple organizations, ensuring that each operation is independently validated before being recorded on the ledger. This collaborative endorsement process mitigates the risk of fraudulent submissions and strengthens trust in the overall system integrity. The proposed solution employs a RBAC framework to govern health-record access, thereby ensuring that patients retain oversight of their data. By mapping specific user roles to well-defined privileges, the system strictly limits the ability to view, modify, or share sensitive medical information to authorized individuals,

Algorithm 1 hChain 4: Data Flow from Sensing to Blockchain Storage

Require:
- IoMT Device
- Edge device
- Valid Account

Ensure:
- Transaction approval by multiple organizations

Sensing Layer
IoMT device senses and transmit real-time data to the edge device.
Edge Layer
Format data.
Encrypt data with AES-256.
Send encrypted data using the client application.
Client Application
Form a transaction proposal containing encrypted data, metadata, and signatures.
Blockchain Layer
Endorsing peers validate the proposal.
if Valid **then**
    Peers in different organizations endorse the transaction.
    Ordering service sequences transactions.
    Commit transaction to the ledger.
else
    Reject the transaction.
end if

reinforcing both security and patient-centric governance.

VI. Conclusion and Future Research

The proposed framework hChain 4.0 employs a permissioned blockchain for EHR management, ensuring security across all tiers. Furthermore, it provides elevated privacy by maintaining ledger and communication isolation from other network communications via multiple of secured channels. Furthermore, it provides significantly enhanced scalability with 717 TPS in testing environment, rendering it more appropriate for real-time applications. The cost efficiency is addressed in the proposed method by utilizing permissioned blockchain to eliminate public blockchain gas costs.

Future research indicates that ABAC improves access control management in the healthcare sector, rendering it more suitable for complex organizations and enhancing flexibility. Furthermore, implementing an interface to enhance usability for the end-user. Moreover, managing and handling large data within the network for high-volume data.

References

[1] M. Masoumian Hosseini, S. T. Masoumian Hosseini, K. Qayumi, S. Hosseinzadeh, and S. S. Sajadi Tabar, "Smartwatches in healthcare medicine: assistance and monitoring; a scoping review," *BMC Medical Informatics and Decision Making*, vol. 23, no. 1, p. 248, Nov 2023. [Online]. Available: https://doi.org/10.1186/s12911-023-02350-w

[2] S. F. Ahmed, M. S. B. Alam, S. Afrin, S. J. Rafa, N. Rafa, and A. H. Gandomi, "Insights into internet of medical things (iomt): Data fusion, security issues and potential solutions," *Information Fusion*, vol. 102, p. 102060, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1566253523003767

[3] J. Carlos Ferreira, L. B. Elvas, R. Correia, and M. Mascarenhas, "Enhancing ehr interoperability and security through distributed ledger technology: A review," *Healthcare*, vol. 12, no. 19, 2024. [Online]. Available: https://www.mdpi.com/2227-9032/12/19/1967

[4] M. Y. Jabarulla and H.-N. Lee, "A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the covid-19 pandemic: Opportunities and applications," *Healthcare*, vol. 9, no. 8, 2021. [Online]. Available: https://www.mdpi.com/2227-9032/9/8/1019

[5] K. Pradeep Kumar, B. R. Prathap, M. M. Thiruthuvanathan, H. Murthy, and V. Jha Pillai, "Secure approach to sharing digitized medical data in a cloud environment," *Data Science and Management*, vol. 7, no. 2, pp. 108–118, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666764923000589

[6] D. B. Srinivas, D. K. M, R. H. P, and L. H, "Securing sharable electronic health records on cloud storage," in *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*, 2023, pp. 1054–1059.

[7] T.-Y. Ou and W.-L. Tsai, "Designing a flow-based mechanism for accessing electronic health records on a cloud environment," *Journal of Web Engineering*, vol. 21, no. 5, pp. 1491–1517, 2022.

[8] V. Chakka, D. Pavuluri, K. K. R. Sagili, S. Akkaladevi, S. Bhaskar, S. Patil, and K. Parmar, "Efficient public data auditing scheme for healthcare systems using ecc-based attribute-based signature in cloud storage," in *2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2023, pp. 171–176.

[9] S. N. Turhan, "Leveraging graph databases for enhanced healthcare data management: A performance comparison study," in *2023 IEEE International Conference on Big Data (BigData)*, 2023, pp. 5007–5013.

[10] R. Ghugare, S. W. Rathod, A. Joshi, and P. V. Patil, "Decentralizing health: The role of private blockchain in secure and patient-oriented ehr management," in *2024 2nd International Conference on Computer, Communication and Control (IC4)*, 2024, pp. 1–6.

[11] 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," *Applied Sciences*, vol. 13, no. 3, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/3/1761

[12] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha, and M. Shukla, "Prms: Design and development of patients' e-healthcare records management system for privacy preservation in third party cloud platforms," *IEEE Access*, vol. 10, pp. 85 777–85 791, 2022.

[13] M. Katoch, K. Devi, A. Sharma, P. K. Angra, P. Singh, and A. Kumar, "Enhancing the security of e-healthcare transactions using hyperledger fabric modular blockchain framework," in *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, vol. 6, 2023, pp. 1344–1348.

[14] N. Kumar Pandit, S. Das, and C. Kumar Panda, "A patient-centric ehr management system using ethereum blockchain," in *2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS)*, 2024, pp. 1–5.

[15] M. N. Alruwaill, S. P. Mohanty, and E. Kougianos, "hchain: Blockchain based healthcare data sharing with enhanced security and privacy location-based-authentication," in *Proceedings of the Great Lakes Symposium on VLSI 2023*, ser. GLSVLSI '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 97–102. [Online]. Available: https://doi.org/10.1145/3583781.3590255

[16] M. Alruwaill, S. P. Mohanty, and E. Kougianos, "hchain 2.0: Leveraging blockchain and distributed file system for ehr management in smart healthcare," Springer Nature Computer Science.

[17] M. N. Alruwaill, S. P. Mohanty, and E. Kougianos, "hChain 3.0: Leveraging Blockchain for Personalized Patient Assessments and Improved Medication Adherence in Chronic Care Management," in *2024 OITS International Conference on Information Technology (OCIT)*, 2024.

[18] S. Bhujel and Y. Rahulamathavan, "A survey: Security, transparency, and scalability issues of nft's and its marketplaces," *Sensors*, vol. 22, no. 22, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/22/8833