hChain: Blockchain Based Healthcare Data Sharing with Enhanced Security and Privacy Location-Based-Authentication

Musharraf N. Alruwaill
University of North Texas
Denton, Texas, USA
MusharrafAlruwaill@my.unt.edu

Saraju P. Mohanty
University of North Texas
Denton, Texas, USA
saraju.mohanty@unt.edu

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

Abstract

In smart healthcare, blockchain technology addresses existing concerns with security, privacy, and electronic healthcare records. In addition, utilizing edge devices with IoMT devices is very advantageous for addressing security, computing, and storage challenges. Symmetric and asymmetric keys are used to conceal sensitive information from unauthorized parties. Moreover, the hash function SHA256 helps for data alteration detection. The proposed system uses a blockchain-based smart healthcare system using IoMT devices for continuous patient monitoring. The edge device is used to hash and encrypt data and provide additional computational capability. A symmetric key maintains data privacy in the blockchain, allowing patients to safely share data through smart contracts while preventing unauthorized physicians from seeing it. A verification node and blockchain sign and validate patient data in the healthcare provider system using an asymmetric key. Location-based authentication is addressed to ensure the authenticity and data source.

CCS Concepts

• **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Keywords

Smart Healthcare, Healthcare Cyber-Physical System (H-CPS), Internet-of-Medical-Things (IoMT), Electronic Health Record (EHR), Blockchain, Data Security, Data Privacy, Data Integrity, Data Sharing

ACM Reference Format:

Musharraf N. Alruwaill, Saraju P. Mohanty, and Elias Kougianos. 2023. hChain: Blockchain Based Healthcare Data Sharing with Enhanced Security and Privacy Location-Based-Authentication. In *Proceedings of the Great Lakes Symposium on VLSI 2023 (GLSVLSI '23), June 18–23, 2023, Knoxville, TN, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3583781.3590255

1 Introduction

The increasing population expansion has overburdened traditional health care. There are not enough physicians to meet the demands of the populace [15]. In addition, traditional health care providers (HCPs) use a centralized client-server architecture for the storage and management of electronic healthcare records (EHRs). Because of technical and architectural constraints, EHRs maintained by HCPs are stored in a repository that is inaccessible to other healthcare providers. As a result, when a patient needs to visit various healthcare providers, they need permission each time to transfer and/or share their data. However, there is no feasible and confidential data sharing solution [27]. Furthermore, numerous technologies have emerged to improve and strengthen traditional systems, such as IoT and wearable devices for remote patient monitoring [3]. However, these devices have capability constraints such as memory, storage, processing, and security issues [6]. Finally, traditional healthcare does not meet the requirements for security, data sharing, and timeliness.

Smart healthcare is the combination of different entities and technologies in a smart city to provide high-quality services to existing patients [15]. It also uses Internet-of-Medical-Things (IoMT) to monitor patients' health status in real time. However, IoMT devices have capabilities issues such as low computational power, storage, memory, and security [10]. The proposed system uses blockchain technology to decentralize the data with security in mind. It also has a smart contract for authentication and user interaction with data validation and robust access control management. In addition, it keeps the patient electronic healthcare records EHRs private due to the cryptography that is used to hide the original message and store it in encrypted form. The proposed system uses multiple authentication factors to raise the security level. The rest of the paper is structured as follows. Section 1 discusses the novel contributions of the current paper, and Section 2 presents prior related work. The hChain is described in section 3. Section 4 discusses the hChain algorithms, while Section 5 presents the system architecture. Experimental results are addressed in section 6. Section 7 concludes the paper.

2 Novel Contributions

2.1 Problem Addressed in the Current Paper

Healthcare provider systems currently have many drawbacks that make the system weak in integrity, security and ability to provide. Currently, there is no data monitoring solution that is both effective and efficient [17]. Centralized systems have security and privacy issues [19]. IoMT and other emerging technologies are not capable to provide enough security to the system due to its device constraints and capabilities.

2.2 The Novelty of the Proposed Solution

IoMT devices with the help of near edge devices improve the security and time of computation processes. Addressing solutions to potential attacks such as the man in the middle attack during

GLSVLSI '23, June 18–23, 2023, Knoxville, TN, USA.

ACM ISBN 979-8-4007-0125-2/23/06…$15.00
https://doi.org/10.1145/3583781.3590255

public transmission [22] is important. Therefore, symmetric key encryption is addressed in this paper to help secure the data. Multiple factors of verification and validation improve the whole system security. Blockchain technology stores the data in decentralized manner and process and offers advantages of blockchain security, integrity and availability to improve the healthcare providers system [18]. Location-based authentication is proposed in hChain to improve the data integrity and authenticity as well. Smart contract helps to save patient time and improve the security as well.

3 Related Prior Works

Different approaches are proposed by researchers based on various frameworks. [9] proposes a secured database, blockchain for a PHR (personal healthcare record), and AES for data encryption before storage.[1] uses fingerprints for authentication, and in [25] a system is proposed with multiple layers of security design to raise the security level. However, both [1, 25] use the cloud to store the raw medical data. In [2], a framework is proposed using blockchain to access control management of the data and provides data integrity beside hospital local database. Alternatively, storing the electronic healthcare records on cloud such as [1, 25] or blockchain [8, 21] the proposed frameworks use IPFS to store the file while blockchain maintains the returned hash value from IPFS. DAAC [4] similarly proposes off-chain storage, whether cloud-based or distributed. However, the DAAC system provides a practical means of transitioning from the current system to blockchain-based e-health.

In [24] the proposed framework uses a distributed database to maintain the healthcare data instead of using blockchain to have the data decentralized. In [5] the framework consists of two blockchain networks to make data sharing in secure manner between EHR and framework stakeholders. In [12] the proposed system provides suitable architecture for ensuring the data integrity of the machine learning model through blockchain. However, the system lacks additional security levels.

Uur proposed system overcomes the drawbacks of the previous works and has a different framework design. It uses multiple authentication factors to ensure the data came from the right source, whereas [2, 5, 12] use a single authentication factor. Therefore, hChain raises the security level. In addition, hChain uses blockchain to store the data making the system fully decentralized in a simple design, unlike [8, 21] which use IPFS to store the data and a complex framework design. In addition, the proposed systems [1, 25] use the cloud to store the raw medical data instead of decentralized data via storing the data on blockchain and avoiding the cloud-centric data storage. [24] uses distributed databases to keep the data, while smart contracts are used for access control management, while hChain uses the blockchain and smart contracts to store the data and provide robust access control management using RBAC to provide secure data sharing to overcome the shortcoming of distributed databases and have multiple security layers and authentication factors in different layers. Table 1 provides a comparative perspective of hChain with related works.

4 The Proposed Framework

The hChain framework components, blockchain technology, location-based authentication, and smart contracts are discussed in the following subsections.

4.1 Framework Components

The proposed system is primarily comprised of five components: Blockchain technology, IoMT devices, Verification node, Public and private key encryption, and symmetric key encryption, as depicted in Fig. 1. The components communicate and interact through various mechanisms. These are covered in detail in this section.

4.1.1 Private Blockchain Based on openness, there are three types of blockchain technology: private, public, and consortium blockchain [20]. The proposed system employs the private blockchain, which restricts blockchain network activity to users who have been validated and invited.

4.1.2 Smart Contract It is a self-executing program that handles the transactions that are received through blockchain network members [13]. hChain uses a smart contract to manage the EHR and interact with the blockchain participants in a secure manner.

4.1.3 IoMT IoMT devices monitor patient health in real-time [14]. These devices have low computational power, memory, and storage capabilities. In addition, IoT devices lack security [7].

4.1.4 Edge Device The Edge device is used to overcome the shortcomings of IoMTs devices by taking over the computation power and memory [26] as well as increasing the security level at the HCP layer.

4.1.5 Verification Node The verification node is located internally inside the healthcare provider to raise the security level. The verification node uses the patient identity, HCP edge device (HCP-E) signature, and patient location to authenticate the patient and the data to ensure the data has not been modified during the transmission. Multiple nodes are needed to authenticate the data to avoid single node authentication and validation. It verifies the patient's identity using the secure database and validates the HCP-E signature to ensure that the data has been previously signed and validated.

4.2 Location Based Authentication

The hChain framework makes use of GPS coordinates as one of the factors in the authentication process. Following the completion of the patient registration process, the patient's home coordinates are stored in an internal, secured database that is only accessible to the healthcare provider nodes. The data pertaining to the coordinates is stored in an encrypted format so as to prevent any unauthorized individuals from reading the data. Calculations of the distance between the received coordinates and the stored coordinates are carried out by the edge device that is located at the healthcare provider layer. These calculations are carried out using the received coordinates. If the distance is considered to be within the home region, then it is acceptable to use the data. Otherwise, the data is rejected, and the process is terminated if it is not accepted.

4.3 hChain Smart Contracts

Patient EHRs are only seen by the patient or an authorized person. Smart contacts are used to manage access control management. The patient has the ability to share the data with any permissioned healthcare provider. The access control management used is called

Table 1: Systems Devices, Security Comparing and EHR Storage Type and Format to hChain

The Framework/System	EHR Data Storage	EHR Format	Edge	Physical Authentication	Security Levels
Gabriel and Sengottuvelan, 2021 [9]	Blockchain	Encrypted	No	No	One layer
Al Baqari and Barka, 2020 [1]	Cloud Storage	Plain-text	No	No	One layer
Srivastava et al, 2019. [25]	Cloud Storage	Encrypted	No	No	Multiple layers
Chakraborty et al, 2019. [5]	Blockchain And Cloud Storage	Plain-Text	No	No	One layer
B et al, 2021. [2]	Database	Plain-Text	No	No	One layer
Simpson et al, 2021. [24]	Database	Plain-Text	No	No	One layer
Haddad et al, 2021. [12]	Blockchain And Cloud	Plain-Text	No	No	One layer
Egala et al, 2021. [8]	IPFS	Encrypted	Yes	No	Multiple layers
Santhosh et al, 2022. [21]	IPFS	Encrypted	Yes	No	Multiple layers
Biswas et al, 2022. [4]	Off-Chain	Encrypted and Plain-text	No	No	One layer
hChain	**Blockchain**	**Encrypted**	**Yes**	**Yes**	**Multiple layers**

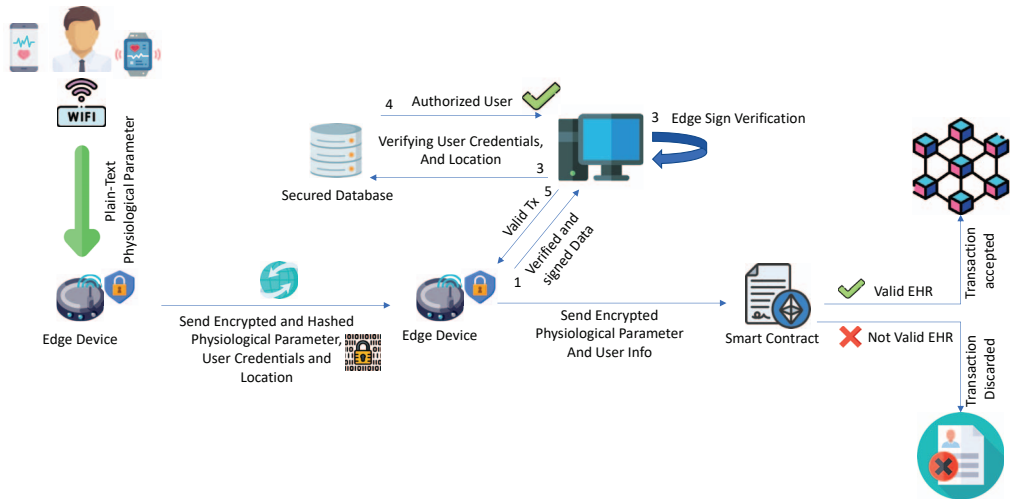

Figure 1: Overview of the Proposed System based H-CPS.

RBAC, which is role-based access control. It provides each membership authorization process based on the member role [23]. Smart contracts have three main types of authorization, HCP, HCP registration, and HCP administration. The administration controls HCP registration membership and HCP registration has the ability to add, remove, and control HCP, while HCP has the ability to control their patients.

5 The Proposed Architecture

hChain consists of three main layers. The first layer is the IoMT layer which contains IoMT and wearable devices and home edge device.Healthcare provider layer is addressed at the second layer and has HCP edge node and verification node. The blockchain is placed at the third layer, as presented at Fig. 2. The following subsections describe hChain based on a layered view.

5.1 Data Origination Layer

The first hChain framework layer is the data origination layer. The physiological parameters are initially collected from the sensors worn by the patient. Data encryption and processing offload are offloaded to the edge device. As shown in Fig. 2, the data is then transmitted to the home edge device via Zigbee or WiFi technology in plain-text format. After that, the edge device encrypts the data using a secret key and performing other functionalities such as data formatting, hashing, adding other information and signing. After the data has been processed, the data is transmitted to the HCP layer.

5.2 HCP Layer

The HCP layer consists of mainly three entities: the edge device, the verification node and the secured database. The edge device validates the signature and integrity of incoming data. Once the data is validated, it forwards it to the verification node to validate the edge device signature to ensure the data has been signed by only authorized nodes. the verification node verifies the patient identity through location based authentication and identity as described at section 4.1.5.

5.3 Blockchain Layer

At the third layer, the blockchain and smart contracts provide robust access control and management and storing the data in decentralized manner to enhance security through decentralized-based storage [11]. RBAC is used to assign each authorization with the proper privileges. Each transaction is handled by smart contracts and after smart contract verification, the data is stored in the ledger.

5.4 The Proposed Algorithms

To be able to connect directly with the healthcare provider via IoMT or wearable devices, the patient must be enrolled in the healthcare

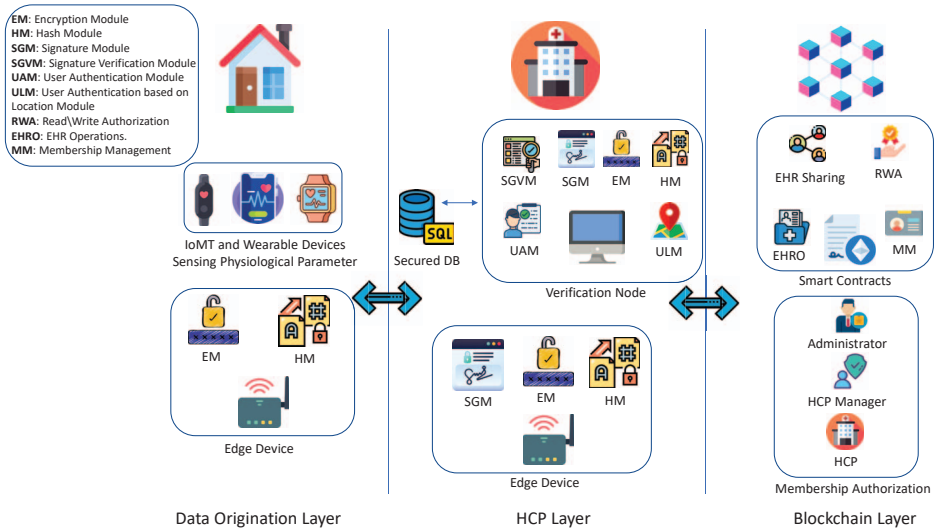

Figure 2: hChain System Architecture.

provider's network. In Algorithm 1, the stages from data collection through its delivery to the healthcare provider's edge device are described. Initially, biosensors are used to measure the patient's physiological parameters. The acquired data is then sent in plaintext to the edge device. After that, the edge device encrypts and signs the incoming data using the edge device keys and generates a hash value for each parameter to ensure its security and integrity. The parameters consist of GPS location, hash values, data signature and encrypted physiological parameters. At the end, the data is sent HCP-E.

Algorithm 1 explains the processes when the data is received from patient edge device until being stored on blockchain. HCP-E receives the encrypted data from PED. HCP-E validates the data against integrity using the same hash function and then signs the data if the hash values are matched and the signature is valid. Later, HCP-E signs the data and sends it to the verification node (VN). VN verifies the HCP-E signature. After the signature verification, the patient's identity is verified by querying patient identity stored in a secure database, as described in Algorithm 2. Later, VN uses the other authentication factors to authenticate the patient using location-based authentication. VN calculates the distance between the location that is stored and the patient's current location to ensure the patient's legitimacy. Once all of the data has been validated and verified, VN sends a signed transaction to the smart contract.

5.5 The Implementation

As seen in Figure 2, blockchain technology, smart contracts, encrypted databases, and cryptography algorithms are employed. Ganache is implemented using a private blockchain environment that functions as the Ethereum blockchain. In addition, Brownie is used to compile, deploy, and test smart contracts. For data privacy and authenticity, it primarily employs the symmetric key encryption and asymmetric key encryption cryptographic techniques. In addition, SQlite is used to store encrypted patient data within the healthcare provider's system and to maintain patient identity and basic information. Python is utilized in conjunction

Algorithm 1 The Steps of EHR data From IoMT to HCP.

Input: Data D_i collected from IoMT Devices.
Output: Authenticated GPD or Discarded GPD.
IoMT Device sends plain-text PD in real-time to PED
PED Receive PD and Encrypt PD using Secret Key
PED Hashes Each PD and Append it to GPD
PED Encrypts and sign UI and append it to GPD
PED Groups all PDs and UI as GPD
PED sends GPD to $HCP-E$
$HCP-E$ receives GPDs
$HCP-E$ generates hashes of all encrypted PD in GPD.
$HCP-E$ generates hash of GPD
if $HCP-E$ Hash Values MATCH GPD hash Values and Signature is Valid **then**
    $HCP-E$ uses own private key to sign the GPD
    Append the signature to signed GPD
    $HCP-E$ sends signed GPD to VN
else
    Discard
end if

Algorithm 2 The Steps of Sending EHR From HCP to Blockchain.

Input: Valid GPD.
Output: Store Valid GPD in the ledger.
VN Receive verified and signed GPD from $HCP-E$.
VN verifies $HCP-E$ Signature
if Signature is Valid **then**
    VN extracts UI and make location query to secured DB
    VN Calculates the distance between current location and stored UI location
    if Location is Valid AND Patient Identity is Valid **then**
        VN signs GPD with private key
        VN Transacts signed GPD to SM
        SM privilege verification
        if HCP privilege is Valid **then**
            Append GPD to UI HCP Hashmap
        else
            Error message appear to request UI
        end if
    else
        Discard
    end if
else
    Discard
end if

with the brownie framework to communicate with the ganache private blockchain. Additionally, it is utilized as a command-line interface to implement various tasks on edge devices and the VN. The smart contracts are written in the solidity language.There are two smart contracts required for hChain implementation. The first smart contract is for the management of access control. The second smart contract is used to manage healthcare records, authorizations, and the remaining hChain functionalities.

6 Experimental Results

6.1 Security Analysis

hChain uses symmetric key encryption to encrypt the data before transmission. Therefore, the data is in unreadable form, and then the encrypted data is sent to the healthcare provider layer. If an attacker gains a copy of the data, it is in encrypted form. As a result, the attacker cannot use or comprehend these data until he obtains the secret key. The second type of unauthorized access is through gaining access to the stored data. The proposed system uses multiple levels of authentication. The stored data requires a different authentication process to gain authorization to access the data. The first authentication process is through the user's identity. The second authentication process is location based on authentication. The location has a set of coordinates that represent the existence of the data. Once the patient has registered with the healthcare provider, the patient's location is stored by the healthcare provider in encrypted form. For patient authenticity, the distance calculation is made on HCP layer to verify that the data came from the right place.

Authorization through brute force attack solution is addressed at hChain. The system is resistant to brute force attacks due to the multiple authentication processes at each layer. Since each layer has different authentication factors, it is difficult to gain all this information and keys for the whole system to gain unauthorized access through a brute force attack.

Data tampering proof is proposed at hChain through a one-way hash function and patient signature. At the hChain framework, EHR and other data are encrypted and hashed before sending the data through the Internet. Therefore, any change to the data will alter the whole hash value. Once, the HCP-E verifies the hash value and the signature, any change to the data will be detected. Moreover, collision and preimage attack prevention are addressed in hChain. A collision attack can be launched by locating two distinct inputs that result in a single output as a hash value. The preimage attack is tarnishing the output, which is the hash value output. The attacker tries to find input that produces the desired hash value. In the proposed system, hChain uses SHA256, which is resistant to collision attacks and premiage attacks.

6.2 Computation Time Analysis

The healthcare provider edge node and the verification node perform encryption, validation, and authentication tasks to increase the security level. Fig. 3 depicts the computation time required to complete a task and determine its validity, authentication, or discard the transaction. Fig. 4 shows the total transaction processing, once the data was received until data validation determination.In Fig. 5, the time of the encryption analysis shows how long it takes to encrypt and decrypt all of the data using both symmetric key encryption and asymmetric key encryption. In order to circumvent latency and the problems that are associated with it in real-time systems, the symmetric key encryption protocol has been introduced to the hChain system.

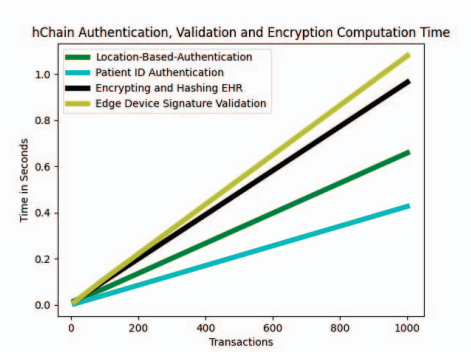

Figure 3: Computation Time.

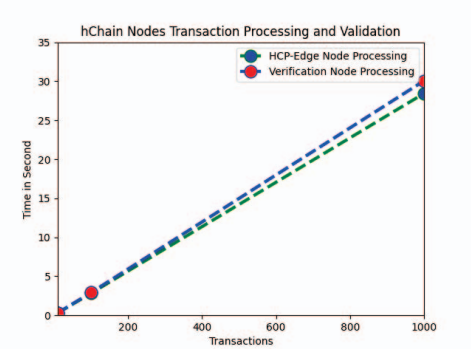

Figure 4: hChain Nodes Tx Processing and Validation.

In addition, the keying process for encrypting the data using the private and public keys takes a significant amount of time, which contributes to the increase in the delay due to the lower computational complexity [16], as seen in Fig. 5. When the amount of data is quite small, the time required varies slightly. On the other hand, when the data is longer than 3,000 bytes, the distinction becomes readily apparent. The suggested use for encryption is using symmetric key when the system relies on real time. Asymmetric key encryption for very low data is suggested.

7 Conclusion

The proposed system uses the blockchain to provide data security and privacy to the traditional healthcare frameworks. A variety of cryptographic algorithms are utilized to ensure system security. Additionally, numerous authentication factors are utilized to guarantee authenticity which leads to proper authorization. The framework is composed of three principal layers: the patient layer, the healthcare provider layer, and the blockchain layer. The first layer is accountable for generating and securing the data source. The second layer is intended to validate patient data and identity. The third layer is responsible for data management and access control management via smart contracts.

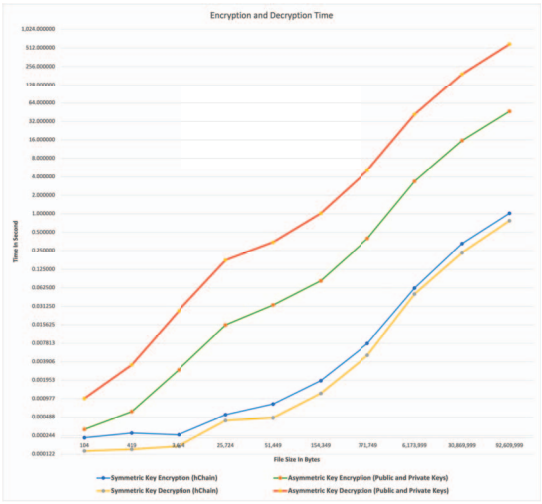

Figure 5: Encryption and Decryption Comparison.

References

[1] Mohammed Al Baqari and Ezedin Barka. 2020. Biometric-Based Blockchain EHR System (BBEHR). In *2020 International Wireless Communications and Mobile Computing (IWCMC)*. 2228–2234. https://doi.org/10.1109/IWCMC48107.2020.9148357

[2] Vardhini B, Shreyas N Dass, Sahana R, and R. Chinnaiyan. 2021. A Blockchain based Electronic Medical Health Records Framework using Smart Contracts. In *2021 International Conference on Computer Communication and Informatics (ICCCI)*. 1–4. https://doi.org/10.1109/ICCCI50826.2021.9402689

[3] Vaidik Bhatt and Samyadip Chakraborty. 2021. Real-time healthcare monitoring using smart systems: A step towards healthcare service orchestration Smart systems for futuristic healthcare. In *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*. 772–777. https://doi.org/10.1109/ICAIS50930.2021.9396029

[4] Sujit Biswas, Kashif Sharif, Fan Li, Iqbal Alam, and Saraju P. Mohanty. 2022. DAAC: Digital Asset Access Control in a Unified Blockchain Based E-Health System. *IEEE Transactions on Big Data* 8, 5 (2022), 1273–1287. https://doi.org/10.1109/TBDATA.2020.3037914

[5] Sabyasachi Chakraborty, Satyabrata Aich, and Hee-Cheol Kim. 2019. A Secure Healthcare System Design Framework using Blockchain Technology. In *2019 21st International Conference on Advanced Communication Technology (ICACT)*. 260–264. https://doi.org/10.23919/ICACT.2019.8701983

[6] Erikson Júlio De Aguiar, Bruno S. Faiçal, Bhaskar Krishnamachari, and Jó Ueyama. 2020. A Survey of Blockchain-Based Strategies for Healthcare. *ACM Comput. Surv.* 53, 2, Article 27 (mar 2020), 27 pages. https://doi.org/10.1145/3376915

[7] Francisco José de Haro-Olmo, Ángel Jesús Varela-Vaca, and José Antonio Álvarez Bermejo. 2020. Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. *Sensors* 20, 24 (2020). https://doi.org/10.3390/s20247171

[8] Bhaskara S. Egala, Ashok K. Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. 2021. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet of Things Journal* 8, 14 (2021), 11717–11731. https://doi.org/10.1109/JIOT.2021.3058946

[9] S Joseph Gabriel and P. Sengottuvelan. 2021. An Enhanced Blockchain Technology with AES Encryption Security System for Healthcare System. In *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*. 400–405. https://doi.org/10.1109/ICOSEC51865.2021.9591956

[10] Ali Ghubaish, Tara Salman, Maede Zolanvari, Devrim Unal, Abdulla Al-Ali, and Raj Jain. 2021. Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. *IEEE Internet of Things Journal* 8, 11 (2021), 8707–8718. https://doi.org/10.1109/JIOT.2020.3045653

[11] Malik Junaid Jami Gul, Anand Paul, Seungmin Rho, and Mucheol Kim. 2020. Blockchain based healthcare system with Artificial Intelligence. In *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*. 740–741. https://doi.org/10.1109/CSCI51800.2020.00138

[12] Alaa Haddad, Mohamed Hadi Habaebi, Md Rafiqul Islam, and Suriza Ahmad Zabidi. 2021. Blockchain for Healthcare Medical Records Management System with Sharing Control. In *2021 IEEE 7th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA)*. 30–34. https://doi.org/10.1109/ICSIMA50015.2021.9526301

[13] Rajesh Kumar Kaushal, Naveen Kumar, Surya Narayan Panda, and Vinay Kukreja. 2021. Immutable Smart Contracts on Blockchain Technology: Its Benefits and Barriers. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. 1–5. https://doi.org/10.1109/ICRITO51393.2021.9596538

[14] Carlos José Martínez and Sebastià Galmés. 2022. Analysis of the primary attacks on IoMT Internet of Medical Things communications protocols. In *2022 IEEE World AI IoT Congress (AIIoT)*. 01–07. https://doi.org/10.1109/AIIoT54504.2022.9817252

[15] Saraju P. Mohanty, Uma Choppali, and Elias Kougianos. 2016. Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine* 5, 3 (2016), 60–70. https://doi.org/10.1109/MCE.2016.2556879

[16] Abid Murtaza, Syed Jahanzeb Hussain Pirzada, and Liu Jianwei. 2019. A New Symmetric Key Encryption Algorithm With Higher Performance. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. 1–7. https://doi.org/10.1109/ICOMET.2019.8673469

[17] Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana, and Aruna Seneviratne. 2021. Blockchain and AI-Based Solutions to Combat Coronavirus (COVID-19)-Like Epidemics: A Survey. *IEEE Access* 9 (2021), 95730–95753. https://doi.org/10.1109/ACCESS.2021.3093633

[18] N. Poonguzhali, S. Gayathri, A. Deebika, and R. Suriapriya. 2020. A Framework For Electronic Health Record Using Blockchain Technology. In *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)*. 1–5. https://doi.org/10.1109/ICSCAN49426.2020.9262369

[19] Jinglin Qiu, Xueping Liang, Sachin Shetty, and Daniel Bowden. 2018. Towards Secure and Smart Healthcare in Smart Cities Using Blockchain. In *2018 IEEE International Smart Cities Conference (ISC2)*. 1–4. https://doi.org/10.1109/ISC2.2018.8656914

[20] Pranav Ratta, Amanpreet Kaur, Sparsh Sharma, Dr. Mohammad Shabaz, and Gaurav Dhiman. 2021. Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives. *Journal of Food Quality* 2021 (05 2021), 1–20. https://doi.org/10.1155/2021/7608296

[21] Egala Santhosh, Ashok Pradhan, Venkataramana Badarla, and Saraju P. Mohanty. 2022. iBlock: An Intelligent Decentralised Blockchain-based Pandemic Detection and Assisting System. *Journal of Signal Processing Systems* 94 (06 2022). https://doi.org/10.1007/s11265-021-01704-9

[22] Sabin Shahi, Margaret Redestowicz, and Nectarios Costadopoulos. 2020. Authentication in E-Health Services. In *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*. 1–10. https://doi.org/10.1109/CITISIA50690.2020.9371820

[23] Roohi Sille, Hussain Falih Mahdi, Tanupriya Choudhury, Samyukta Sahoo, Akshita Kapoor, Ishita Nanda, and Arnav Sharma. 2022. Review Study on Blockchain Frameworks for Security Issues in IoT Devices. In *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. 876–881. https://doi.org/10.1109/ISMSIT56059.2022.9932744

[24] Grace Simpson, Laurent Nana, and Quist-Aphetsi Kester. 2021. A Centralized Data Validation System Model for Healthcare Systems Based on Blockchain. In *2021 International Conference on Cyber Security and Internet of Things (ICSIoT)*. 55–58. https://doi.org/10.1109/ICSIoT55070.2021.00019

[25] Gautam Srivastava, Jorge Crichigno, and Shalini Dhar. 2019. A Light and Secure Healthcare Blockchain for IoT Medical Devices. In *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*. 1–5. https://doi.org/10.1109/CCECE.2019.8861593

[26] Sukrutha Vangipuram, S. P. Mohanty, and Elias Kougianos. 2021. CoviChain: A Blockchain Based Framework for Nonrepudiable Contact Tracing in Healthcare Cyber-Physical Systems During Pandemic Outbreaks. *SN Computer Science* 2 (09 2021). https://doi.org/10.1007/s42979-021-00746-x

[27] Ting-Le Zhu and Tzung-Her Chen. 2021. A Patient-Centric Key Management Protocol for Healthcare Information System based on Blockchain. In *2021 IEEE Conference on Dependable and Secure Computing (DSC)*. 1–5. https://doi.org/10.1109/DSC49826.2021.9346259