hChain 3.0: Leveraging Blockchain for Personalized Patient Assessments and Improved Medication Adherence in Chronic Care Management

Musharraf N. Alruwaill*, Saraju P. Mohanty*, Elias Kougianos†
* Department of Computer Science and Engineering, University of North Texas, USA
† Department of Electrical Engineering, University of North Texas, USA
Email: MusharrafAlruwaill@my.unt.edu, saraju.mohanty@unt.edu, elias.kougianos@unt.edu

***Abstract*—Chronic disease patients require ongoing observation, even if not physically in healthcare facilities. Each patient, even with the same condition, may have a unique health profile, necessitating personalized assessments for accurate and effective care. Emerging technology such as the Internet of Medical Things (IoMT) could help with remote patient real-time monitoring, utilizing a deep learning model for personalized patient assessment to enhance patient quality of life and support healthcare provider decision-making. However, IoMT devices are resource-constrained, which makes them vulnerable to several attacks that could provide false data, raising life-threatening risks to the patient. To address these issues, the proposed hChain 3.0 system leverages blockchain technology to overcome IoMT vulnerabilities and the limitations of centralized healthcare systems, such as single points of failure (SPoF). It provides a decentralized, secure data infrastructure to ensure data integrity and immutability. In addition, smart contracts enable secure electronic healthcare records (EHR) management and automates manual processes, while cloud computing is utilized to enhance the framework's scalability. Moreover, it presents effective detection of heart rhythm abnormalities in electrocardiogram (ECG) signals via an accurate Long Short-Term Memory (LSTM) model.**

***Index terms*—** Smart Healthcare, Blockchain, Smart Contract, Healthcare Cyber-Physical Systems.

I. Introduction

Smart healthcare employs technologies such as the Internet of Medical Things (IoMT), artificial intelligence (AI), data analytics, and real-time monitoring systems [1]. These technologies optimize data use across multiple locations, improving efficiency, patient-centricity, and quality of life.

Traditional healthcare systems face challenges such as data fragmentation [2], restricted access, and incomplete patient documentation. Additionally, there is restricted accessibility to healthcare data and the ownership of this data lies with the facilities rather than the patients [3]. Furthermore, existing research tends to focus on security, yet often lacks scalability, involves complex designs, is difficult to integrate with existing systems, or proves costly.

Traditional healthcare also struggles with IoMT integration [4], as limited device capabilities compromise data protection. In context of healthcare, blockchain addresses these issues by creating a unified, decentralized ledger that securely stores patient data, ensuring complete, consistent, real-time access for authorized stakeholders. Smart contracts automate processes like patient consent, access control, and data sharing, enabling secure, transparent transactions without intermediaries. This reduces inefficiencies, enhances privacy, and ensures timely access to EHRs.

Blockchain shifts data ownership from facilities to patients, resolving delays in EHR transfer [5]. The proposed framework integrates blockchain, smart contracts, and cloud computing to provide secure EHR management, real-time patient monitoring, and data sharing, supported by multi-tier authentication, encryption, and anomaly detection in ECG signals using LSTM models, as shown in Figure 1.

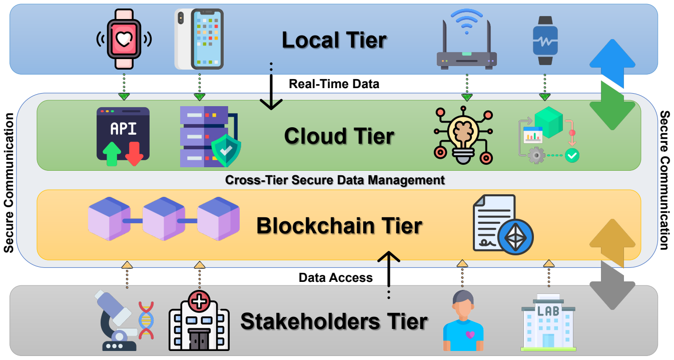


Fig. 1: System Overview.

The structure of this paper is as follows: Section II outlines the novel contributions of the proposed framework. In Section III presents the existing works on EHR management. Section IV describes the components of the proposed framework. Section V outlines the architecture of the proposed system. Section VI discusses the experimental results of the system. Finally, Section VII concludes the proposed framework and suggests future research directions.

II. Novel Contributions

A. Problem

Current healthcare systems suffer difficulties in maintaining data privacy and enabling secure and effective real-time monitoring for chronic care management, particularly in terms of data integrity and reliability. Moreover, because the respective facilities own these records, the process of transferring EHRs between healthcare centers is lengthy. Delivering care for patients with chronic diseases necessitates a system of utmost reliability and precise data to align the doctor's decision-making with the patient's health condition. Furthermore, the implementation of a secure automation system is essential to accelerate the processing of patient EHR data and ensure its integrity and authenticity. However, centralized systems encounter numerous obstacles and risks when implementing these developing technologies and relying on the associated data. These include single points of failure, vulnerabilities in centralized databases, the possibility of data breaches, a lack of transparency, and limited access to data. Moreover, it faces challenges in collecting longitudinal data in a secure manner, which makes it difficult to put together a complete medical record for patients. The dispersion of their medical records among various healthcare providers results in inefficient decision-making.

B. The Novelty of the Proposed Solution

Our proposed solution offers several novel contributions to address the challenges in chronic care management:

- **Integration of IoMT and Blockchain**: It uses blockchain and cloud computing to improve scalability, security, and efficient data management.
- **Smart Contract for Automation System**: Employing smart contracts to automate procedures and agreements in a secure manner.
- **Enhanced Privacy and Transparency**: The health data is securely stored in an encrypted and hashed format on the blockchain, enabling both privacy and transparency.
- **Ensuring Avaliability, Integrity and Security**: The public blockchain provides availability, integrity, and security through its mechanisms.
- **Effecenit Access Control Management**: It employs a multi-layered approach to access control management, utilizing smart contract and cloud-based authentication and authorization.
- **Abnormalities In Heart Rhythm And Notification System And Risk Mitigation**: The LSTM model is utilized to detect anomalies and notify and transmit EHR to the nearest emergency room for assistance for mitigating the risk of chronic diseases.
- **Personalized assessment And Medication**: The system utilizes an automation threshold to assess the patient's health status and adjust the drug dosage accordingly, taking into account the patient's progress.
- **Easier Adoption**: It facilitates adoption by integrating cloud technology and delivering a secure Application Programming Interface (API) for system access, hence simplifying its adoption and usage within the existing framework.

III. Related Work

Several prior studies have examined the methodology by which data infrastructure adopts a decentralized structure rather than centralized systems [6]–[8]. The proposed system [9] utilizes blockchain to store all health data and manage EHR using smart contracts, resulting in significantly increased costs. The proposed framework [10] integrates several technologies, including blockchain, IoMT, and peer-to-peer networks, to securely manage EHRs. Furthermore, deep learning is employed for emergency response in situations where the patient has a fall. However, proposed solutions [9], [10] do not provide a personalized patient assessments and have limited scalability. The author proposed a framework based on blockchain technology to enhance the management of EHR in healthcare facilities across India. The use of blockchain technology improves the management of data, ensures privacy, and facilitates the secure exchange of EHRs among various stakeholders while it lacks automation processes and personalized assessments [11]. In their proposal, [12] suggests the implementation of a permissioned blockchain to protect healthcare data and enable secure access control. The system utilizes the Hyperledger Fabric platform and Chaincode to augment confidentiality and uphold the accuracy of data. The author [13] suggested the utilization of a NEM public blockchain and cloud framework to ensure the precision and reliability of data during the training of machine learning models. Additionally, this framework safeguards privacy by filtering out personal information. It enables the prevention of emerging diseases while preserving individuals' privacy. The Innovation Key Management Protocol A blockchain-based solution is suggested in [14] to ensure the security of Personal Healthcare Records (PHRs) and improve privacy. Additionally, it offers a secure method of sharing data through the use of cryptographic algorithms, which are used to encrypt and decrypt PHRs while maintaining confidentiality. However, the proposed solutions [12]–[14] do not include robust smart contract functionalities for EHR management and dynamic assessment in real-time.

The system proposed in [15] heavily relies on smart contracts to analyze encrypted health data in real-time and determine whether a patient requires an immediate emergency response or not. Furthermore, threshold predicate encryption (TPE) preserves patient privacy and security by preventing the exposure of patient health data in plain text during health data reading. The author [16] suggests the integration of Aadhaar-based authentication and blockchain technology. The proposed system uses Aadhaar, a unique identification system in India, to authenticate patients and ensure their uniqueness. Furthermore, it improves the overall security of the system by leveraging blockchain technology to ensure transparency, immutability, and streamline insurance claims. However, the scope of the proposed solutions [15], [16] is limited, as EHR process automation, robust smart contracts for EHR management, and dynamic real-time care monitoring are not sufficiently addressed.

TABLE I: Comparison of Related Works

Works	**Data Storage Tech**	**Auto Process**	**Smart Contract**	**Access Control Management (ACM)**	**Personalized Patient Assessment**	**Scalability**	**Cost**	**Dynamic Medication Adherence & Monitoring**
Pandey et al. 2023 [11]	Permissioned Blockchain	No	Few	RBAC	No	Moderate	Low	No
Sheeraz et al. 2023 [12]	Permissioned Blockchain and IPFS	No	Very Few	RBAC	No	Moderate	Low	No
Haddad et al. 2021 [13]	Blockchain and Cloud	No	Not specified	Grant-Based	No	High	Low	No
Zhu and Chen. 2021 [14]	Blockchain and Off-Chain	No	No	Encryption Key Management	No	High	Low	No
Panda et al. 2022 [15]	Private Blockchain Hyperledger Fabric	Few Automation Process	Monitoring and emergency detection	Condition-Based Access Control	Yes	Moderate	Low	Real-Time Phycological Parameter Monitoring
Haidar and Kumar. 2021 [16]	Blockchain	No	Not specified	Aadhaar-Based	No	Moderate	Not specified	Not personalized
Alruwaill, et al. [9] (hChain)	Blockchain	Yes	Yes	Several ACM Types	No	Low	High	No
Alruwaill, et al. [10] (hChain 2.0)	Blockchain and IPFS	Yes	Yes	Smart Contract	No	Moderate	Low	Real-time monitoring
The Proposed System (hChain 3.0)	Blockchain and Cloud	Yes	Multiple functionalities and Services	Smart Contract and Multi-layers of ACM	Yes	High	Low	Personalized and real-time monitoring

IV. Proposed System Methodology

A. Framework Components

The proposed system involves various technologies, which will be discussed in the subsequent subsections.

1) Blockchain Technology: Blockchain technology is an essential component of the proposed system. It utilizes Ethereum due to its well-established, supporting smart contract and widespread adoption.

2) Smart Contract: A smart contract is a self-executing software that automates the process of an agreement between parties in a secure manner, based on specified conditions. Smart contracts are utilized to automate the agreement process, in addition to storing the hash value of EHRs and sharing data through various access control methods [6].

3) Cloud Computing: The cloud is utilized to enhance the scalability of the proposed system, reduce costs, and facilitate the adoption of the system for traditional systems. Furthermore, it serves the purpose of enabling data sharing, facilitating communication between stakeholders and cloud software through an API, offering notification services, implementing an extra layer of authentication and authorization, and ensuring data backup in various locations.

4) Long-Short-Term Memory Model: LSTM is a type of recurrent neural network (RNN) that is particularly effective at capturing and understanding long-term relationships in sequential data. Its ability to evaluate temporal patterns makes it well-suited for detecting heart rhythm anomalies in ECG readings.

B. The Architecture

The proposed system was developed using several technologies, such as blockchain, cloud computing, and IoMT, which work together to assure the security of real-time data management, as shown in Figure 2 . Blockchain is utilized for assuring the secure and permanent storage of data while maintaining its integrity, availability, and transparency. Smart contracts are applied for the objective of automation, while cloud technology is used to enable the adoption of the traditional healthcare system. The system can be divided into four primary layers, as shown in Figure 2. The first layer is the generation layer, which utilizes IoMT to acquire and transmit data to the nearby edge device. An edge device is utilized to strengthen data security and address the limits of IoMT. The edge device promptly obtains the data and encrypts it using the appropriate key. It then transmits the encrypted data through a secure channel to the cloud. The data is then hashed using the SHA-256 algorithm, which is an advanced way of creating a unique identifier. Finally, the data is published in the blockchain associated with the patient's account. The second layer is the cloud, which provides an infrastructure for delivering system notifications to promptly inform the stakeholders and caregivers involved with the patient about any potential risks in real-time. Furthermore, it offers a secured database and backup service to guarantee the permanent existence of data when it is required. Furthermore, it possesses an API that enables communication with stakeholders, streamlining system adoption, and enhancing system scalability. Furthermore, it utilizes an LSTM model for identifying irregularities in heart rhythm and software for managing and organizing incoming data. Furthermore, it employs additional security measures by undergoing authorization and authentication processes when communicating with the cloud, thereby guaranteeing the validity and confidentiality of the data. The blockchain and smart contract technology is the third layer, establishing a secure and immutable record system, as well as a robust automated agreement mechanism among the participants in the blockchain network. Smart contracts enable secure data transfer with Role-Based Access Control (RBAC) and efficient management of different access controls. Furthermore, it allows for emergency data exchange in situations where there is a risk to the patient and an inability to perform data sharing. The fourth tier consists of stakeholders, such as research centers, laboratory centers, and healthcare providers. They possess the capability to securely communicate and access patient data by undergoing several authentication and authorization processes during the smart contract and cloud phases.

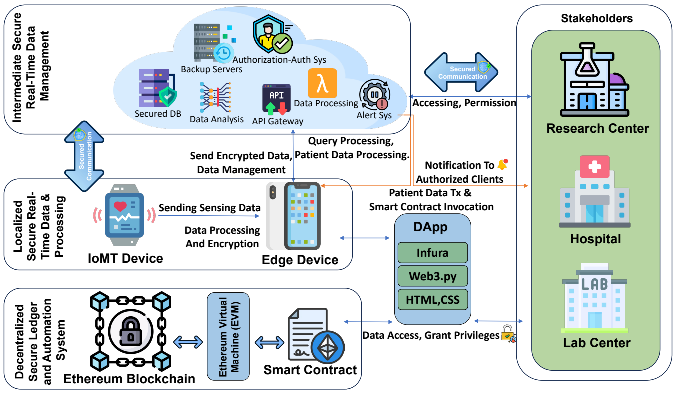

Intermediate Secure Real-Time Data Management
Backup Servers
Authorization-Auth Sys
Secured DB
Data Analysis
API
API Gateway
Data Processing
Alert Sys
Secured Communication
Accessing, Permission
Stakeholders
Research Center
Secured Communication
Send Encrypted Data, Data Management
Query Processing, Patient Data Processing.
Notification To Authorized Clients
Hospital
Localized Secure Real-Time Data & Processing
Sending Sensing Data
Data Processing And Encryption
IoMT Device
Edge Device
Patient Data Tx & Smart Contract Invocation
DApp
Infura
Web3.py
HTML,CSS
Decentralized Secure Ledger and Automation System
Ethereum Blockchain
Ethereum Virtual Machine (EVM)
Smart Contract
Data Access, Grant Privileges
LAB
Lab Center

Fig. 2: System Architecture.

C. The Proposed Algorithms

The process of securely storing the sensed physiological data involves several stages, as outlined in Algorithm 1. Initially, the sensors detect physiological parameters and transmit them to the edge device in a plain-text format. Edge devices receive the data and convert it into JSON format for efficient management. Edge device then encrypt the data via symmetric key encryption, using an appropriate key. Afterwards, the data is transmitted to the cloud over a secure API gateway and stored it in a secure cloud database linked to the client ID. This process involves passing through security measures such as token validation, certificate verification, and authorization and authentication using associated keys. If information is not deemed legitimate, it should be discarded. Otherwise, the data is stored in a secured cloud database, and the cloud hashes the data and returns it back to the edge device. Then, the edge device securely transacts the hash value to the blockchain via a smart contract, associating it with the client's account to ensure the integrity of the data. If there are any irregularities in the data measurements, the cloud notification systems will inform the closest registered emergency room and the registered caregiver about the patient's condition in order to provide medical aid.

Algorithm 1 Storing Sensing Data in Real-Time

```
Require: Physiological parameters sensed by IoMT device,
    Cloud $C_{srv}$, Ethereum blockchain $BC$
Ensure: Secure storage and processing of sensing data, and
    alert generation for abnormalities
Data Sensing and Transmission
Sensors sense physiological parameters
IoMT device transmits data to edge device in plain-text format
Data Processing at the Edge
Edge device receives data
Edge device formats data in JSON format
Edge device encrypts data with appropriate key
Edge device transfers data to the $C_{srv}$ via a secure channel using Secured API Gateway
$C_{srv}$ Data Validation and Storage
$C_{srv}$ checks token validation and verifies keys and certificates for authorization and authentication
if Validation successful then
    $C_{srv}$ processes incoming data
    Store data in secure cloud database associated with client ID
    Store data in multiple tables if needed, associating it with client ID
    $C_{srv}$ returns hash value of the data after successful storage
else
    Discard incoming data
end if
$BC$ Logging and Alerts
Edge device transacts hash value to $BC$, associating it with client account through smart contract
if Incoming data has abnormalities then
    Alert associated caregiver and ER to evaluate client status and provide an assessment
else
    Store data normally
end if
```

Sharing data is crucial for facilitating the sharing of medical records with other stakeholders. Algorithm 2 illustrates the procedure for sharing data across various stakeholders. Initially, the patient initiates a data sharing request through using the cloud and completing a form via a patient interface. This form includes details such as the specific limitations and type of data sharing, as well as whether it is time-restricted or not. Subsequently, the cloud securely stores the data via a sharing verification table and an access control table. Subsequently, the cloud generated a token using token generation and stored it in a shared verification mechanism. It then securely transmitted the hash value back to the edge device. The edge devices encrypt the hash value using the public key of the stakeholders and transmit it to the blockchain via a smart contract. A smart contract stores the encrypted hash value in a hashmap, which may be accessed by stakeholders with authorization in view mode. The stakeholders can access the hashmap by using the function permissionToken and the smart contract verifies the validity of the permission. If the permission is valid, the encrypted token can be viewed. Subsequently, the stakeholder decrypts the data and transmits the token via the cloud using an access validation interface to verify the stakeholder's authorization to access the client's data. Subsequently, the client and stakeholder were informed of the successful completion of the sharing procedure.

Algorithm 2 Sharing EHR with Healthcare Provider

```
Require: Patient $P$, Healthcare Provider $HCP$, Cloud $C_{srv}$,
    Ethereum blockchain $BC$
Ensure: Secure sharing of EHR with HCP
Initialization
Patient $P$ requests data sharing via $C_{srv}$
Filling Access Control Tables
$P$ fills out Sharing_Verification Table and AccessControl_Table
Token Generation and Encryption
$C_{srv}$ initializes new hashed token and stores it in Sharing_Verification
$C_{srv}$ sends the token to edge device
Edge device encrypts the token using the public key of $HCP$
Edge device stores the encrypted token in a smart contract on $BC$ using grantToken function.
Smart Contract Interaction
$HCP$ requests access to EHR
if $HCP$ has permission then
    $HCP$ views the encrypted token on $BC$ through getToken function.
    $HCP$ decrypts the token using their private key
    $HCP$ writes the decrypted token to the $C_{srv}$
    $C_{srv}$ hashes the token and sets Verified and AccessGranted attributes to True
else
    Access denied
end if
Confirmation
Both $P$ and $HCP$ are notified of successful EHR sharing
```

V. EXPERIMENTAL RESULTS AND DISCUSSION

1) Cost and Time Analysis: Our approach achieved an average transaction time of 7.370 seconds and an average block confirmation time of 12 seconds. The average cost per transaction is 0.00007213572 ETH, demonstrating that using a public blockchain ensures high availability and transparency with minimal cost and time overhead.

2) Privacy and Data Security: Integrating public blockchain with cloud technologies for secured data processing, storage, and sharing improves privacy and security. Data is encrypted on the edge device, sent via a secure API Gateway, and verified in the cloud. Token validation, authorization, and authentication are handled by the cloud, which stores encrypted data and generates a hash. This hash is transmitted to the blockchain utilizing smart contracts for immutability and security as described in 2. EHR sharing is secure utilizing blockchain, smart contracts, and cloud technology and multi-layered authentication for approved retrieval of data.

3) Scalability: The proposed system delivers higher scalability and achieves the maximum data retrieval rate per second compared to earlier works, as shown in table II.

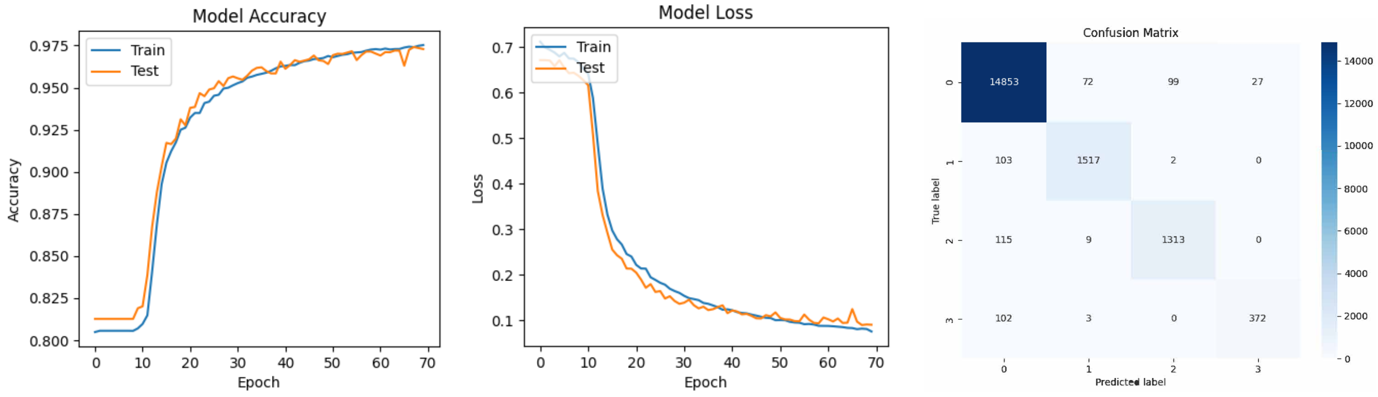
TABLE II: Scalability Performance Comparison

Tx	hChain	hChain 2.0	hChain 3.0
1	0.1017 seconds	0.0027 seconds	0.0002 seconds
10	0.1183 seconds	0.1335 seconds	0.0019 seconds
25	0.1508 seconds	0.2531 seconds	0.0028 seconds
50	0.1730 seconds	0.4928 seconds	0.0040 seconds
75	0.2020 seconds	0.8119 seconds	0.0060 seconds
100	0.2447 seconds	1.1546 seconds	0.0074 seconds

4) Model Performance Evaluation: The model demonstrated an impressive overall accuracy of 97.50 percent with a training loss of 0.0751, which indicates efficient learning and effective mitigation of errors while training. Furthermore, it has a strong performance over unseen data, as evidenced by its remarkable validation accuracy of 97.29 and low loss value of 0.090, as depicted in Figures 3a and 3b. The confusion matrix as shown in Figure 3c shows excellent prediction accuracy across all classes.

5) Availability and Auditability: The integration of blockchain and cloud enhances availability, auditability due to its decentralization behavior, which also overcomes centralized system issues and increases reliability. The system logs all data and transactions, links them into immutable blocks, and arranges them in an orderly manner to facilitate auditability. To ensure availability, blockchain records and broadcasts each transaction and operation to all nodes in the network.

6) Anonymity and Access Control Management: The proposed approach improves anonymity by employing modern cryptography and a client address instead of an actual identity. Even if the data is accessed without authorization, the identification of the patient remains independent of their actual identity. The proposed approach utilizes smart contracts to handle access control to the data, resulting in increased access control management. This is achieved by leveraging the decentralized nature of the system. The system offers multiple types of data sharing, including grant-based, time-based, and quantity-based. The patient must determine the suitable form of information to provide to the healthcare professional.



(a) Training and Validation Accuracy

(b) Training and Validation Loss

(c) Confusion Matrix

Fig. 3: Model Performance Metrics

VI. Conclusion and Future Directions

hChain 3.0 integrates blockchain and cloud computing for secure, real-time management of EHRs, ensuring data integrity and reliability for predictive modeling and abnormality detection. It supports healthcare providers in making accurate decisions. In addition to real-time monitoring, it offers personalized patient assessments and improved medication adherence by storing medication and EHR data, which include the patient's current status and dosage. The system dynamically adjusts medication dosage based on the patient's health status, stored provider guidelines, and threshold levels, ensuring that both the healthcare provider and the patient are notified of any modifications or improvements. This is crucial for chronic patients needing more care and immediate response, supported by accurate data. Unlike traditional centralized healthcare systems vulnerable to data breaches, it effectively reduces risks that threaten the lives of chronic patients.

In future work, enhancing system interoperability and scalability is crucial to accommodate real-time data processing. Furthermore, enhancing system flexibility by allowing each stakeholder to deploy their own smart contracts and create tailored agreements for each patient, instead of depending on pre-configured contracts, will be a primary objective.

References

[1] P. Mishra and G. Singh, "Internet of Medical Things Healthcare for Sustainable Smart Cities: Current Status and Future Prospects," *Applied Sciences*, vol. 13, no. 15, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/15/8869

[2] Z. Guo, Y. Wang, A. Liang, W. Van Devanter, and P. Zhang, "HealthBridge: A Decentralized and Interoperable Healthcare App for Rare Disease Communities," in *Proceedings of the IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 2023, pp. 2729–2736.

[3] O. Aldamaeen, W. Rashideh, and W. J. Obidallah, "Toward Patient-Centric Healthcare Systems: Key Requirements and Framework for Personal Health Records Based on Blockchain Technology," *Applied Sciences*, vol. 13, no. 13, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/13/7697

[4] M. Wazid and P. Gope, "BACKM-EHA: A Novel Blockchain-enabled Security Solution for IoMT-based E-healthcare Applications," *ACM Trans. Internet Technol.*, vol. 23, no. 3, aug 2023. [Online]. Available: https://doi.org/10.1145/3511898

[5] 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

[6] M. N. Alruwaill, S. P. Mohanty, and E. Kougianos, "Forti-Ins: A Blockchain Based Framework to Automate Healthcare Insurance Processing in Smart Cities," in *Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES)*, 2023, pp. 353–358.

[7] S. L. T. Vangipuram, S. P. Mohanty, E. Kougianos, and C. Ray, "agroString: Visibility and Provenance through a Private Blockchain Platform for Agricultural Dispense towards Consumers," *Sensors*, vol. 22, no. 21, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/21/8227

[8] A. Mitra, A. Singhal, S. P. Mohanty, E. Kougianos, and C. Ray, "eCrop: A Novel Framework for Automatic Crop Damage Estimation in Smart Agriculture," *SN Comput. Sci.*, vol. 3, no. 4, jun 2022. [Online]. Available: https://doi.org/10.1007/s42979-022-01216-8

[9] 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.

[10] A. M. Nasser, 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.

[11] S. Pandey, A. K. De, S. Choudhary, and M. Asim, "A Decentralized Blockchain-Based Architecture for Healthcare Industry," in *Proceedings of the International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, vol. 1, 2023, pp. 1–5.

[12] M. M. Sheeraz, M. A. I. Mozumder, M. O. Khan, M. U. Abid, M.-I. Joo, and H.-C. Kim, "Blockchain System for Trustless Healthcare Data Sharing with Hyperledger Fabric in Action," in *Proceedings of the 25th International Conference on Advanced Communication Technology (ICACT)*, 2023, pp. 437–440.

[13] A. Haddad, M. H. Habaebi, M. R. Islam, and S. A. Zabidi, "Blockchain for Healthcare Medical Records Management System with Sharing Control," in *Proceedings of the IEEE 7th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA)*, 2021, pp. 30–34.

[14] T.-L. Zhu and T.-H. Chen, "A Patient-Centric Key Management Protocol for Healthcare Information System based on Blockchain," in *Proceedings of the IEEE Conference on Dependable and Secure Computing (DSC)*, 2021, pp. 1–5.

[15] S. Panda, A. Mukherjee, R. Halder, and S. Mondal, "Blockchain-Enabled Emergency Detection and Response in Mobile Healthcare System," in *Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2022, pp. 1–5.

[16] M. Haidar and S. Kumar, "Smart Healthcare System for Biomedical and Health Care Applications using Aadhaar and Blockchain," in *Proceedings of the 5th International Conference on Information Systems and Computer Networks (ISCON)*, 2021, pp. 1–5.