Blockchain Based Remote Patient Monitoring system for Healthcare Data Security

Vishal Sharma, Anand Sharma

Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan, India
er.vishu1983@gmail.com; anand_glee@yahoo.co.in

Abstract

In the field of digital health system, Remote Patient Monitoring (RPM) is strengthens the online healthcare services and it permits to deliver the healthcare services to patient remotely doctors can get real-time health updates of their patients. Presently, RPM is widely used in smart healthcare system to remotely monitor the vital signs of patients. Remote patient monitoring (RPM) have also become more popular and demanded than ever in the critical situation of COVID-19 pandemic. RPM is one of the considerable fields that widely use IoT infrastructures. In this system various body sensors and wearable devices collects the vital signs of patients and the actuator processes and analysed them and sends them to the central storage such as the cloud. Aforesaid centralization and unsecure transmission of heath information can be challenging, as it can be a single point of failure, manipulation of data and tampering with information, and leak of privacy. Blockchain can be a potential solution to solve these problems due to its distributed and tamper proof structure. However, due to the expansive mathematical calculations in the blockchain technology it comprises the overhead of high bandwidth and delay; it may not fit perfectly into the energy efficient and time critical RPM system. In this paper we have proposed a design for integration of modified blockchain approach and RPM systems to obliterate the overhead of the conventional blockchain technology and its benefits for security and privacy preservation of patient's critical healthcare data. The amalgamation of these two approaches will be highly favourable not only for the patient but also for the doctors and other healthcare providers.

Keywords. IoT, Blockchain, RPM, Healthcare System, Privacy, Security.

1.   INTRODUCTION

The report from the Ministry of Home Affairs, Government of India showed that 68.84% of the population are staying in rural areas [1]. The doctor and patient ratio is very low in these areas. The non-availability of doctor's services in these areas is also a big problem in the crucial time of COVID-19 Pandemic. RPM can become an effective solution to overcome these barriers of healthcare services. Through the RPM system, doctors can monitor the patient's health condition from anywhere at any time. In the era of digital health system RPM is a field in which key architecture is IoT. An Internet of Things network is a network of many physical objects; even human beings behave like a thing in it which can communicate with each other. All these things which are available in this network are embedded with different types of sensors and software. All these things and devices are in this network; they can communicate and collect data among themselves without any human intervention, as shown in Figure 1. These sensors might be a moisture sensors, pressure sensors, light

522

sensors, motion sensors and temperature sensor etc. The concept of "Internet of Things" was first introduced by Kevin Ashton in his presentation, which he presented in P&G (Proctor & Gamble) in 1999 [2].
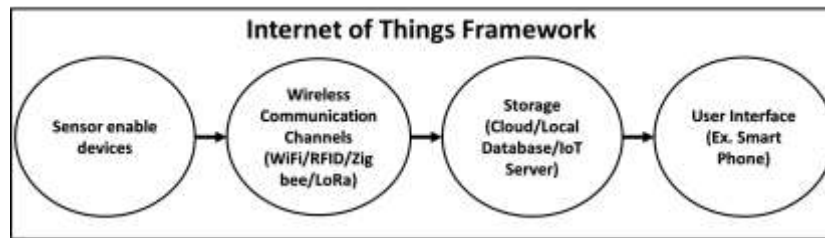

Figure 1: Structure of IoT framework

As shown in Figure 2, the architecture of an IoT network is divided into three tiers, i.e. Cloud layer, Gateway or Fog layer and Sensor layer. Subsequent, we briefly discussed each and every layer [3].
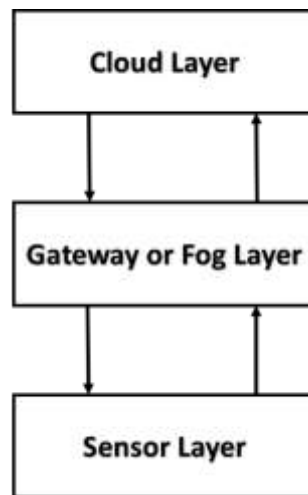

Figure 2: Layered architecture of IoT

- **Cloud Layer:** This is the uppermost layer of the IoT layered architecture. To provide the needed data information and required services to meet the necessary requirement of the user is the principal responsibility of this layer. Data information storage, different types of services and backup are also offered by this layer. This layer also provides different analysis services to estimate the future state of the devices [4].
- **Gateway or Fog Layer**: This is the middle layer of IoT layered architecture. By interconnecting many different physical infrastructure network and network devices (Bluetooth, RFID, Zigbee, Wi-Fi, etc.), this layer provides an integrated and heterogeneous network. This layer works to route and transmit the collected

data from the sensor layer through a secure channel to central control or cloud storage. This layer also provides the services like processing of data, computation and decision making. Gateways, hubs, switches, cloud etc. networking devices are parts of this layer [5].

- **Sensor Layer**: This layer is the lowermost layer of this architecture and it is liable for interacting with a number of actuator, different types of sensors, RFID enabled devices and other physical devices. Therefore this layer is also known as sensor layer. The main responsibility of this layer are sensing of data, measuring of sensed data and also data processing sometimes. This layer is responsible for connecting all the things to the Internet [6].

Remote Patient Monitoring system integrated with body sensor or wearable devices to collect the vital signs of patients and store these health data on the central storage such as cloud and also send the health alert in the suspicious situations. In addition to the vital signs, other information such as demographic data, geographic location of the patient can also be there. The top most priority of any RPM system is the security and privacy preservation of patient health data. Privacy of patient's health data also includes the capacity to have control over data and determine access levels to be granted to others. Blockchain technology can prove to be a revolution for the security and privacy of patient health data in RPM systems. Since Blockchain possesses the advantages of distributed, tamper proof and access control architecture [7].

This paper proposed an integrated architecture of RPM and Blockchain for securing and preserve the privacy of critical healthcare data. This proposed design contain three layers architecture: Sensor layer, Blockchain layer and cloud layer. Rest of the paper includes the general architecture and challenges of general RPM architecture, outlines the existing literature related to the use of blockchain in the digital healthcare field, Blockchain and its integration with RPM system architecture, Presents the detail about our proposed framework and finally concludes the paper and sets a road map for future research [8].

2.   RELATED WORKS

Remote patient monitoring system is a demanding field of healthcare system that contains sensors for collecting biomedical data of the patients and by which healthcare professionals can remotely monitor the patient's vital signs outside the traditional healthcare locations such as the healthcare places viz. hospital, clinic etc. Consequently, when storing, sharing, and retrieving these remotely collected healthcare data, it might be possible to tamper with these critical data.

Alexandru Archip et al. in [8] have developed a prototype using mobile sensors and gateway. The functionality of this system can be accessed by RESTful API on any mobile device of the physician. They have analyzed their work based on power consumption test and feasibility test and they found system performed well in both the result.

Rui Guo et al. inm [9] have proposed a blockchain based on demand access policy changed ABE model for maintaining the integrity and privacy of patient's sensitive data in smart healthcare system. They have also proved prevention of collusion attack. They have proved their work by analyzed the security and performance comparison with other related works in different phases.

Sandi Rahmadika et al. in [10] have proposed a model for storing the patient health data on to the blockchain which are coming from various sources. They have also analyzed their work against various attacks.

Md Ashraf Uddin et al. in [11] have proposed a two tier based model based on many layers of interfacing for storing the required and non-required data. They have discussed the optimized and secure communication between various layers. They have also analyzed their work for energy consumption; delay in data processing and against various types of attacks.

Kristen N. Griggs et al. in [12] have proposed a model for storing the all events on the blockchain using smart contract. They have also analyzed their work against various security aspects and compared their work with traditional system.

Aiqing Zhang et al. in [13] have proposed a model for sharing patient's data using the combination of private and consortium blockchain architecture using public key encryption with keyword search. They have evaluated the performance of their work on JUICE platform.

Md Ashraf Uddin et al. in [14] have proposed a three level patient centric model for storing patient health data on the blockchain implemented at Fog and Cloud level. They have also proposed a modified PoS consensus mechanism. They have analyzed the energy consumption in block generation.

Gautam Srivastava et al. in [15] have proposed a blockchain integrated network with various lightweight cryptographic services like ARX and ring signature to enhance security and privacy and smart contract for IoT enabled healthcare network security.

Bashayer Al-Ahmadi et al. in [16] have proposed a three layers blockchain enabled model for storing the patient's health data.

Jigna Hathaliya et al. in [17] have proposed a blockchain and machine learning integrated RPM model for classify the patient according to symptoms of health data.

Lei Hang et al. in [18] have proposed a permissioned smart contract enabled blockchain and IoT integration model for securing sensing healthcare data integrity using web interface. They have analyzed their work by various performance analysis analysis.

Muhammad Salek Ali et al. in [19] have proposed a combination of on-chain and off-chain system model for record keeping and securely transfer the health data between patient and healthcare provider respectively. Their proposed model preserve the privacy of health data and anonymously and securely transfer the data using Tor network. They have used Ethereum's Rinkeby testnet for analysis of their framework.

Partha Pratim Ray et al. in [20] have proposed a blockchain enabled IoT based healthcare model for storing the healthcare data on chain. They have compared various blockchain platform and consensus algorithm those are suitable for IoT based healthcare system.

Hoe Tung Yew et al. in [21] have proposed a model for real time sensed health data sending via MQTT broker on the database in both public and private network from where healthcare provider can view the real-time data via Android mobile application (App).

Lei Ru et al. in [22] have proposed a model which builds around the six different modules as a data gathering module, a data receiving module, a data transmission module, a data processing module, and a display and alarm module for a health monitoring project. They have analyzed their work by observing the pulse readings, body temperature readings, ECG readings, and physiological data gathering

M. Dhinakaran et al. in [23] have proposed a machine learning enabled IoT based health monitoring system.

Bessem Zaabar et al. in [24] have proposed a three layer blockchain enabled IoT based model for storing and communicating the patient's private data between patient and healthcare providers and RESTful API is used for the creation of web services.

3. REMOTE PATIENT MONITORING (RPM) ARCHITECTURE

In-home monitoring or remote patient monitoring is a type of system such that by which healthcare professional can track the real-time healthcare data of patient remotely and use it in various treatment plans. Remote Patient Monitoring (RPM) is one of the areas where IoT technology is being used. It is a fundamental component of the e-health domain. It can become an alternative to hospital visits, increasing the number of people monitored without increasing workloads for healthcare providers [9]. RPM focuses on rural area's patients, patients of chronic diseases, post-operative patients, senior citizen patients, and where healthcare facilities are limited. RPM devices capture a masses of health data, from heart rate to blood pressure, without any surveillance by any healthcare provider. They can be either sensors enabled user-friendly wearable or implanted devices in a body or stationary devices having physical location and transmission of these health readings for further diagnosis and treatment [10].

Figure 3: General RPM Architecture

Thus, a remote patient monitoring system may comprise the following components as shown in Figure 3:

- **Health Data acquisition:** This module is responsible for acquiring health data (Such as Blood Pressure, Temperature, ECG.etc) through the various sensors or sensor embedded wearable devices and then sending of these collected data to central storage for further analysis through a smart device [10].
- **IoT Gateway:** IoT Gateway is responsible for connecting smart devices to the cloud either physically or virtually. Though, IoT gateway provides preprocessing, normalization of data and the connectivity of network. It translates the diversified data set which is obtained from various sensors in a common format by data normalization [11].
- **Cloud repository:** The storage of massive and ever changing health data array and retrieval servers is an important module of these systems. It also plays a very important role for the identification and testing of abnormal healthcare data. It also aggregate and analyzed crucial health data from various sources and process it to

gain a real-time view of health state, as well as promptly alert the doctors and patients about potential issues [12].

4.   ISSUES OF RPM

4.1.   Security and Privacy

A lot of data is stored on the central cloud where it is handled by third parties, due to this there is a full risk of data stolen. The Integrating a third-party system that can be hacked puts patients' privacy and security at risk as a result. Subsequently RPM systems have to be ensured proper security and privacy of stored and processed sensitive and private data like electronic health records, various diagnostic results, etc. There are some risks related to track the location of a patients and use their private data to harm the patient. There is no such provision that the healthcare provider should take the consent for data collection and to review and access their private information. And no any explicit consideration are there for what information will be shared; with whom; and for how long time. There is also no transparency about how privacy and security will be managed. Although there are no universally agreed standards for health the privacy and confidentiality of data, still it is essential to achieve compliance with all the necessary standards, such as HIPAA and HITECH in the USA, as well as GDPR in the Europe [13].

4.2.   Integrity

In RPM systems, a lot of data is transferred from sensor devices and wearables across the cloud and from the cloud to the healthcare provider. Any intruder can integrate the data, and the data that has been integrated can put the patient's life at risk. And also the healthcare data of the patient aggregated from various sources can be obtained in several formats, including unstructured or semi-structured data formats. Apart from this, there are many vendors who do not use the same data format for sensor and wearable devices [14].

4.3.   Real-time Access to Data

Timely transfer of health data information in RPM system is a long and tedious process as it involves multiple transfers. Healthcare data of the patient is collected and uploaded from various sensors and wearable devices. Now if this device is on the mobile network, then this data reaches the healthcare provider through many networks and RPM network. If there is an interrupt or outage at any of these hops, then the data sending will either fail or it will reach late to the healthcare providers. Because there is no guarantee that the mobile network will always be available. Because due to this the question of patient's life and death remains, so it is very important for the data to reach reliably and timely [21].

4.4.   Accuracy of Data

The data quality is also matter in the case of RPM system. The results of the diagnostic practitioner always depend on the accuracy of the data, Even if the system, the sensors, and the network are running fine, the reached data must be accurate [22].

4.5.   Storing and processing massive arrays of data

A very large amount of data is generated from the RPM system. So it takes a lot of time to process, analyze and respond [23].

4.6. *Scalability and high availability*

Scalability also a big issue in the RPM system. If the system is not scalable, then it will take a lot of time for the patient's information to be processed and response, due to which the life of the patient can also be at stake [24].

5. BLOCKCHAIN ARCHITECTURE

An anonymous researcher Satoshi Nakamoto first time presented that concept in a white paper in 2009 [25]. The blockchain concept is built on the linked list premise. So similarly there is a series of blocks in a blockchain, all these blocks are linked to their previous block with a unique numerical value. Each and every block in this contain hash value, set of transactions, timestamp and one time varying value, nonce. In this, each block keeps the hash value of its previous block, resulting in a chain of cryptographically secure blocks. This concept was raised for bitcoin, a digital currency. Blockchain technology was introduced so as to eliminate the need for a central authority and trust can be developed for the transaction between two entities without the involvement of any third party. So, thus, the blockchain is a trusted, distributed and decentralized digital ledger. In a point-to-point network, this technology operates, and each and this network's blocks are all tamper-proof and unchangeable. Blockchain technology plays an important role in securing various applications because of its properties (tamperproof, Immutability, cryptographically secure etc.) [26]. Figure 4 shows the working of the blockchain network. The first block in this network is called the generic block and rest of the blocks are called miner or validator blocks. Miner peers add newly constructed blocks to this chain of blocks, for this they solve a complex mathematical puzzle and whoever miner solves the puzzle named as proof of work called consensus algorithm, he adds the new block to the previous chain. As a result, over the untrusted participants, all of the participating nodes can establish a trusted network. [27].
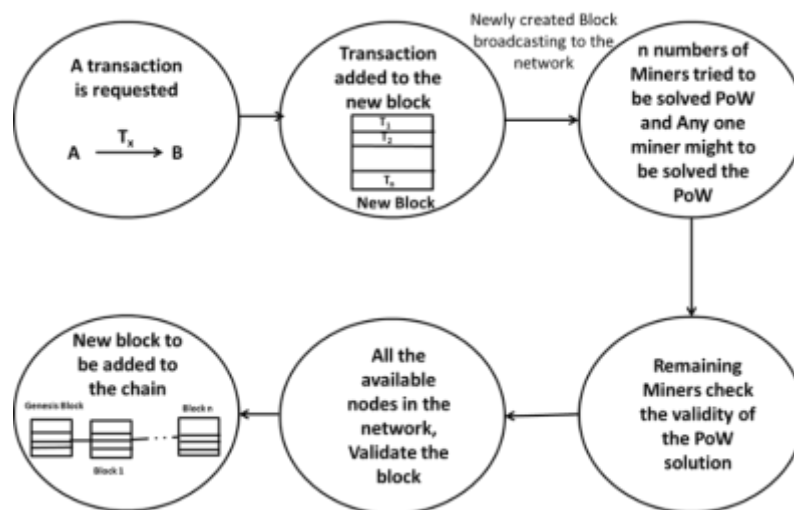

Figure 4: Working architecture of Blockchain

5.1. *Blockchain's Types*

Blockchain can be categorized into following three types based on peer's permissions:

1. **Public (Permissionless) Blockchain:** This is a category of blockchain which is also called permissionless blockchain because anyone can join it whenever they want. In this, any participant can see the ledger and can take part in the consensus process. [26]. Example; Bitcoin, Ethereum.
2. **Private (Permissioned) Blockchain:** This category of blockchain is also called permissioned Blockchain. Any participant who wants to join in this has to take permission. In this there is a limited decentralized system. In which only a single organization can access and control the system [26]. Example; Hyperledger.
3. **Consortium blockchain:** this is a type of semi-private blockchain network. In this, several organizations work together to run the platform. [26]. Example; Corda, Quorum and Hyperledger.

5.2. *Components of Blockchain*

- **Consensus mechanisms:** Consensus Mechanism in Blockchain is a procedure by which at least 51% peers to validate the global state of the distributed ledger by achieving a single data value agreement. In this way double spending attack can be prevented. In this way trust can be developed among unknown peers in a distributed environment through consensus mechanism. [27].
- **Smart Contract:** In blockchain network smart contract works as a self-executing program that automatically executes business logics set by peers in a distributed ledger. It is an interface to interact with the data in the blockchain. It is available for each of the participating peers in the network [3]. Smart contracts are added to each block of the blockchain. [12]. If any of the transactions make changes in it, then that too gets updated in the ledger like the transaction. Therefore, like transactions, smart contracts are also immutable. [27].

6. PROBLEM STATEMENT

A lot of data is generated day by day in RPM system. Storage of this big data is also a big problem, because complete health data is not important but it is useful for medical research. When the data collected by the sensor is sent to the gateway and cloud, then that data can also be tampered by the attacker. Adequate medical facilities do not reach the patients living in remote areas and rural areas. That's why we need such an approach so that the healthcare provider can take care of the patient from afar without being physically present and simultaneously, the problem of storage of large volume data and the problem of privacy and security of data should also be solved. On the basis of studied some existing applications and architectures in healthcare systems, we found some research finding as specified below in the existing systems that encourage us to work in the integration of blockchain and RPM in the digital medical system.

- No efficient and effective light weight cryptographic algorithm has been used in the Resource Constrained RPM system.
- A scalable and less computational power blockchain framework is needed that can integrate with energy efficient RPM applications in an efficient manner.

- Better security is required between every hop from the patient's healthcare data gathering to the data reaching the healthcare provider.
- There is a need for a smart contract based healthcare system that maintains critical healthcare data privacy and also verify the identity of the user..
- An efficient mechanism is required which can efficiently collect real time accurate data without any delay.

7. PROPOSED REMOTE PATIENT MONITORING (RPM) HEALTHCARE SYSTEM FRAMEWORK

Amalgamation of blockchain technology with smart healthcare system might be an excellent solution due to its features as cryptographic security, decentralization, immutability and transparency, for above discussed challenges for RPM. This future changing technology was conceptualized for the first time by an anonymous person Satoshi Nakamoto in his white paper in 2009 [25]. She/he introduced a digital currency as bitcoin in the distributed ledger. At the present time, several researchers, academician, industry professional and government are showing concern in this potential technology for securing the various applications. Although this technology can resolve the above discussed challenges of RPM, but this technology is founded on rich computation and cryptographic techniques, such that, It entails a significant bandwidth and delay overhead. Consequently, it is not totally fit in its original form for the IoT devices those are resource-constrained. Integration of Healthcare and Blockchain technology comes with some serious risks, because the logs of all the transactions are updated in the distributed ledger, due to this the privacy of the user can be leaked, the risk of privacy and security increases. [26]. Even due to process delay and due to privacy leaks, the life of the patient can also come to the fore.

Three layered architecture of proposed integrated RPM - Blockchain platform is represent in the Figure 5. In this proposed architecture all the medical sensors and wearable devices can sense patient's vital signs and transmit these data via Bluetooth or Wi-Fi to a mobile device. The mobile device sends this data to the gateway and the gateway sends this data in an encrypted form to the blockchain. Blockchain execute the master smart contract and it executes specific smart contract according to the threshold value of data [12]. If there is uneventful data then it is stored on the cloud and if there is eventful data then the event gets stored in the blockchain and the data is stored on the cloud and a hash of that data is created and that hash value is stored in the form of a transaction in the blockchain. And also an alert signal is sent to the healthcare provider and patient and his/her relative [12]. In this way, the security and privacy of the patient's data is not compromised.
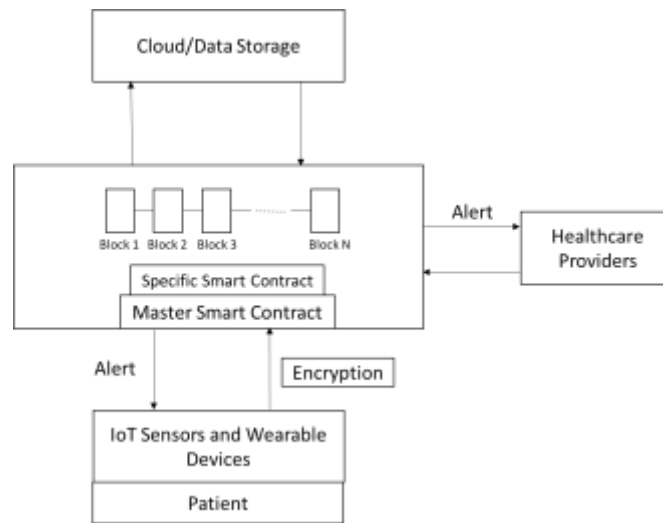
Figure 5: Blockchain in RPM based digital healthcare System

8.   CONCLUSION

This paper proposed a three layer blockchain enabled RPM system for the healthcare data security and privacy preservation. This proposed model provides a solution to the majority of security and privacy issues while deal with the resource constraint aspect of the RPM system and ensures all information security constraints confidentiality, integrity and availability. In this paper, we proposed a novel hybrid approach that combines the benefits of blockchain, IPFS and lightweight cryptographic primitives to evolve a patient-centric access control for electronic health records and providing effective security and privacy to critical health information. Since in this model only metadata will be stored in the blockchain, it is also scalable. As our proposed model is resolving almost all RPM issues against the rest of the state of the art solution. Hence, it can become an efficient RPM solution that can secure the health information of the patient. In the future, we will practically test this proposed architecture in different IoT networks.

REFERENCES

[1]   https://censusindia.gov.in/2011-prov-results/paper2/data_files/india/paper2_1.pdf
[2]   Sandro N. et al., "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future", Journ. of Cleaner Prod., Vol. 274, 2020.
[3]   Sharma V., Lal N. (2022) Role of Blockchain in IoT Enabled Power and Energy Related Healthcare System-Platform for the Development of IoT Security. In: Malik H., Ahmad M.W., Kothari D. (eds) Intelligent Data Analytics for Power and Energy Systems. Lecture Notes in Electrical Engineering, vol 802. Springer, Singapore. https://doi.org/10.1007/978-981-16-6081-8_27
[4]   Aakriti Singla, Anand Sharma "IoT Crypt–An Intelligent System for Securing IoT Devices Using Artificial Intelligence and Machine Learning" Artificial Intelligence and Global Society: Impact and Practices, Pages 161-174, CRC Press

[5]   Anand Sharma, Alekha Parimal Bhatt "Quantum Cryptography for Securing IoT-Based Healthcare Systems" Limitations and Future Applications of Quantum Cryptography, Pages 124-147, IGI Global

[6]   Raju, Joel et al. "Cyber Security in IoT Devices using Blockchain Concept." (2020).

[7]   Daniel M. and Benedict O. "Blockchain mechanisms for IoT security", IoT,Vol.1, pp. 1-13, 2018.

[8]   A. Archip et al.,"An IoT based system for remote patient monitoring," 17th ICCC, 2016, pp. 1-6, 2016.

[9]   R. Guo et al., "Flexible and Efficient Blockchain-Based ABE Scheme With Multi-Authority for Medical on Demand in Telemedicine System," in IEEE Access, pp. 88012-88025, 2019.

[10]   Rahmadika S and Rhee K-H, "Blockchain technology for providing an architecture model of decentralized personal health information," Int. Jrnl. of Engg. Business Mgmt., 2018.

[11]   M. A. Uddin et al., "Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture," in IEEE Access, pp. 32700-32726, 2018.

[12]   Griggs, K.N. et al. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med. Syst. (2018).

[13]   Zhang, A., and Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J Med. Syst. (2018).

[14   ]M. A. Uddin et al., "A Decentralized Patient Agent Controlled Blockchain for Remote Patient Monitoring," Int. Conf. on WiMob, pp. 1-8, 2019.

[15]   G. Srivastava et al., "A Light and Secure Healthcare Blockchain for IoT Medical Devices," IEEE CCECE, pp. 1-5, 2019.

[16]   Bashayer Al-Ahmadi and Sanaa Sharaf, "Blockchain Based Remote Patient Monitoring System", JKAU: Comp. IT. Sci., pp: 111 – 118, 2019.

[17]   J. Hathaliya et al., "Blockchain-Based Remote Patient Monitoring in Healthcare 4.0," IEEE 9th IACC, pp. 87-91, 2019.

[18]   Hang, L. and Kim, D.-H. Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity. Sensors 2019.

[19]   Ali, M.S. et al. A Decentralized Peer-to-Peer Remote Health Monitoring System. Sensors, 2020.

[20]   P. P. Ray et al., "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," in IEEE Sys. Jrnl., pp. 85-94, 2021.

[21]   H. T. Yew et al., "IoT Based Real-Time Remote Patient Monitoring System," 16th IEEE Int. CSPA, pp. 176-179, 2020.

[22]   Lei Ru et al., "A Detailed Research on Human Health Monitoring System Based on Internet of Things", WCMC, 9 pages, 2021.

[23]   M. Dhinakaran et al. "A System of Remote Patients' Monitoring and Alerting Using the Machine Learning Technique", JFC, 7 pages, 2022.

[24]   Zaabar et al., "Secure and Privacy-aware Blockchain-based Remote Patient Monitoring System for Internet of Healthcare Things," 17th Int. Conf. on WiMob, pp. 200-205, 2021.

[25]   Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.

[26]   V. Sharma et al., "A Detail Dominant Approach for IoT and Blockchain with their Research Challenges," ICONC3, India, pp. 1-6, 2020.

[27]   V. Sharma et al., "A Novel comparison of Consensus Algorithms in Blockchain," AAMS, Vol. 19, 2020.

Biographies

Vishal Sharma received his bachelor's degree in computer engineering from Rajasthan University, Jaipur in 2006 and master degree from Jagannath University, Jaipur in 2012 and pursuing Ph.D. degree from Mody University of Science and Technology, Sikar. His research areas include Network Security, Information Security and Blockchain. He has a total teaching experience of 13 years. He has published and reviewed several articles in journals of repute. Currently he is working as Assistant Professor in CSE Department of School of Engineering and Technology at Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan, India.

Dr. Anand Sharma, received his Ph.D. degree in Engineering from MUST, Lakshmangarh, M.Tech from ABV-IIITM, Gwalior and B.E. from RGPV, Bhopal. He has been working with Mody University of Science and Technology, Lakshmangarh for last 12 years. He has more than 14 years of experience of teaching and research. He has been invited to several reputed institutions like ISI-Kolkata, IIT-Mumbai, IIT-Jodhpur, IIT-Delhi, RTU-Kota etc. He has pioneered research in areas of Information Engineering, Information Security, IoT, Knowledge Management and Machine Learning. He is a member of IEEE, IET, ACM, IE(India), Life Member of CSI and ISTE. He is serving as Vice-Chairman of CSI-Lakshmangarh Chapter and Student Branch Coordinator of CSI-MUST Student branch. He has authored / edited 10 books of national/international publishers. He has more than 90 papers in reputed International Journals and conferences. He has organized more than 15 conferences / seminars and workshops. He is serving on advisory capacity in several international journals as Editorial Member and in International Conferences as Technical Programme committee / organizing committee.