Smart and secure medical device gateway for managing patient recovery

Vijayaraja Rathinasamy, Paul Fromme, Krishnan Balasubramaniam, Prabhu Rajagopal

Vijayaraja Rathinasamy, Paul Fromme, Krishnan Balasubramaniam, Prabhu Rajagopal, "Smart and secure medical device gateway for managing patient recovery," Proc. SPIE 12488, Health Monitoring of Structural and Biological Systems XVII, 124881J (25 April 2023); doi: 10.1117/12.2659070

SPIE.

Event: SPIE Smart Structures + Nondestructive Evaluation, 2023, Long Beach, California, United States

Smart and secure medical device gateway for managing patient recovery

Vijayaraja Rathinasamy[a], Paul Fromme[b], Krishnan Balasubramaniam[a], Prabhu Rajagopal[a]
[a]Center for Nondestructive Evaluation, IIT Madras, Chennai 600036, INDIA;
[b]Department of Mechanical Engineering, University College London, WC1E 7JE, UK

ABSTRACT

Patients recuperating from orthopedic surgery require frequent monitoring and hospital visits with a wealth of personal medical data generated both on and off-site, making it challenging to maintain records. This paper discusses a secure blockchain-based data management software to enable safe remote access without compromising patient information. The BlockTrack software developed at our group will be customized to interface with modules for orthopedic recuperation monitoring. Modules can consist of ultrasonic bone health monitoring sensors, connected to relay nodes that can transmit patient data to the BlockTrack mobile app, which then intercepts the information to be stored securely on a cloud-based Blockchain network. Each record will have a unique ID enabled by Blockchain, for secure access and review of patient information by other parties, including doctors and pharmacists. Key findings are discussed with a goal to further develop this solution.

Keywords: Data Privacy, Blockchain Ecosystem, Medical Workflow, Healthcare, IoMT, Unique Health ID

1. INTRODUCTION

Chronic orthopedic patients require frequent hospital visits and regular vital checks and monitoring for doctors to validate their health condition diagnosis, resulting in sensitive and often digital personal data records. Electronic Medical records (EMRs) are generally difficult to construct because the existing electronic data collection sources are limited, and most devices are operated manually. Moreover, sensitive patient data stored in the cloud as EMR puts it at risk of violations such as technical and privacy breaches, potentially even leading to criminal acts such as tampering in rare cases. When such errors occur, and if the remote EMR software does not have the information properly backed up, privacy laws often give patients the right to examine or obtain a copy of their own health records and request corrections. Medical data security has thus become a necessity rather than a choice, empowering individuals to control disclosures of their personal health information.

1.1 Issues with current Electronic Health Record (EHR) systems

EHR systems play a very important role in improving care for patients. Despite being developed and improved over the years, issues such as a lack of standardization hinder interoperability between health institutions, since the records are not exchangeable digitally. Paper records have to be requested by the patient from a given health institution, and then have to be produced elsewhere. EMR departments in hospitals consist of medical staff converting physical records into digital counterparts by methods such as printing, scanning, and photocopying. These methods are inefficient since they require humans to convert a physical document into a digital format without making it machine readable. Patients do not have direct access to and control over their health records. Health records stored in the healthcare institutions are being used by other users such as researchers, analysts, and insurance agents without proper data transfer and management methodologies. Data security is a challenge, which has led to major data breaches and attacks on healthcare systems over the past years. Examples of this include data breaches by hackers, DDoS attacks, and others.

1.2 Literature review

Blockchains have been observed to be ideal databases for storing sensitive data securely, and there are multiple studies and proposals for the design and implementation of a blockchain-based health record management system. Several studies have appreciated the use of blockchains for managing consultation data as mentioned in (Schlatt et al. 2021), and others

Health Monitoring of Structural and Biological Systems XVII, edited by
Paul Fromme, Zhongqing Su, Proc. of SPIE Vol. 12488, 124881J
 · 0277-786X · doi: 10.1117/12.2659070

discuss the usage of federated blockchains for building an ecosystem for multiple organizations to work together (e.g., Rojo et al. 2021). These papers propose the use of layers of blockchains for maintaining security and privacy standards within the network. Literature also lays a strong emphasis on the high-level architecture of decentralized data management systems, but may fail at scale, as the authors have speculated, due to the sheer size of the data being transacted continuously on the network.

Integration of IoT elements into this EHR domain has been discussed in Azbeg, Ouchetto, and Andaloussi (2022), where continuous IoT data from devices is logged onto the blockchain database. This approach has been further continued to employ federated learning by employing the edge devices to take the computational load, and the IoT devices to collect data required for the learning model (Yuan et al. 2022). This paper briefs the use of DAG blockchains (directed acyclic graphs) for the higher layers, and also has been proven to be more efficient than typical blockchains. The security aspects of IoT ecosystems have been thoroughly studied (Palli, Mirza, and Chowdhry 2022), where multiple data vulnerabilities have been identified in an IoT-enabled health data ecosystem. The solution offered, however, is not patient-centric and does not encompass the health data ecosystem in its entirety. Our paper proposes a complete end-to-end solution for managing health records in a patient-centric manner from all data sources, and by managing all stakeholders, after thorough analysis of the above cited resources.

2. METHODOLOGY

2.1 Federated health record management system

A Federated Health Record System is a type of Electronic Health Record (EHR) system that allows multiple healthcare organizations to share patient health information while still maintaining control over their own data. Patient health records are stored in separate databases maintained by each participating healthcare organization, but they can be accessed by authorized providers across different organizations. The goal of a federated health record system is to improve the coordination and continuity of patient care by enabling healthcare providers to access a patient's complete medical history, regardless of where the patient received care. This can help avoid duplication of tests and treatments, reduce medical errors, and improve the overall quality of care.

In a federated system, patient health information is protected by strict privacy and security measures. Each healthcare organization maintains control over their own data and can choose which information to share and with whom. Patient consent is typically required before any health information is shared. One advantage of a federated health record system is that it allows healthcare organizations to maintain their own unique workflows and processes, while still enabling collaboration and information sharing.

However, federated health record systems can also present challenges with interoperability, data security, and privacy. Interoperability as an issue occurs due to having a federated system that requires all the partaking organizations to agree on a particular standard and use a common system for decision making. As for data security, a chain of regulations has to be built within the system, in order to build a secure protocol for transitions within the ecosystem and is a concern usually raised with health data transfers between multiple organizations within the system. Personal data privacy is a major concern in federated systems since the data created by patients is owned by health organizations and is shared to other organizations, without explicit access requests from patients in existing systems.

2.2 Health records and the notion of a personal health trajectory

A Personal Health Trajectory (PHT) is a concept that refers to an individual's unique pattern of health and illness over time (Rojo et al. 2021). A PHT takes into account a person's medical history, health behavior, social determinants of health, and environmental factors to create a comprehensive understanding of their health trajectory, as has been depicted in Fig. 1. A PHT can be used as a tool to help individuals and healthcare providers plan for future health needs. PHT can also be used to identify patterns and trends in population health, allowing public health officials to target interventions and prevention efforts more effectively. By analyzing the PHTs of a population, healthcare professionals can identify areas of high risk and implement interventions to prevent or mitigate future health issues.

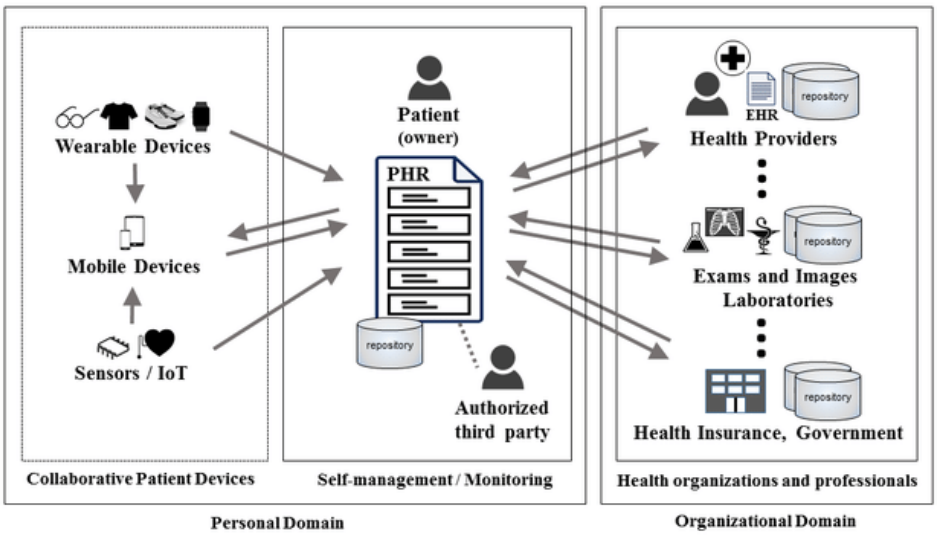

Figure 1. Schematic showing the data flow in a personal health record.

Advancements in technology, such as wearable devices and electronic health records, have made it easier to collect and analyze personal health data and create personalized health trajectories. As with any type of health information, it is important to ensure that PHTs are collected, stored, and shared securely and with the individual's consent.

2.3 A Consortium blockchain for building an FHR management system

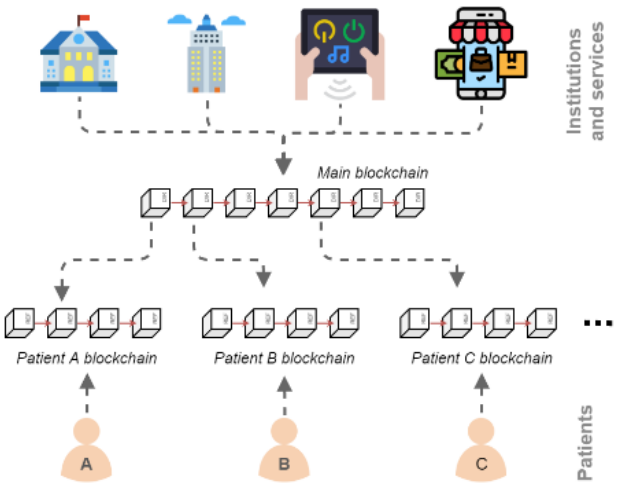

Figure 2. Schematic showing the concept of federated blockchains for storing health records.

The concept of federation of blockchains, as shown in Fig. 2, is the linking of low-level patient blockchains (referred to as ‘subchains’), to a high-level chain which consists of the routing record of all the patients in the network (referred to as ‘mainchain’). The patients’ blockchains are in charge of saving the information in the system. Each patient's blockchain is self-contained and can be considered and employed as a data structure independent of the federation. The key of the blockchains’ federation concept is that each of these blockchains stores the information of one patient. Patients can interact directly with their Personal Health Trajectory through their blockchain. In order to solve the problem of identity management, and to abandon duplication, the mainchain maintains a transaction for indexing the patient’s location with respect to the organizations on the network. Each institution has one node of the main blockchain, so that any change in the patients or in the location of their blockchains is noted by all institutions and services in the system. Nodes are added

to the patient's blockchain based on the visited institutions. Whenever a patient is visiting a new institution, a new node belonging to that institution will be added to the patient's blockchain, and a select node will be removed from the network, to reduce consensus time and keep the network responsive, but the number will be kept at a particular threshold keeping the security of the network in mind. The data is stored in off-chain storage services, and the transactions contain a link to the actual location of the storage of the data, which can be accessed only by authorized users (the patient and the institution which produced the data).

Finally, API resources will be created for people to interact and perform operations on the network. The API resources will be of delegated access to people with access to that particular resource, and can be implemented in smartphone, desktop applications, or web-based applications.

3. IMPLEMENTATION

3.1 Implementation of a multi-host blockchain network

Blockchain tools and traditional software components were put together to demonstrate some parts of the workings of a Federated Health Record Management system. Hyperledger Fabric is the blockchain framework that was used to set up the private blockchain, and back-end software programming was done using Node.js. Digital Ocean cloud servers were used to deploy the blockchain.

Blockchain networks are inherently capable of communicating over distributed systems and attain consensus over the transactions they are recording, i.e., computers present in various locations or different networks can pass to each other the transactional details they are handling, and all computers would still maintain the same copy of the history of transactions happening at these different locations, in an orderly manner.

Figure 3. Schematic showing a sample federated blockchain contract for user registration, and writing the basic details.

In this implementation, transactions refer to the patient-doctor actions such as User Registration, Appointment Booking, and Request for Patient Data Access. These actions are recorded in the blockchain ledger as transactions happening between a patient and a doctor, and the details are secured. Other transactions such as Sensor Data from medical devices can also be transmitted through the Blockchain network in a similar manner.

In Fig. 3, the register() function will register 'patient' and 'doctor' to the blockchain network. Here, the writeData() function is used by the patient to upload basic health data to the ledger. Only registered members can access this function.

3.2 Appointment booking - transaction flow

An explanation of the Transaction flow initiated from the Patient node - For Appointment booking as shown in Fig. 4 is given below:
Here,

- Patient(P) can be classified as the Client who belongs to Organization 1.
- Peer(P1) can be classified as the peer that can endorse or commit the transaction for Organization 1.
- Doctor(D) can be classified as the client who belongs to Organization 2.
- Peer(P2) can be classified as the peer that can endorse or commit the transaction for Organization 2.

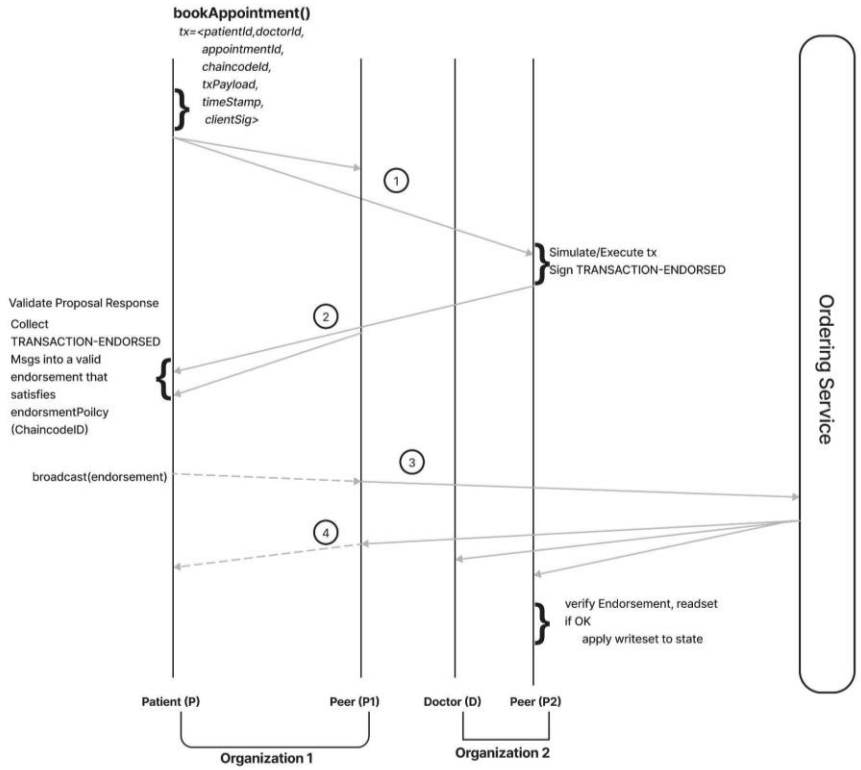

Figure 4. Schematic showing the transaction flow to book appointment through the system described here.

The Transaction flow for Appointment booking will adhere to the following four steps:

1. A transaction to Book an Appointment is proposed by the Patient(P) of Organization 1 and the required parameters are passed. This proposed transaction is sent to peer P1 and P2, of organizations 1 and organization 2, respectively.
2. In this step, the transaction is verified by the peers for transaction proposal format, to avoid replay attacks it checks if the transaction has been submitted in the past, and it also checks if the submitter is authorized to perform the proposed operation. After all the checks, it executes the smart contract against the current state database to produce a transaction proposal. Finally, the 'Proposal Response' is sent back to the Submitter.
3. Again, the Patient(P) node will inspect the proposal response before submitting or Broadcasting the transaction to the Ordering Service.
4. The Ordering Service does not inspect the entire content of the Appointment Booking transaction, it simply receives transactions, orders them, and creates blocks of transactions per channel. These blocks of transactions are "delivered" to all the peers on the channel. The transactions within the blocks are validated to ensure the endorsement policy is fulfilled. Transactions in the block are tagged as valid or invalid. Each peer appends the block to the channel's chain, and for each valid transaction, the write sets are committed to a current state database. An event is emitted by each peer to notify the client application that the transaction (invocation) has been immutably appended to the chain, as well as notification of whether the transaction was validated or invalidated.

3.3 Requesting for patient data access (attribute-based access control)

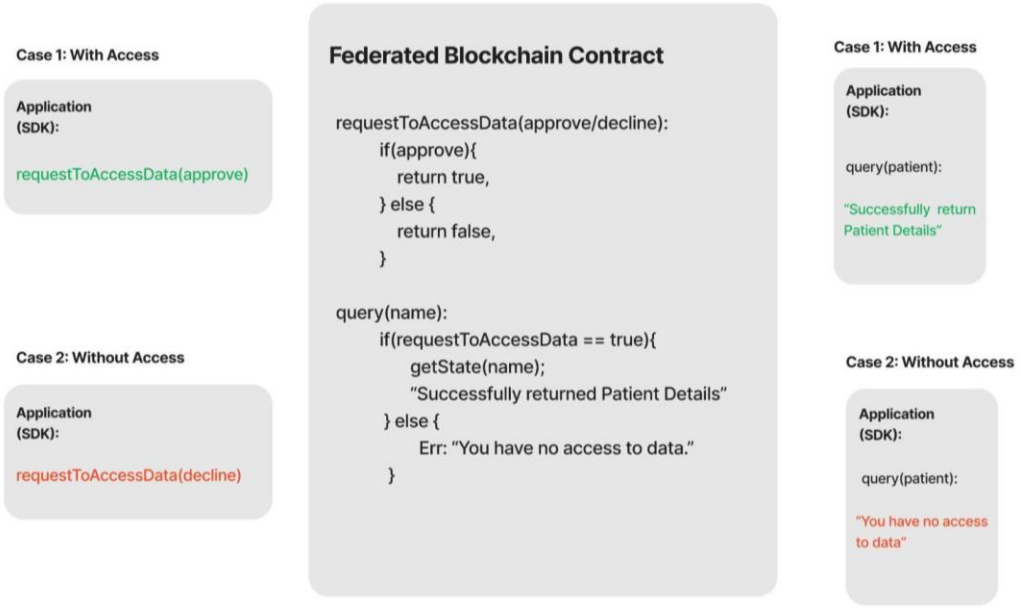

Figure 5. Schematic showing a sample federated blockchain contract instance for attribute-based access control.

Access control decisions can be made by Chaincode (and by the Hyperledger Fabric Runtime) based on an entity's attributes. This is called Attribute-based Access Control (ABAC). To make this possible, an identity's enrollment Certificate (E-cert) may contain one or more attribute names and values. The chaincode then extracts an attribute's value to make an access control decision.

For Example: In the above smart contract instance we have 2 organizations. Org1 belongs to the patient on the left. Org2 belongs to the doctor from the clinic on the right. There are particularly two cases shown in Fig. 5:

Case 1: The Doctor requests Access to the Patient's data and the patient approves the request.
Case 2: The Doctor requests access to the patient's data and the patient declines the request.

This chaincode then extracts the value of the attribute and makes the access control decision. In the second case, the doctor's identity did not get access to the patient's data, hence, when the doctor tries to access the data it gives an Error: "You have No Access to the Data". In this manner, attribute-based access control is achieved, and so that patient data is securely handled.

4. RESULTS AND DISCUSSION

This paper presents the development of a private blockchain-based data management software to enable safe remote access without compromising patient information. The BlockTrack software developed at IIT Madras will be customized to interface with implant modules for Orthopedic recuperation monitoring developed at University College London. The implant modules consist of ultrasonic bone health monitoring sensors, connected to relay nodes that can transmit patient data to the BlockTrack mobile app, which then 'blockchainizes' the information to be stored securely on a cloud based Blockchain network. Each record has a unique ID enabled by Blockchain, for secure access and review of patient information by other parties including doctors and pharmacists. Demonstration of the system in limited laboratory trials and key findings are discussed with a goal to further develop this solution.

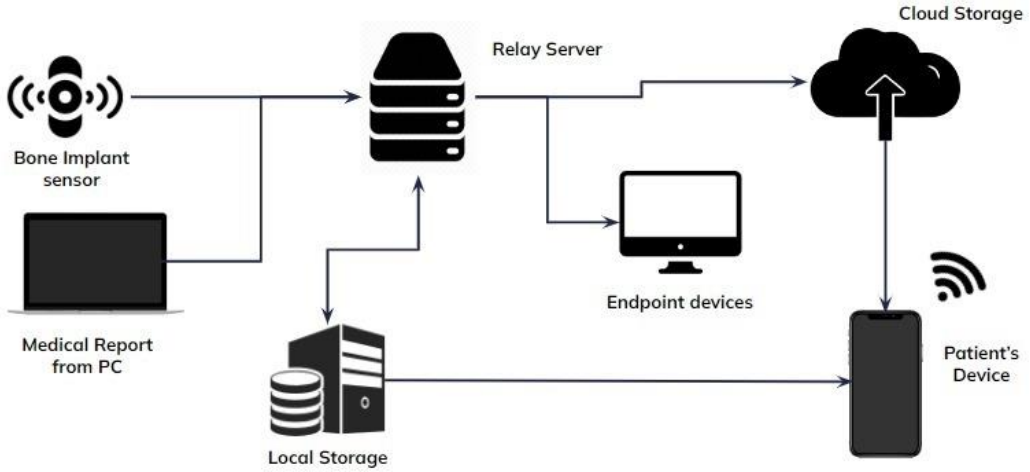

Figure 6. Schematic showing IoMT devices interfacing with a blockchain database.

Point-of-care devices collect sensitive important data, which is to be automated and recorded under the Personal Health Record of the patient. This data can be easily integrated into the blockchain health record by the use of relay servers, and edge devices. The use of blockchain helps to evolve a unique identifier for every patient, and all health records including doctor consultations, biosensor measurements, pharmacy and therapy, and interventions are hence securely connected.

Considering the specific case of the bone implant sensor, the relay server or the 'blockchainizer' being developed interfaces with a particular bone implant sensor, which would be linked to the patient's identifier, and the data collected would be logged onto the patient's blockchain, and the hospital's record management system, after processing the received data. The logged time-domain data is processed using the endpoint device (smartphone application or web-based application) into raw signals, analytic formats, and graphical formats, and are displayed on the endpoint devices. A number of functionalities will be added in a modular manner that will be uniquely indexed to a patient, as well as permit access and visualization operations. The proposed system would assist the bone implant operation process significantly by continuously tracking and monitoring the progress securely.

5. CONCLUSION

This paper discussed an architecture for integrating distributed health data, with trials meeting the expectations and validating the main hypothesis. The federated blockchain system was implemented and tested to be functional in terms of interoperability, transparency, access control, and readability of the stored data. The proposed architecture's main contribution is not the use of blockchain to store patient health data references, which is already done by other proposals. Instead, the proposal's main contribution is the use of federated blockchains to make it easier for institutions to access integrated patient information and maintain the patient data structure, and achieve interoperability, privacy, security, digitization, and standardization and also to accommodate other third-party health data users. This solves the problems associated with using blockchain for patient-centered health systems and facilitates the transition to such systems. The proposal also reaffirms the suitability of blockchain for developing patient-centered health systems due to its decentralization, sharing, openness, traceability, and security.

FUTURE WORK

This paper discusses the usage of federated blockchains for a patient-centric health record management system, which have many possible vectors of development, on the assumption of proper deployment of these systems in healthcare institutions: Implementation of complex consensus mechanisms and better blockchain data structures can be explored (Yuan et al. 2022). Personalized predictive healthcare can be achieved by applying a federated learning algorithm on this FHR ecosystem. The mass data can be used to train various models for various purposes, and a personalized model can be built for each person after achieving a consensus on the parameters obtained by the FL model. The notion of a Global

Health ID, to hold health records from multiple countries can be built on top of an FHR system, where organizations from multiple countries are all on the same consortium and are able to append records to the patient's personal health record. All IDs from different countries will be indexed under one global ID on the blockchain.

REFERENCES

[1] J. Chen, C. C. Akoh, R. Kadakia et al., "Analysis of 408 Total Ankle Arthroplasty Adverse Events Reported to the US Food and Drug Administration From 2015 to 2018," Foot Ankle Spec, 14(5), 393-400 (2021).

[2] Shuo Yuan, Bin Cao, Yao Sun, Zhiguo Wan, Mugen Peng et al., "Secure and Efficient Federated Learning Through Layering and Sharding Blockchain", 8 Aug 2022.

[3] Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi et al., "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security" Volume 23, Issue 2, July 2022.

[4] A. Rana and P. Rajagopal, " Method and blockchain device for managing health records of users in blockchain based collaborative network" patent filed with Indian Patent Office, No. 202141006659, provisional filing on 17/2/2021 and complete filing on 17/2/2022.

[5] P. Rajagopal, A. Varna, V. Vijayaraj and V. Rathinasamy, "Secure and interoperable federated blockchain health record ecosystem", patent filed with Indian Patent Office, No. 202341009753, provisional filing on 14/02/2023.

[6] Javier Rojo; Juan Hernández; Juan M. Murillo; Jose García-Alonso et al., "Blockchains' federation for integrating distributed health data using a patient-centered approach" Madrid, Spain; 07 July 2021.

[7] Ghulam Hyder Palli; Ghulam Fiza Mirza; Bhawani Shankar Chowdhry, et at., "Novel IoT-Based E-Health System: Hospital Management, Telemedicine and Quarantine Management for COVID-19" Publisher: IEEE, Karachi, Pakistan November 2022.

[8] Warmanto Firmansyah; Teddy Mantoro; Pratama Dahlian Persadha et al., "Regulatory Support to Prevent Health Data Breaches", Publisher: IEEE Sukabumi, Indonesia; January 2023.

[9] Schlatt, Vincent, Johannes Sedlmeir, Janina Traue and Fabiane Völter. "A Decentralized Electronic Prescription Management System." *ArXiv* abs/2109.06174 (2021).