A Patient-centric Blockchain-based system for access management in telehealth and telemedicine domain

Ayoub Ghani
Faculty of Sciences
Sidi Mohamed Ben Abdellah University
Fez, Morocco
ayoub.ghani@usmba.ac.ma

Ahmed Zinedine
Faculty of Sciences
Sidi Mohamed Ben Abdellah University
Fez, Morocco
ahmed.zinedine@usmba.ac.ma

Mohammed El Mohajir
Faculty of Sciences
Abdelmalek Essaadi University
Tetouan, Morocco
m.elmohajir@ieee.ma

2023 7th IEEE Congress on Information Science and Technology (CiSt) | 978-1-6654-6133-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/CiSt56084.2023.10409917

Abstract— **The rapid development of Internet of Things (IoT) and wearable devices enable healthcare providers to remotely collect and instantly process patient's health data for monitoring and diagnosis. In COVID-19-like virus scenario, the social destination is crucial to avoid virus propagation. Thus, such wearable devices can mitigate the spread of virus, and provide important information of patients such as breathing patterns, blood glucose level, and blood pressure to health providers. Hence, the health-related devices also generate a large amount of medical data. As a result, many of these data are exposed to privacy breach, data leakage, and other security-related issues. Blockchain as a prominent technology can mitigate the privacy and security issues in the telemedicine and telehealth systems. In this paper, we propose a blockchain-based system for access management in telehealth and telemedicine domain. The main purpose of this work is to build a patient-centric access management system that comply with the General Data Protection Regulation (GDPR) of the European Union. Hence, it also aims to record all access management related data in an immutable ledger which gives more transparency over shared data. In addition, we use Ethereum built-in environment to develop our smart contract and Interplanetary File System (IPFS) to store patient's data. We conducted a security analysis using Oyente tool, to demonstrate that our smart contract code is sufficiently secure against common security vulnerabilities.**

Keywords— Blockchain, Ethereum, Smart contract, IoT, Oyente, telemedicine, telehealth.

I. Introduction

The development of connected devices with built-in biosensors has completely revolutionized healthcare systems [1], as a step towards enhanced telehealth and telemedicine services. Hence, the connected devices can be incorporated into clothing or worn on the body as accessories. In a COVID-19-like virus scenario, it is crucial to maintain social destination and keep vulnerable patients with severe health problems in-doors. Moreover, healthcare providers need to remotely keep a permanent control over vulnerable patients' health. To do so, the connected devices can enable healthcare providers to remotely monitor, diagnose, and treat patients. These devices are able to track patient's general health data, among others: blood pressure, blood sugar rate, heart rate, sleep conditions, breathing patterns. Furthermore, these devices have been categorized by [2] as follows: (A) Stationary Medical Devices: these devices are used for specific physical locations, (B) Medical Embedded Devices: these devices are placed inside the human body, (C) Medical Wearable Devices: these devices prescribed by doctors, and (D) Wearable Health Monitoring Devices: these devices are worn on the body. By leveraging the Internet of Things (IoT) technology, telehealth and telemedicine enable efficient healthcare access and offer better care coordination and treatment results. However, IoT devices are vulnerable to security and privacy issues, due to permanent Internet connection [2]. As a result, patient's data can be a subject to privacy leakage. In fact, 44 major security and privacy breaches occurred worldwide in 2021. Security and privacy breaches affected both commercial and governmental entities, such Microsoft and the California State Controller's Office [3]. Moreover, most current telehealth and telemedicine systems rely on centralized-based solutions which require a trusted central authority. This type of systems suffers from single point of failure (SPoF). In addition, in case of malicious attacks, alterations made to patient's data cannot be identified or recovered [4]. Furthermore, such centralized systems store and share data using local or cloud databases under the healthcare provider's control, leading to severe privacy issues, such as, sharing patient's data unlawfully without patient's permission. Furthermore, access management suffers from many drawbacks: The unlimited time of accessing data shared with third-parties, the limited trust on third-parties with whom data is shared, the difficulty of conducting audit trail. Moreover, the General Data Protection Regulation (GDPR) [5] of the European Union was applied in order to impose data protection laws for restricted processing and provide users more control over potential data usage. These issues in the current telehealth and telemedicine systems compel us to enhance the security and privacy level of patient's data storing and sharing based on a patient-centric approach. Additionally, our approach aims to be in compliance with GDPR regulations on access management.

Blockchain as a prominent technology can mitigate the privacy and security issues in the telemedicine and telehealth systems. Further, Blockchain has been defined as a decentralized technology, in which peer-to-peer transactions between unreliable parties take place without the involvement of a middleman. The verification and validation process involves users. Moreover, Blockchain provides a robust security structure by utilizing cryptography mechanisms for encryption. Blockchain is a tamper-proof distributed ledger, which consists of a sequence of blocks, tied with hash values. The blocks record lists of public or private peer-to-peer network transactions [6]. All occurred transactions data is converted to a hash value by leveraging Merkle tree [7], in order to manage data storage and control the accessibility to data. Therefore, Blockchain cannot be modified or altered. Indeed, the alteration might introduce changes to all subsequent blocks of the network. Moreover, Consensus algorithms maintain data consistency in such distributed networks. the following key characteristics best describe blockchain technology:

- **Decentralization**: It aims to eliminate any central party from owning and making control over the system.
- **Transparency**: It means that all recorded data is now transparent to each node in a public Blockchain.
- **Persistency**: The validation process can be done in few minutes. Blocks with invalid transactions could be figured out instantly. There is no way to delete or roll back recorded transactions.
- **Immutability**: All recorded data are stored forever, unless malicious miners take control over Blockchain network.
- **Anonymity**: In a public Blockchain, users interact with the network using generated address, which hides user identity. In contrast to public Blockchain, private one is in need to identify the real identity of the users.

Moreover, Ethereum [8] blockchain introduces Smart Contract concept, with the promise of increasing efficiency and reducing costs compared to current existing enterprise systems. Smart contract is intended to define the core logic of a decentralized application dApp to transfer financial assets, products, or services in a trustless environment. In addition, InterPlanetary File System (IPFS) [9] is a decentralized storage system. It is defined as a peer-to-peer distributed file system that aims to connect all computing devices with the same system of files. Furthermore, IPFS provides a high throughput content-addressed block storage model, with content-addressed hyperlinks. IPFS calculates the unique Hash of a file which is accessible to all peers of the network. The Hash is changed if the file is being tampered with.

The paper is organized as follows: Section II discusses the related works and contributions. Section III defines the system prerequisites, whereas section IV describes the proposed system design including participants, smart contract, and the process of storing and sharing health-related data. Section V includes a discussion over the testing setup, smart contract security analysis, validation of security prerequisites, and GDPR compliance, finally a conclusion is found in section VI.

II. Related works and contributions

A. Related works

The authors in [10] examined the potential benefits and adaptability issues for blockchain technology in the telehealth and telemedicine sector, which led to the conclusion that blockchain technology is essential for successfully securing health data from malicious actors using smart contracts by ensuring a strict patient-centric access management. In addition, the authors in [11] offered an overview of the key improvements of Blockchain technology for healthcare data management among others accurate health data, access management, secure data sharing, traceability, authenticity, and immutability. Moreover, the authors in [12] identified the blockchain impact on the healthcare and biomedical industry for security and privacy purpose. As a result, Blockchain can impact positively data integrity, non-repudiation, access control (access management), auditing, and so on. Moreover, the work in [13] proposed a framework for healthcare based on Blockchain and IoT in order to secure patient monitoring health signs. As a result, the implemented work offered a performance analysis based on network response (latency and transaction throughput). However, it does not take into consideration security analysis and privacy preserving performance.

Further, many works based on Blockchain and IoT have been done while it has some limitations related to security and privacy such in [14], [15], [16], [17] and [18]. However, several researches have been conducted to overcome and reduce security and privacy-related risks in an IoT environment by the mean of Blockchain, also Known as Blockchain 4.0. The work in [19] provides a taxonomy of security and privacy requirements for Blockchain-based Industry 4.0 applications. It categorized the security requirements into 4 different types: 1) Confidentiality, Integrity, Availability (CIA) Triad; 2) Authentication, Authorization and Accounting (AAA) Triad; 3) Securing Smart Contracts. The latter work is lately used to define the system prerequisites.

B. Contributions

Our paper proposes a blockchain-based system for access management in telehealth and telemedicine domain. The main purpose of this work is to build a patient-centric access management system that comply with GDPR regulations. Hence, it also aims to record all access management related data in an immutable ledger which gives more transparency over shared data. On the other hand, the Interplanetary File System (IPFS) is used to store patient's data. Indeed, the aforementioned key characteristics of blockchain technology drive us to use this technology for dynamic access management in telehealth and telemedicine sector. Further, blockchain is a suitable technology to mitigate the mentioned limitations in current telehealth and telemedicine systems. The proposed approach makes use of smart contract for more automated tasks, including managing healthcare providers' access to patient' data and detecting unauthorized access, as well as, add authentic nodes to the system network or ban fraudulent ones. To this end, we define the main enhancement of blockchain in telemedicine and telehealth sector as follows:

- **Security**: Blockchain can provide authenticity to data requestor, and ensure patient's data integrity, as well as data confidentiality.
- **Immutability**: It is one of the key features of Blockchain which provides a tamper-proof and time-stamped record.
- **Persistency:**. Blocks with invalid transactions could be figured out instantly. There is no way to delete or roll back recorded transactions.
- **Transparency**: All transactions related to access management are visible.

On the other hand, IPFS network ensures data availability and data integrity.

This work aims to make two contributions towards enhanced patient's privacy and security, which are shown below.

1) *The definition and presentation of the proposed system for patient-centric access management system using blockchain, as well as the design of the system, all possible algorithms that fulfill decision making mechanism.*
2) *The development and testing of the smart contract code including security analysis using Ethereum built-in environment and Oyente tool, as well as ensuring that the system is in compliance with GDPR regulations.*

III. System prerequisites

The telemedicine and telehealth systems present several security and privacy-related risks. Our purpose is to be focused on data sharing issues. To this end, the system must be in compliance with GDPR requirements on data protection. Below, an explanation of the system prerequisites in details.

A. Security

Security remains a major part of the system requirements, which involved to ensure trustworthiness over the system. To this end, following [19], the security prerequisites are listed as follows:

- **Confidentiality**: It aims to protect data from unauthorized access. Otherwise, it might compromise patient's privacy. It may happen that data can contain sensitive information about patient.
- **Integrity**: It prevents malicious agents from altering or changing stored data.
- **Availability**: The system should make data available to authorized users without failing or being inaccurate, even in case of a network attack.
- **Authentication**: This is the first security layer in the system since it verifies the user's identity.
- **Authorization**: This denotes that access to data is based on prior authorization from data owner.
- **Nonrepudiation**: This is a crucial requirement for the system, where all users in the system cannot deny a performed transaction.
- **Accountability**: This is a critical security requirement where users can act as adversaries in the network including unauthorized data usage. Moreover, accountability enables data owners to monitor unlawful access to their data.

B. Privacy

The GDPR [5] requires that certain prerequisites must be satisfied before data access is granted:

- **Unambiguous:** This indicates that a clear affirmative action must be used to give access.
- **Informed**: This denotes that the data owner has detailed information about data usage.
- **Freely given:** Willingly given and without being forced. The data owner needs to be aware of every possible effect related to data access.
- **Specific**: Requests for access must be specific with a clear objective. As a result, the data owner must be fully informed of the reasons behind and procedures followed when accessing their data.
- **Auditable:** All access-related data must be recorded in order to be audited in the future and afterwards utilized as legal proof.
- **Withdrawable:** Data owner can withdraw a previously granted access at any time.
- **Explicit:** Access should be informative, and for what purpose is requested and what data is demanded.

C. Transparency

It is one of the key prerequisites for any transparent system. It ensures that all users activities are lawful. Otherwise, it may affect patient's privacy. Further, patients must have information about all activities regarding access to their data after granting access to other users. To address transparency, this system aims that every single activity related to data access is stored permanently and accessible at any time.

IV. System architechture

In this section, we provide the system design and define the system' participants, as well as all possible algorithms that automate storing and sharing health-related data process.

A. Participants

The system has three main actors, provided as follows:

- **Regulatory Authority (RA):** RA checks user's identity and provides trusted users in the system. RA can also reject users from the network if they perform unlawful actions.
- **Patient:** Patient is the data owner who grants access to his data.
- **Healthcare provider (HP):** HP can be a healthcare professional, hospital or Laboratory who can request access to patient's data.

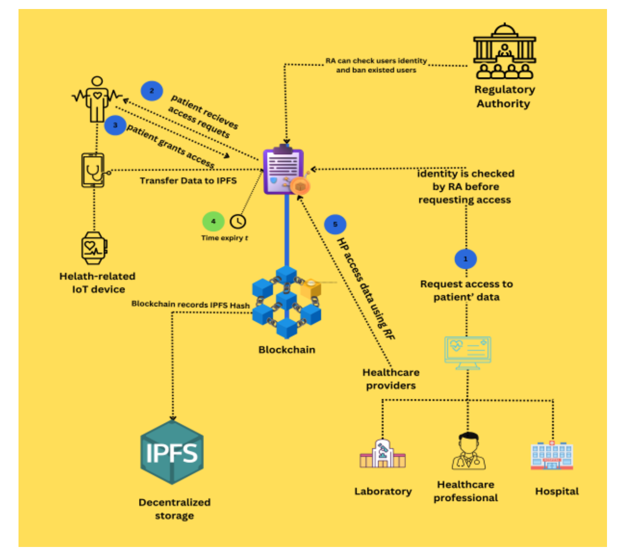

RA can check users identity and ban existed users
Regulatory Authority
2
patient recieves access requets
3
patient grants access
Transfer Data to IPFS
identity is checked by RA before requesting access
4
Time expiry t
5
HP access data using RF
1
Request access to patient' data
Helath-related IoT device
Blockchain records IPFS Hash
Blockchain
Healthcare providers
IPFS
Decentralized storage
Laboratory
Healthcare professional
Hospital

Figure 1. system architecture.

B. Smart Contract design

In this section, we discuss the proposed algorithm that are designed to securely automate the health-related data storing and sharing. To this aim, the system design contains five Algorithms as follows:

1) ***Algorithm 1****:* It checks the identity of healthcare providers at first place. In addition, Regulatory Authority (i.e, Healthcare Ministry) is the smart contract owner. RA can add new users to the system or ban existed users.

2) ***Algorithm 2****:* It has two main functions, the first one enusres the authenticity of health-related data transferred to the decentralized storage database. The algorithm 3's input parameters are IPFS hash, time and date when data is measured and data hash. The second function enables Healthcare providers to check the authenticity of shared data.

3) ***Algorithm 3***: It enables healthcare provider to request access health-related data from patient. It also enables patient to grant access for a period of time ***t*** or reject the request.

4) ***Algorithm 4****: It* automatically withdraws granted access once ***t*** is expired. Therefore, access becomes unallowed. It also enables patient to withdraws a granted access.

5) ***Algorithm 5****:* It checks the validity of accesing data based on patient's granting decision. It enables the system to detect unlawfull access to data.

Note: The health-related devices are connected to the patient's smartphone using Bluetooth. The smartphone has the patient' blockchain account.

C. System process

ALGORITHM 3 Request health-related data from patient.

```
Input:
    • User information, (i.e, The occupation: Doctor or nurse,
      The medical institution that he belongs to, etc.);
    • The purpose of requesting data;
    • Expiration time t;
    • Nature of requested data.

Unique number is a number that solely refers to a granted access
Duration refers to a period of time when a granted access is valid

If(BannedUser == False) then
If(Access == Granted ) then
        RF = unique number;
        t= duration;
        Emit an event declaring that the healthcare provider can access
        to patient's data for a period of time t with access reference RF.
Else if (Access == Rejected) then
        Emit an event  declaring that the healthcare provider is not
        allowed to access patient's data.
End if
End if
```

As depicted in Figure 1, the system has one regulatory authority RA which validates the healthcare provider identity, once the healthcare provider requires to join the network. This process is done via Algorithm 1. Once the healthcare provider joins the network, they are able to request health-related data from patient via Algorithm 3. They are called to inform the patient about the purpose of requesting such data, nature of data (i.e, Blood glucose level, Blood pressure, etc.), time ***t*** required, and some other information related to healthcare provider identity (i.e, the occupation: doctor or nurse, the medical institution that he belongs to, etc.). Then, patient can grant access for a period of time ***t***, and the healthcare provider gets a reference number ***RF*** for the granted access. ***RF*** is used by Algorithm 5 to verify the validity of the access when the user tries to access data. Further, if Algorithm 5 detects unlawful access from the healthcare provider, it reports that to RA. Then, RA can decide to ban the user from the network. Further, the patient can at any time revoke the granted access via Algorithm 4.

Moreover, once data is measured using health-related device, the patient' smartphone transfers data to ***IPFS*** network and gets IPFS hash using Algorithm 2. The IPFS hash is stored on blockchain with time and date when data is measured and data hash (to ensure data integrity).

Note: All the actions performed by the users are stored on Blockchain.

ALGORITHM 4 Manage access status.

```
Withdraw: Patient initiates a transaction to withdraw access to
healthcare provider or time is expired;
Input:
    • Expiration time t;
    • RF.
If( (t == 0) or (withdraw == true)) then
        Emit an event the healthcare provider becomes unallowed to
        access to patient' data with reference RF.
Return false.
Else If( (t != 0) & (withdraw == false)) then
        Emit an event the healthcare provider is still allowed to access
        patient' data;
Return true.
End if
End if
```

ALGORITHM 5 Check validity of access.

```
Access patient's data after granted access: The healthcare provider
initiates transaction
Input:
    • Algorithm 4's output;
    • RF.

If( (Access == Granted ) & (Algorithm 4's output == true) then
        Emit an event the healthcare provider is accessing patient' data
        with RF.
Else if((Access == Revoked ) & (Algorithm 4's output == false) then
        Emit an event the healthcare provider tries to access data
        unlawfully. (RA gets notifieds)
End if
End if
```

V. Discussion

A. Testing setup & Security analysis

The smart contract code is written in solidity programming language [20] and tested using Remix IDE which is a no-setup tool with a GUI for developing Ethereum smart contracts [21]. In our scenario, every participant has an Ethereum address and the Regulatory Authority is smart contract owner.

In addition, The code is tested using Remix IDE which enables smart contract developers to detect some vulnerabilities in code such as Re-entrancy, Authorization through tx.origin, Low-level calls, Self-destruct, and In-line assembly use. However, this built-in security analysis is not far enough to develop a proper code in order to avoid security threats. Further, Oyente [22] is one of the security analysis tools that detects security vulnerabilities in Ethereum smart contract code and Ethereum Virtual Machine EVM bytecode and ensure that code is free of bugs [23]. Oyente conducts a deeper analysis over security vulnerabilities including integer underflow, integer overflow, transaction ordering dependency, and timestamp dependency. As a result, it reports back the result with the EVM coverage and the aforementioned vulnerabilities. Figure 2 shows the analysis result of our smart contract with a high EVM coverage and undetected vulnerabilities (False).

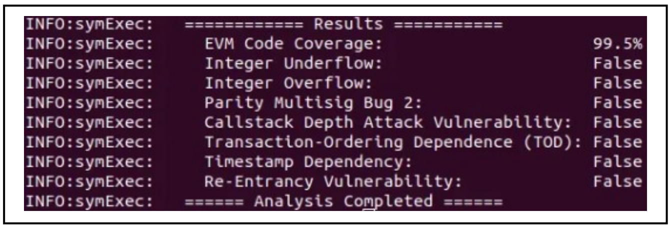
In addition, the key-characteristics of blockchain contribute positively to achieve the aforementioned system prerequisites. Moreover, immutability ensures data integrity and nonrepudiation, because all transactions are stored permanently and no one can deny a performed transaction. On the other side, accountability is ensured since data is stored permanently. Moreover, data is stored in a distributed ledger which means that every node has a copy of the ledger. As a result, it satisfies the availability requirement.

Further, confidentiality, authorization and authentication prerequisites are satisfied through Algorithm 1, Algorithm 2 and Algorithm 3 defined above.

B. *Compliance with GDPR regulations*

In this part, we discuss the compliance of our proposed system with the GDPR regulations:

- **Unambiguous:** Algorithm 3 and Algorithm 4 ensures that the granted access is given for a period of time ***t***.
- **Informed**: Algorithm 3 ensures that the patient has enough information for what purpose data is used and the identity of who requested access.
- **Freely given:** Algorithm 3 ensures that the patient has the right to reject the access request.
- **Specific**: Algorithm 3 enables patient to get informed of data nature is demanded and for what purpose. On the other hand, Algorithm 5 enables patient to know when data is accessed and who accessed to data.
- **Auditable:** All performed transactions are recorded on blockchain, and can be accessible at any time.
- **Withdrawable:** Algorithm 4 enables the patient to withdraw access at any time, while Algorithm 5 ensures that given access remains valid only for a period of time ***t***.
- **Explicit:** Algorithm 3 ensures that the patient is informed of data nature requested.



```
INFO:symExec:   ============ Results ===========
INFO:symExec:     EVM Code Coverage:                      99.5%
INFO:symExec:     Integer Underflow:                      False
INFO:symExec:     Integer Overflow:                       False
INFO:symExec:     Parity Multisig Bug 2:                  False
INFO:symExec:     Callstack Depth Attack Vulnerability:   False
INFO:symExec:     Transaction-Ordering Dependence (TOD):  False
INFO:symExec:     Timestamp Dependency:                   False
INFO:symExec:     Re-Entrancy Vulnerability:              False
INFO:symExec:   ====== Analysis Completed ======
```

Figure 2. Oyente security analysis tools.

To this end, our system is in compliance with GDPR regulations.

VI. Conclusion

In this paper, we proposed a patient-centric approach for health-related data sharing in telehealth and telemedicine domain. It is a blockchain-based access management system that relies on patient decision to grant or revoke access. This system stored all access-related data on blockchain which ensured transparency and immutability. We used Ethereum built-in environment to develop and test our smart contract, and Interplanetary File System (IPFS) to store patient's data. We conducted a security analysis to our smart contract code using Oyente tool. As a result, our smart contract is sufficiently secure against common security vulnerabilities including integer underflow, integer overflow, transaction ordering dependency, and timestamp dependency. Further, our access management system proved compliance with GDPR regulations. In addition, our system results proved security prerequisites including data integrity, nonrepudiation and confidentiality, authentication and authorization.

References

[1] A. E. B. Tomaz, J. C. D. Nascimento, A. S. Hafid and J. N. De Souza, "Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof and Blockchain," in IEEE Access, vol. 8, pp. 204441-204458, 2020, doi: 10.1109/ACCESS.2020.3036811.

[2] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives," in Journal of Food Quality, Hindawi, volume 2021. https://doi.org/10.1155/2021/7608296.

[3] C. Chen, S. B. Goyal, K. Ramaswamy, "BSPPF: Blockchain-Based Security and Privacy Preventing Framework for Data Middle Platform in the Era of IR 4.0," in Journal of Nanomaterials, vol. 2022, Article ID 2219006, 14 pages, 2022. https://doi.org/10.1155/2022/2219006.

[4] B. Houtan, A. S. Hafid and D. Makrakis, "A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare," in IEEE Access, vol. 8, pp. 90478-90494, 2020, doi: 10.1109/ACCESS.2020.2994090.

[5] General Data Protection Regulation GDPR, (EU) 2016/679, [Online]. Available: https://gdpr-info.eu/issues/consent/.

[6] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed. Elsevier, 2015.

[7] E. Zaghloul et al., "Bitcoin and Blockchain: Security and Privacy," https://arxiv.org/pdf/1904.11435.pdf/.

[8] V. Buterin, "A next-generation smart contract and decentralized application platform," White paper, 2014.

[9] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," 2014. [Online]. Available: https://arxiv.org/abs/1407.3561.

[10] RW. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The role of blockchain technology in telehealth and telemedicine," in International journal of medical informatics vol. 148 (2021): 104399.

[11] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," in Neural Comput. Appl. 34, 14 (Jul 2022), 11475–11490. https://doi.org/10.1007/s00521-020-05519-w.

[12] K. Sheela, and C. Priya, "Blockchain-based security & privacy for biomedical and healthcare information exchange systems, " Materials Today: Proceedings, Volume 81, Part 2, 2023, Pages 641-645.

[13] F. Jamil, S. Ahmad, N. Iqbal, and D. Kim, "Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals," Sensors 20, no. 8: 2195. https://doi.org/10.3390/s20082195.

[14] O. Attia, I. Khoufi, A. Laouiti and C. Adjih, "An IoT-Blockchain Architecture Based on Hyperledger Framework for Healthcare Monitoring Application," 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 2019, pp. 1-5, doi: 10.1109/NTMS.2019.8763849.

[15] H.-N. Dai, M. Imran, and N. Haider, "Blockchain-enabled Internet of Medical Things to combat COVID-19," IEEE Internet Things Mag., vol. 3, no. 3, pp. 52–57, Sep. 2020.

[16] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortifiedchain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control, " IEEE Internet Things J., vol. 8, no. 14, pp. 11717–11731, Jul. 2021.

[17] B. A. Y. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna, and K. Shankar, "Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things environment," Pers. Ubiquitous Co., pp.1–11, Feb. 2021, doi: 10.1007/s00779-021-01543-2.

[18] Jia Qu, "Blockchain in medical informatics," in Journal of Industrial Information Integration, Volume 25, January 2022, doi: 10.1016/j.jii.2021.100258.

[19] K. Hameed, M. Barika, S. Garg, M. Bilal Amin, B. Kang, "A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues," in Journal of Industrial Information Integration, Volume 26, March 2022, doi: 10.1016/j.jii.2021.100312.

[20] Solydity [Online]. Available: https://docs.soliditylang.org/en/v0.8.21/.

[21] Remix IDE [Online]. Available: https://remix.ethereum.org/.

[22] Oyente [Online]. Available: https://github.com/enzymefinance/oyente.

[23] M. Debe, K. Salah, R. Jayaraman, I. Yaqoob and J. Arshad, "Trustworthy Blockchain Gateways for Resource-Constrained Clients and IoT Devices," in IEEE Access, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3115150.