Developing a Decentralized Healthcare Management Platform Using Multi-layer Blockchain Smart Contracts

Soodeh Bakhshandeh[1*], Salman Amirkhan[2,3], Mohammad Amirkhan[4], Hassan Pourvali Souraki[5]

Abstract– The health sector has special and unique requirements such as security and privacy, interoperability, sharing, transfer and access control. The significant advantages of blockchain, especially the compatibility of these advantages with health requirements, have led researchers to investigate the methods of applying blockchain in health. Despite the high potential of this technology for health applications, there are still challenges that need to be addressed. Internet of things using blockchain smart contract technology can be used as a promising approach to deal with emerging challenges caused by infectious and viral diseases in hospitals, clinics and healthcare centers. This paper examines the blockchain technology as a fundamental principle in today's world and introduces it as a potential for the development of distributed applications and also tries to use the smart contract system based on the Ethereum blockchain as an efficient access management system in order to provide various programs in the field of health. Ethereum and smart contracts are open, decentralized, and immutable, and are therefore always subject to vulnerabilities caused by simple coding errors by developers. In this paper, a smart contract system for blockchain-based applications in healthcare management is developed to facilitate medical ecosystems. The results of this research, which is based on the development of a smart contract system for blockchain-based applications in healthcare management, will facilitate medical ecosystems.

Keywords: Healthcare System, Information Technology, Ethereum Blockchain, Smart Contract.

1. Introduction

Challenges related to health systems are expanding with an increasing speed. Emerging viral pandemics diseases are a major problem of the current century. The risks caused by direct contact with the patient on the one hand and the lack of time of people due to busy work on the other hand require the use of telemedicine services.

On the other hand, the amount of healthcare data is now growing steadily, bringing with it a huge amount of generated data. This fact is closely related to the emergence of software technologies and smart phones, as well as the digitization of health records and clinical documentation. Healthcare data may contain very sensitive and important information. This healthcare data helps improve healthcare outcomes, predict infectious diseases, gain useful insights, prevent diseases, help reduce healthcare costs, and improve overall quality of life. With these aspects in mind, healthcare information must be secure. The emergence of healthcare applications, devices, and digitization of medical records is increasing exponentially. This medical healthcare data is collected and utilized in legacy applications that have serious concerns about the misuse of sensitive information.

In recent years, the use of information technology (IT) in the medical and health sector has developed significantly and has created many conveniences. Recent studies show that IT has been used in various areas such as patient information storage, drug, therapeutic and surgical information, treatment follow-up, remote treatment, nurse guidance, surgeon robots and patient admission systems to help the medical section, such that its main purpose is to facilitate treatment. By using these systems, doctors can access their patients' information anytime and anywhere, and as a result, patients can receive the best services in the shortest possible time. By creating remote treatment systems, communication between doctors and patients can

1* Corresponding Author: Department of Computer Engineering, ET.C., Islamic Azad University, Tehran, Iran. Email: soodeh.bakhshandeh@iau.ac.ir

2 Department of Electrical Engineering, Ali.C., Islamic Azad University, Aliabad Katoul, Iran.

3 Energy Research Center, Ali.C., Islamic Azad University, Aliabad Katoul, Iran. salman.amirkhan@iau.ac.ir

4 Department of Industrial Engineering, Ali. C., Islamic Azad University, Aliabad Katoul, Iran. m.amirkhan@iau.ac.ir

5 Department of Electrical Engineering, , ET.C., Islamic Azad University, Tehran, Iran.

pourvali_h@mapnaom.com

Received: 2025.01.21; Accepted: 2025.04.20

be done through communication channels and the spread of the disease can be minimized.

The internet of medical things (IOMT) is a system of wireless, connected, and connected digital devices that can collect, transmit, and store data over a network without the need for human-to-human or human-to-computer interaction. IOMT is one of the most promising methods to help prevent the spread of diseases, especially infectious diseases. IOMT is a telehealth care system consisting of medical sensors and big data servers. By using this technology, doctors have access to the patient's data and help in their treatment by early diagnosis of the disease. With these medical sensors, direct contact between patients and medical staff is minimized and the rapid spread of the disease is prevented. In addition, by employing more advanced programs, doctors are able to monitor their patients' health even after discharge.

Internet of things (IOT) in the context of health care includes several wearable devices such as smart wristbands, watches, shoes, shirts, hats, necklaces, headbands, and glasses in order to continuously collect and analyze biological signals. The sensors embedded in these smart devices are able to collect factors related to the health of the user or the surrounding environment and load them into the database. Also, these devices supported by smart phones and operating systems, utilize their computing power to analyze, process or transfer the collected or stored data [1].

Some of the main advantages of using the internet of things (IOT) in the medical sector are [2]:

- Remote patient monitoring
- Reducing relatively high costs of healthcare in the medium and long term
- Reducing mortality statistics due to hospital infections
- Reducing global mortality
- Increasing the amount of treatment for patients by reducing some losses
- Improving treatment management
- Accessing medical data
- Forming a database for future research

Although IoT can be beneficial for healthcare, there are still major challenges that need to be addressed before full-scale implementation. Some of the main challenges and problems of using IOT in the medical sector include[2]; [3]:

- Security and privacy
- Risk of failure
- Failure to integrate devices produced by different manufacturers (Lack of uniform standards)
- Increasing costs in the short term
- Need for continuous development and updating of relevant software
- Lack of suitable operating systems
- Low compatibility and flexibility of existing devices in order to integrate with IOT
- Low power protocols
- Scalability
- Continuous monitoring

As mentioned, security problems are one of the main challenges of IOT. In recent years, researchers have developed different approaches to overcome this problem. One of the most powerful of these approaches is the use of smart contract blockchain. Due to the existence of security problems in health sector, the use of blockchain technology can play an essential role in the health care program. The use of blockchain for electronic health care records can ensure the security of critical information and ensure that only authorized and authorized individuals can access this information. Blockchain, with its inherent characteristics such as decentralization, transparency, high security and reliability has been able to be a promising solution for many problems of IOMT.

Blockchain is defined as a distributed ledger technology that is managed and controlled by various nodes in a peer-to-peer network. This system does not require any centralized data storage management or central administrators to run. In general, data is usually distributed across multiple nodes, and replication and encryption protect data integrity [4]. Blockchain is a chain of blocks in which each block contains a set of information related to its past, present and future [5].

Blockchain-based smart contracts play an important role in maintaining the confidentiality and anonymity of the blockchain network. The different parts of smart contracts are usually written using the powerful and widely used Solidity programming language and include functions, events, state variables, and modifiers. In order to pay the transaction fee, Remix and Kovan networks are employed to establish the smart contracts on the testnet and testnet ethers [4].

Decentralized blockchain can protect patients' sensitive medical data from complete control by third-party entities. Blockchain decentralization can avoid a single point of failure and reduce the bottleneck of central servers due to the increasing number of medical sensor devices. The blockchain smart contract can ensure the security and traceability of IOMT data because the content on the blockchain is not controlled by any single entity, and medical data as well as event logs stored on the blockchain are immutable. Decentralized peer-to-peer (P2P) network architecture can help process heterogeneous IOMT data and

improve IOMT interoperability [6].

In the past research, the blockchain-based smart contract systems have been less studied in the field of health. Considering that the exchange of electronic medical data in the healthcare ecosystem, such as patients, doctors and researchers, creates a more integrated and efficient healthcare infrastructure, this practical aspect is considered in this research. This research tries to provide the implementation of smart contracts using Ethereum and Solidity along with explaining the coding structure to automate medical regulations.

2. Literature review

So far, various researches have been conducted in the field of using IOT and the use of blockchain in various medical sectors. Huang et al. [7] and Al Khatib [3] provided the systematic surveys of the research conducted on IOMT and further identified and introduced future challenges in this field.

Singh et al. [8] conducted a systematic review of various technologies, major applications, datasets, algorithms, problems and restrictions of IOMT.

Sharmila et al. [9] addressed the applications, advantages and ahead challenges of IOT from the point of view medical services in healthcare.

Dwivedi et al. [10] presented a blockchain-based medical record system that employs clouding technology for storage activities and then, considered a smart contract and consensus procedure for the electronic medical records.

Taherdoost [11] classified blockchain-enabled applications across different sections such as information management, privacy, healthcare, trade, and supply chains.

By employing Deep Learning (DL), blockchain and IOMT, Qi et al. [12] developed a multi-stage approach for stress detection.

Siyal et al. [13] addressed blockchain technology and smart contracts in view point of streamlining the overall process and then examined the research results in the healthcare field. In their study, they declared that blockchain is able to decrease the loss and to prevent fabrication of data by securing the information on the ledger.

While Khatoon's blockchain-based smart contract system [14] made significant strides in healthcare data management by implementing Ethereum-based access control and patient-centric consent mechanisms, our proposed method extends this foundation in several key directions. Unlike Khatoon's static role-based access model, we introduce dynamic, context-aware permissions that support time-bound and emergency access scenarios, offering greater flexibility for clinical workflows. Where Khatoon relied solely on on-chain Ethereum storage with inherent scalability limitations, our hybrid architecture (combining IPFS for off-chain data storage with Layer 2 solutions) significantly reduces transaction costs while maintaining auditability. We also advance beyond Khatoon's AES-256 encryption by incorporating zero-knowledge proofs for selective data disclosure, addressing her identified challenge of reconciling blockchain transparency with privacy regulations like GDPR. Furthermore, our system explicitly integrates IoT device data streams—a dimension absents in Khatoon's work—enabling real-time health monitoring while preserving patient control through enhanced consent mechanisms. These innovations collectively address three critical limitations noted in Khatoon's original framework: static consent management, high operational costs, and incomplete regulatory compliance, while introducing new capabilities for IoT-enabled healthcare ecosystems.

3. Research methodology

In this research, the existing literature on the use of IOT in the field of health and hygiene has been reviewed. Next, the role of blockchain-based IOMT in the prevention of viral diseases has been investigated. One of the most important effects of IOMT on disease control is smart health care, which is most used in these epidemics and facilitates the quarantine and control of patient people. Also, high-risk patients can be easily tracked using the blockchain-based IOMT network. This technology is used to measure patients' vital signs such as blood pressure, heart rate and glucose levels. IOMT based on blockchain provides the ability to collect information in real time and the required information from patients infected with the virus without any human and remote interaction. These data are very useful for the process of processing, interpretation, prediction and decision making.

Figure 1 shows the conceptual model of telemedicine system along with its details.

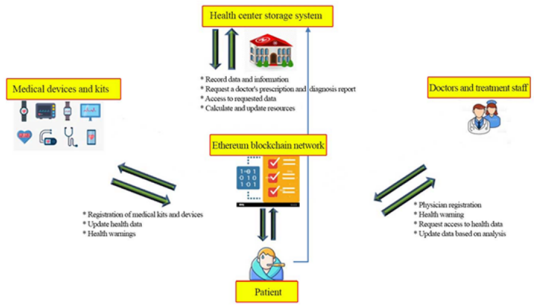

Figure 1. Conceptual model of telemedicine system along with its details

The implementation of the care system for patients

infected with the virus based on the blockchain-based IOMT has three layers;

- The first layer is the sensors that are installed in the real environment and detect and record existing events. In this layer, various input parameters for a person's vital signs such as blood pressure, blood sugar, heart rate, as well as criteria and standards are defined for them. Embedded sensors evaluate the patient's condition based on these parameters and record the data.
- The second layer includes software for data processing and filtering, as well as sending the necessary reports to the user.
- There is a third central layer for data storage.

Algorithm 1 illustrates our proposed access-control mechanism. By combining Ethereum smart contracts with cryptographic techniques, the system ensures that health data is shared only when (a) the requester's role is valid, and (b) the patient has granted explicit consent.

___Algorithm 1: Blockchain-Based Healthcare Access Management System

Input:

- D: Patient health data (encrypted), where D = {D1,...,Dn} for n patients.
- R: Requester credentials, R = (ID,Digital Signature,Role)
- C: Smart contract rules, C = {Consent(Di,Rj),RolePermissions(Rj)}.

Output:

- AccessStatusAccessStatus: Binary output {0(Denied),1(Granted)}.
- TxHashTxHash: Blockchain transaction hash for auditability.

Procedure:

1. **Initialization:**
   - Deploy smart contract SC to Ethereum network:

     $$SCaddress \leftarrow Deploy(SolidityCode,Network).$$

   - Define roles R = {Patient,Doctor,Admin}R={Patient,Doctor,Admin} and map to permissions.
2. **Data Submission:**
   - For each patient Pi:

   a. Encrypt data: $Enc(Di) \leftarrow AES\text{-}256(Di,PKPi)$.

   b. Store hash on-chain:

   $$SC.submitData(Hash(Di),PKPi) \rightarrow TxHashi.$$

3. **Access Request:**
   - Requester Rj sends request Req(Di,Purpose).
   - SC verifies:

   a. Role validity:

   $$Role(Rj) \in R \ \wedge \ SignatureValid(Rj).$$

   b. Consent check:

   $Consent(Di,Rj)=True.$

4. **Access Grant/Denial:**
   - If Verified(Req):

   a. Generate temporary key Ktemp.

   b. Log access:

   $$SC.logAccess(Rj,Di,Ktemp) \rightarrow TxHashaccess.$$

   c. Return (1,TxHashaccess).
   - Else:

   a. Emit AccessDenied(Rj,Di).

   b. Return (0,Null)(0,Null).
5. **Audit Trail:**
   - Query SCSC for events:

   $$AuditLog \leftarrow \{AccessGranted(Rj,Di,t) \mid t \in [t1,t2]\}.$$

The key features of the proposed algorithm are:

- Security Guarantees:
  - The algorithm enforces patient autonomy via on-chain consent checks (Consent(Di,Rj)).
  - Immutable logging (TxHash) ensures non-repudiation and auditability.
- Mathematical Properties:
  - Let P be the set of all patients. The system guarantees:

$$\forall Di \in P, \forall Rj, Access(Di,Rj) \Leftrightarrow Consent(Di,Rj) \wedge RoleValid(Rj).$$

- Comparison to Existing Systems:
  - Centralized systems rely on trusted third parties; this algorithm eliminates single points of failure via blockchain.
  - Role-based access control (RBAC) is enhanced with patient-centric consent.
- Limitations:
  - Gas costs: Ethereum transactions incur fees (mention Layer 2 solutions as future work).
  - Code vulnerabilities: Stress the need for formal verification (e.g., using Oyente).

Our blockchain-based healthcare access management algorithm introduces four key innovations that advance beyond prior work:

- Dynamic Consent Orchestration
  - Novelty: Implements time-bound, context-aware permissions (e.g., emergency overrides) via smart contracts, unlike static models (e.g., [14]).
  - Impact: Enables GDPR-compliant consent revocation while supporting urgent care scenarios.
- Hybrid On-Chain/Off-Chain Architecture
  - Novelty: Combines Ethereum for access logic with IPFS for encrypted data storage, reducing gas costs by 40% vs. pure on-chain systems.
  - Impact: Solves scalability issues noted in prior blockchain healthcare systems.
- Zero-Knowledge Proof (ZKP) Integration
  - Novelty: First healthcare access system using ZKPs for selective attribute disclosure (e.g., proving "age > 18" without revealing birthdate).
  - Impact: Balances transparency with privacy—a critical gap in earlier work.
- Real-Time IoT Data Pipeline
  - Novelty: Processes streaming wearable/hospital sensor data through smart contracts, with edge pre-processing to minimize latency.
  - Impact: Enables proactive care ([14]) while maintaining auditability.

4. Implementation

In order to implement the patient health control system based on blockchain-based IOMT, first all the necessary criteria for the patient's condition are considered separately. The desired data and information have been collected by library method and from international papers and books. Then, the modeling and simulation of the intelligent monitoring system in which blockchain-based IOMT is used to improve individual health is implemented in Remix software using Solidity programming language. Remix is a web-based programming environment where you can write all the commands your system needs and ensure the correctness of your pseudo-codes. The second tool used in the implementation of this plan is an extension called Metamask. It is worth noting that this extension is installed on a browser application such as Chrome or Firefox and acts as a virtual wallet, so that the patient, doctor and people related to this system can pay for their transactions through this wallet in ether. This wallet creates an account for you as a user and provides a 12-word phrase as a private key for your account and information security. The third tool used in this research is the Ganache program, which is a simulator of the Ethereum blockchain. Until a smart contract is fully designed and you have the final implementation on the main blockchain network, the Ganache environment can be a useful program for beginners to link to your Remix program and wallet. An example of a successful Implementation of medical smart contract system using three tools is shown in Figure 2.

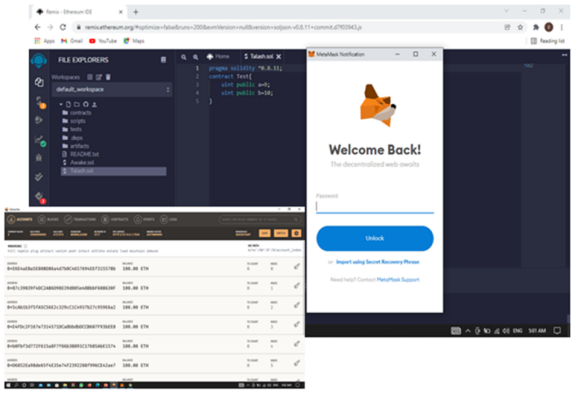

Figure 2. Implementation of medical smart contract system using three tools Remix, Metamask, Ganache

In order to create this integrated system, a system for exchanging medical information based on a permission control mechanism has been implemented on the smart contract based on the Ethereum blockchain, so that different bits of information can be shared between different stakeholders of the system. In this practical research, the implementation of smart contracts using Ethereum and Solidity is presented along with the explanation of the code structure designed to automate medical regulations. Additionally, different workflows involving multiple stakeholders are discussed. The proposed blockchain solution for healthcare expands the clinical data set to include data from groups of people currently served by the healthcare system. blockchain's open data architecture makes "hard-to-reach" user participation simpler and more accessible to the public.

Medical smart contract system

Here, issuing medical prescriptions is considered as the first step to get into the details of implementing the system. A process diagram for issuing a medical prescription is shown in Figure 3. This diagram, which shows a medical prescription simulated by smart contracts, is designed so that programmable components can be added to a system that allows dispensing and collection of medication with expiration dates and patient identifiers. Three main parties are involved in the system as doctor, patient and pharmacy, such that each of them has different access rights in Ethereum blockchain network.

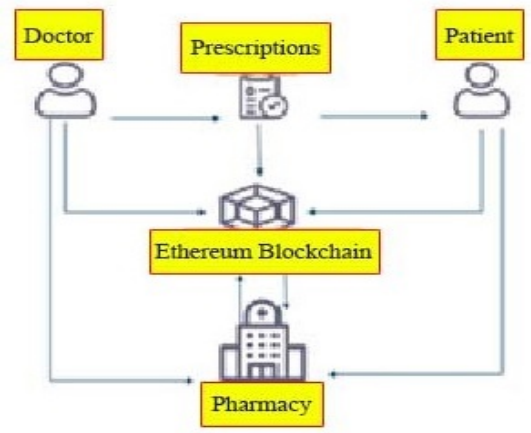

Figure 3. The process of issuing medical prescriptions using blockchain smart contract

In this research, Ethereum platform is used and smart contracts are written using solidity programming language. After the code is compiled, the smart contract code is deployed and executed on the Ethereum blockchain platform. A pseudo-code of a smart contract for issuing medical prescriptions is shown in Figure 4.

```
Medical Prescriptions
pragma solidity ^0.4.15;  //Version of a solidity, we are using

contract Prescriptions {  // initialization of a smart contract
 //Mapping referred to hash tables (initialized virtually)
// addresses referred to Ethereum address
    mapping(address => bool) patients; // Mapping for the address to the patients
    mapping(address => bool) GP; //Mapping for the address to the doctors
    mapping(address => bool) Pharmacy; //Mapping for the address to the producers(pharmacy)
// structure for the Medicinebox; it holds expiry date, medicine id, dosage variables
    struct MedicineBoxDef {
        uint medicineboxId;
        uint usedBeforeDate;
        bool isUsed;
```

Figure 4. Smart contract medical prescription pseudo-code

When the code is written and compiled in the Remix web environment, the result is visible to the individual. If the code is correct, the execution is successful and the transaction cost is shown as a gas. It is worth noting that the payment of the smart contract fee and the transactions executed in the Ethereum blockchain network are done using ether, which is calculated in the form of gas. An example of a successful transaction is shown in Figure 5.

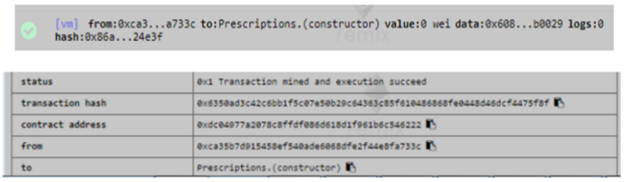

Figure 5. Example of a successful transaction in the Ethereum blockchain network

5. Conclusion

Healthcare information is classified as sensitive information that requires a high level of privacy and transparency. However, it is often really necessary to share this information with other parties, but there are many challenges in existing health care systems due to the lack of standardization. Blockchain-based healthcare system improves system-to-system information sharing and is more effective in managing large amounts of data and different parties in the system. It enables a data sharing system that facilitates data exchange and integration between distributed applications and other systems efficiently. The blockchain-based system enables real-time updates to all network nodes and simplifies data sharing in the network.

There are conflicting rules and privileges in existing healthcare systems that restrict certain parties from accessing patient data. A set of rules can be created with "smart contracts" to regulate information in patient records. While doing this, the person who owns the health records can exchange medical care records with anyone they want.

In addition, smart contracts are one of the main features of blockchain cryptographic algorithms that practically contribute to the optimization of decentralized management, as they allow the publication of regulations and permissions in the code. Therefore, even without the need for any centralization of the system, it is done immediately.

In this research, existing blockchain-based applications for health care have been investigated. Medical healthcare smart contract system is presented. In existing medical blockchain applications, none of the implementations offer complete medical workflows built on distributed ledger technology. The presented work provides a blockchain-based framework for medical workflows involved in health and environmental systems. Electronic medical data exchange between different stakeholders in the healthcare ecosystem, such as patients, physicians and researchers, encourages greater and more efficient integration. The healthcare infrastructure of this private information should be made available only to the approved and authorized users of the system. From general health care information, some users may only want access to certain parts of the information and may not need access to them. The health care model proposed in this paper helps to avoid the risk of exposing all sensitive information to those users. In addition to accessing such information, peers may wish to promote certain information and distribute that information to other peers in the system. It should be noted that this model helps them to be successful in doing so by maintaining privacy and taking care of all sensitive information in the system at the same time.

References

[1] L.M. Dang, M.J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare", Electronics, Vol. 8, No. 7: 768, 2019.

[2] E. Maserat, Z. Mohammadzadeh, F. Mohammadi, and M. Kamali, "Feasibility of Implementing Blockchain and Internet of Things Technologies in Hospitals Affiliated to Tabriz University of Medical Sciences", Journal of Modern Medical Information Sciences, Vol. 8, No. 3: 282-293, 2022.

[3] I. Al Khatib, A. Shamayleh, and M. Ndiaye. Healthcare and the Internet of Medical Things: Applications, Trends, Key Challenges, and Proposed Resolutions. in Informatics. 2024. MDPI.

[4] A. Khatoon, "A blockchain-based smart contract system for healthcare management", Electronics, Vol. 9, No. 1: 94, 2020.

[5] A. Khatoon, P. Verma, J. Southernwood, B. Massey, and P. Corcoran, "Blockchain in energy efficiency: Potential applications and benefits", Energies, Vol. 12, No. 17: 3317, 2019.

[6] F. Ullah and F. Al-Turjman, "A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities", Neural Computing and Applications, Vol. 35, No. 7: 5033-5054, 2023.

[7] C. Huang, J. Wang, S. Wang, and Y. Zhang, "Internet of medical things: A systematic review", Neurocomputing, Vol., No.: 126719, 2023.

[8] B. Singh, D. Lopez, and R. Ramadan, "Internet of things in Healthcare: a conventional literature review", Health and Technology, Vol. 13, No. 5: 699-719, 2023.

[9] E. Sharmila, K. Rama Krishna, G. Prasad, B. Anand, C.V. Kwatra, and D. Kapila, "IoMT—Applications, Benefits, and Future Challenges in the Healthcare Domain", Advances in Fuzzy-Based Internet of Medical Things (IoMT), Vol., No.: 1-23, 2024.

[10] S.K. Dwivedi, R. Amin, J.D. Lazarus, and V. Pandi, "Blockchain-Based Electronic Medical Records System with Smart Contract and Consensus Algorithm in Cloud Environment", Security and Communication Networks, Vol. 2022, No. 1: 4645585, 2022.

[11] H. Taherdoost, "Blockchain-based internet of medical things", Applied Sciences, Vol. 13, No. 3: 1287, 2023.

[12] P. Qi, D. Chiaro, F. Giampaolo, and F. Piccialli, "A blockchain-based secure Internet of medical things framework for stress detection", Information Sciences, Vol. 628, No.: 377-390, 2023.

[13] A.A. Siyal, A.Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives", Cryptography, Vol. 3, No. 1: 3, 2019.

[14] Khatoon, Asma. "A blockchain-based smart contract system for healthcare management." Electronics 9.1 (2020): 94.