EAI Endorsed Transactions
on Pervasive Health and Technology
Review Article EAI.EU

Blockchain for IoT-enabled Healthcare

Ravendra Singh[1,*], Hitesh Kumar Sharma[2], Tanupriya Choudhury[2], Anurag Mor[2], Shlok Mohanty[2], Sachi Nandan Mohanty[3]

[1]Department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh, India
[2]School of Computer Science, University of Petroleum & Energy Studies (UPES), Energy Acres, Bidholi, Dehradun, Uttarakhand, India
[3]School of Computer Science & Engineering (SCOPE), VIT-AP University, Amaravati, Andhra Pradesh, India

Abstract

Emerging technologies including such Internet of Things (IoT) and blockchain contribute significantly to the improvement of health services. The purpose of this chapter is to achieve and democratize services through the provision of medical care as a service. The result was the development of medical gadgets integrating healthcare sensors. It links medical equipment like the temperature controller to the cloud environment of medical doctors and staff. This study introduced the combination of IoT and Blockchain as a secure platform to reduce the scarcity of nurses. Blockchain was employed for storing and validating patient information in the proposed operating framework. A significant reduction in nursing gaps for large-scale patients has been shown. All technological specifications have been given to allow the prototyping execution of these suggested medical services simply adaptable. This article deals with Blockchain technology inclusion in Remote Medical Monitoring Devices Internet of Things (IoT) security. The document provides the advantages of Blockchain based safety methods and practical barriers in remote health monitoring via IoT devices. The study also examines several cryptographic methods appropriate for IoT implementation.

Keywords: E-Healthcare, Security Protocol, Internet of Things (IoT), Blockchain, Network Attacks, Passive and Active Attack.

Received on 15 February 2023, accepted on 20 April 2023, published on 28 June 2023

doi: 10.4108/eetpht.9.3348

1. Introduction

Smart Healthcare is proving its requirement across the globe. Corona Pandemic is one of the major use cases for using TMIS (Tele-Medicine Information System) from remote locations. As the number of patients is increasing day by day, the physical or traditional method for treating a patient is not feasible today and it will be a challenge for almost every county in the coming years. In recent years, the increase of IoT and wearable devices through remote monitoring has enhanced patient quality [1]. By remote location-based healthcare system will help a doctor to treat more people than a physical-based healthcare system. A particularly developed monitoring equipment for monitoring and transmitting health data to smart contracts, a smartphone with Internet access may be the core component of a TMIS system [2]. In TMIS and the current drive to build Smart Cities, wearable and IoT gadgets play a vital role. Wearable equipment collects and transfers patient health data to hospitals or medical facilities for monitoring, diagnostic and therapeutical purposes. This shows that all patient data is processed and exchanged from a big-data scenario. Such infrastructure requires safe data sharing for handling patient data with other organizations. Data confidentiality and security solutions may be extremely well covered with Blockchain technology in IoT applications [2]. The resilience against failure and data exposure is provided by technology. Miners (in charge of block building) continually try to solve cryptographic problems in the form of a hash calculation. A mining procedure is dubbed the addition of a new block to the network. But it is not easy to use Blockchain in the IoT environment. There are numerous challenges, including

*Corresponding author. Email: ravendra85@gmail.com

but not limited to, in Blockchain. High computer power to overcome PoW low transaction confirmation scalability delay. We propose a new blockchain model and remove the PoW idea to make it appropriate for IoT devices. Our approach is based on the dispersed nature and other network security features. In the following sections, we will address the inconveniences in the existing IoT blockchain concepts in depth. IoT has become an important technical component in recent years to overcome compatibility, variability and web resistance. Nevertheless, Blockchain provides a safe, stable and trustworthy infrastructure. Health is another problem that directly affects people's lives. There was little focus and significant manual research to combine all three fields into an unified technical environment. This article analyses how Blockchain operates on different platforms and says that Blockchain solutions cannot be reached on IoT devices and full-size ecosystems. The current Blockchain has an important defect in that it employs highly computational, noncritical hash operations, such as resource-controlled systems willing to sacrifice some data integrity for computation reductions and the use of energy, such as IoT. The original aim of this paper is to explore many commonly-used consensus algorithms in different types of Blockchain networks and decide which are useful for IoT-based healthcare services. The suitability in terms of healthcare applications of prominent IoT-blockchain systems is then assessed. The real difference or resemblance between these platforms or consensus techniques is also compared. Four instances are described methodologically in which IoT-blockchain may be utilised successfully for medicinal applications. IoT-based patient and organisational layered Blockchain architecture supports the administration of health data. Finally, an IoT-based Blockchain platform that can unite three main players in the healthcare sector, including public authorities, health plans and health organisations. Smart contracts and data flow structures are also discussed with IoT health block structures.

2. Literature Review

Blockchain is the most secure mechanism for healthcare system security. A lot of work has been done by many researches on one-way, two-way and multi-way authentication mechanisms. Wang et al. published a one factor authentication. It is based upon username and Password authentication system [9]. This mechanism stores username and password in RDBMS and it authenticate user based upon this saved credentials. In 2012 [3], authors discovered two-factor authentication protocol based upon username, password and RFID card. It is more secured than one-factor authentication system. In [4]. Authors proposed and implemented three-factor authentication system. In which username password, ID card and Biometric identity is used for authenticating a user. In [5] Blockchain based authentication is proposed for accessing E-Healthcare systems.

3. Types of Security Attacks in a Network

It has been categorized as two main kind of attaches an attacker can perform on a network

1. Passive
2. Active

In Passive attack, the attacker only captures the data packets float through the network. He will not make any changes in that and he will not re-transmit to the receiver. But in active attacks one more level of work is performed by attacker that with capturing the data packets he also make changes in those and re-transmit to the receiver (Figure 1 & 2)

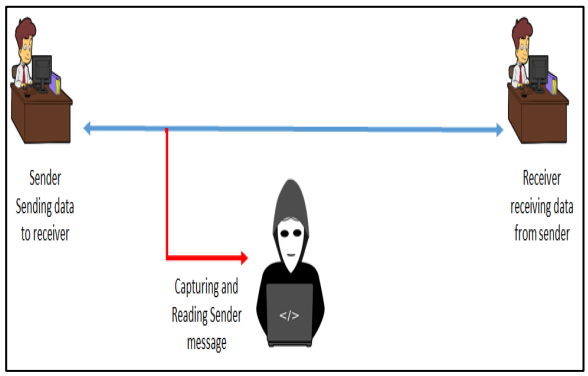

Figure 1. Passive Attack

We have shown both kinds of attacks in the following figure in figure 1 passive attack is shown where the attacker does not send it back to the receiver. In Figure 2 active attack is shown where modified packet is re-transmitted to real user and he got corrupted data packet.

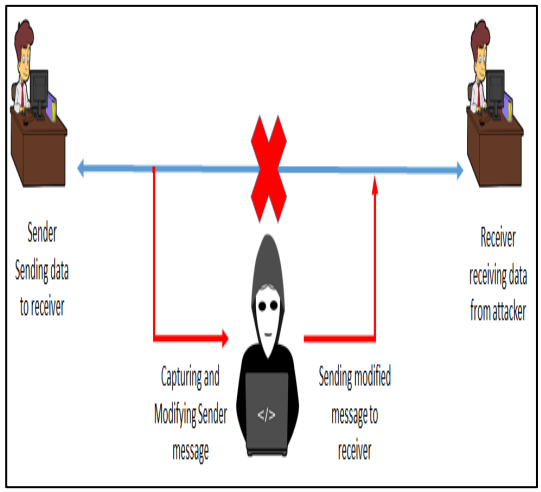

Figure 2. Active Attack

4. Tele-Medicine and E-Healthcare Authentication

TIMS are sophisticated technology that enable doctors to treat patients who live in remote places and are unable to go to hospitals remotely. Patients keep track of their diagnoses and treatments in the TIMS repository, which the doctor can access to review the patient's medical history. It helps the patient save time and money on hospital visits. Additionally, it lowers the cost for the hospital and doctor to physically care for the patient. Every time a patient needs medical care, the patient must verify themselves and give a smart device their smart card information. According to this perspective, numerous TIMS authentication schemes were suggested. However, there were certain security concerns with these authentication schemes, and they are vulnerable to network attacks. (Figure 3)

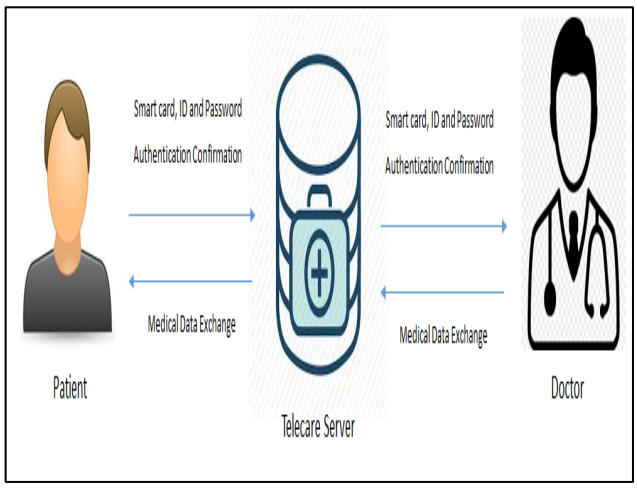

Figure 3. E-Healthcare Authentication process flow

5. Issues in Security and Limitations

Secure transfer of medical data is the major problem with RPM systems [10][16]. Blockchain technology is the finest technology for health care systems and may prevent these concerns since it cannot remove or modify information from blocking. But Blockchain technology is not a long-term answer in its original form. There are constraints that are quite obvious in connection with IoT situations. In this part, we explore the obstacles of integrating blockchain to IoT and how these problems may be resolved in our approach [13][14]. Encroaching: We need a decentralised system in order for us to assure resilience and scalability and to remove numerous traffic flows. Using the difficulties that occur with Blockchain with the information latency of such decentralised systems. We use a decentralised network overlay in our concept. Encryption based Protection: user cloud services contain data that can be changed or deleted as they are being transmitted. The retention of such erroneous manipulated data increases the system burden and may also generate RPM problems for the patient. So, we utilise digital signature technique to verify that the data is not changed. Data is validated using the digital signature of the user on the recepter side and send a receipt of data to the patient if received successfully. Connectivity: solution of "Work Proof" (PoW) is computationally demanding yet IoT devices are highly resource-limited. The IoT network usually comprises a number of nodes, while the number of nodes in the network expand, Blockchain technology scales poorly to big networks. In our overlay network, we abolish the idea of PoW and divide the overlay network into many clusters rather than a single chain of blocks. A single blockchain, therefore, does not have a responsibility for all nodes in the network. Information Processing: It is not feasible to store IoT large data via Blockchain technology and so we recommend the usage of cloud servers in order to store encrypted blocks of data.Due to the additional protection available like digital signatures and high-grade encryption, the data may be seen as safe via the cloud. User anonymity: A patient's medical data may include sensitive information and so the anonymity of data across the network must be achieved. We use a Ring structure together with digital signatures for anonymity. An anonymous signature allows a signature to sign data. In other words, the signatures are mingled with other groups and nobody knows whose members have signed the communication (save the actual signing party). Data security: We use a double encryption system to preserve data from hackers. We encrypt the data with low-weight ARX techniques and then again encrypt the data with the recipient's public key. In addition, we use a key exchange mechanism from Diffie-Hellman to transfer public keys and it is therefore nearly hard for an attacker to obtain the keys.

6. E-Healthcare Depose

An increasing number of data named cryptographic blocks is a Blockchain. A cryptographic hash of the preceding block is included in each block. Blockchain in a brief phrase is a complex yet straightforward system for fully automated and reliable transmission of information from A to B. One side starts the procedure by building a block. This block is checked by thousands, maybe millions, of computers on the net [15][16]. The confirmed block is added to a network chain, which creates not only a single record, but a unique historical record. (Figure 4). Blockchain based: The Blockchain is the public leader of all transactions (e.g. Bitcoin, Ether) to be completed and previously conducted. (A record booking is a record booking which tracks all transactions inside an organisation.). This directory is termed the block chain of previous transactions as it is a block chain. Prospector: Mining is the way entries are added to the blockchain public/private directory. A blockchain network miner is a node which can validate transaction by consensus, that is a member of the same network. A 51% assault refers to a miner or a group of miners who aim to dominate the

mining, computing or hash rate of more than 50 percent network. Persons having this capacity to exploit can stop or confirm new transactions. The number of miners continuously rises in order to track all the latest transactions by adding new blocks to the process. In a linear and chronological process, blocks are always added to the Blockchain. Intelligent Agreement: a software designed in order to digitally facilitate or verify the negotiation or fulfilment of specific computer protocols. Intelligent agreements typically allow transactions without third parties being included that are irreversible, trustworthy and trackable. Intelligent detractor: a novel concept of programming meant to tackle a questionable contract execution.

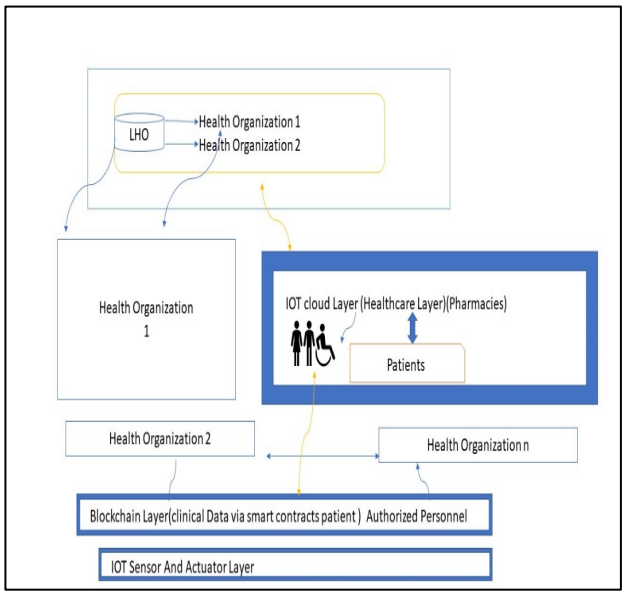

Figure 4. IoT and Blockchain in E-Healthcare

6.1. E-Health Blockchain Features

The technology provided enables you to keep your assets (e.g. contracts, paperwork, etc.). which allows you to have internet access. In this scenario, the owner will fully manage his account and allow the owner to transfer his belongings to anybody the owner wants. Transparency of a blockchain is due to the fact that each public address is available to observing the holding and transaction.it cannot be amended while the data is kept in the ledger. You don't have the power to change things, no matter who you are. If an error occurs, the error should be reversed by a new transaction. Both transactions are apparent at that moment. In the recorded ledger, the first transaction is seen as a mistake. The confirmed transaction then contributes with additional transactions that create a new data block. If a person wants to give blockchain information using a specific connection key and a public address, the transaction is signed with a private key. This type of information is very safe, because it doubles thousands of times and every hacker has to alter over 51% of nodes[15-18].

7. IoT and Blockchain

The internet is an extension of Internet links to common physical objects. Internet of things Incorporated with electronics, internet connectivity and other physical forms, such gadgets may communicate with, interact with and monitor distant devices through the internet. Because of the rigorous IoT networking requirements, blockchain looks to be. highly suitable for manipulative network assaults that target saved data and provide a safe platform for communication between devices on each other within the network. Discover the limitations of existing paradigms and what blockchain pledges leads to the paradigm of IoT-based e-health. Additionally, it is expensive to set up massive IoT networks, maintain centralized clouds, and network all the equipment. IoT devices must also be resistant to attacks on both the physical and informational levels. Although many of the currently used methods offer security for IoT systems, they are complex and inefficient for low-resource IoT devices. Blockchain creates a peer-to-peer network, reducing the installation and maintenance costs of central clouds, data centers, and networking equipment by distributing compute and storage requirements across all networked devices. The issue of failure is addressed by this communication strategy. Blockchain utilizes cryptographic methods to overcome difficulties with data protection for IoT networks. The majority of IoT networks currently in use rely on client-server architecture, which has tremendous storage and processing capacity and can identify, authorize, and link to all devices through cloud servers. Additionally, all communication between the devices must take place through the internet, despite the fact that they may be close to one another. This paradigm is helpful for small-scale IoT networks, but it has poor scalability. (Figure 5 and Figure 6) (Figure 7)

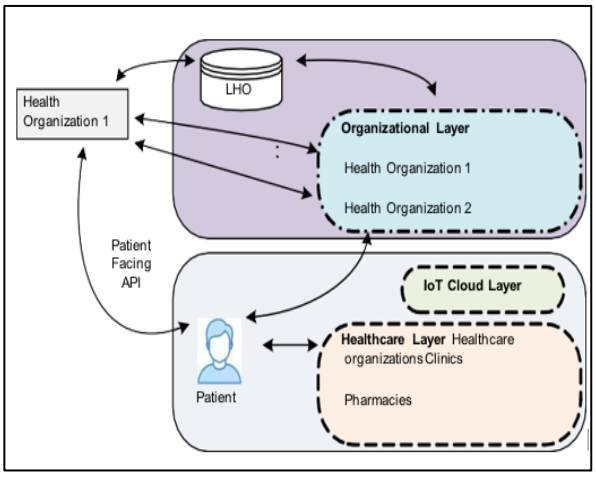

Figure 5. Process Flow in E-Healthcare(part 1)

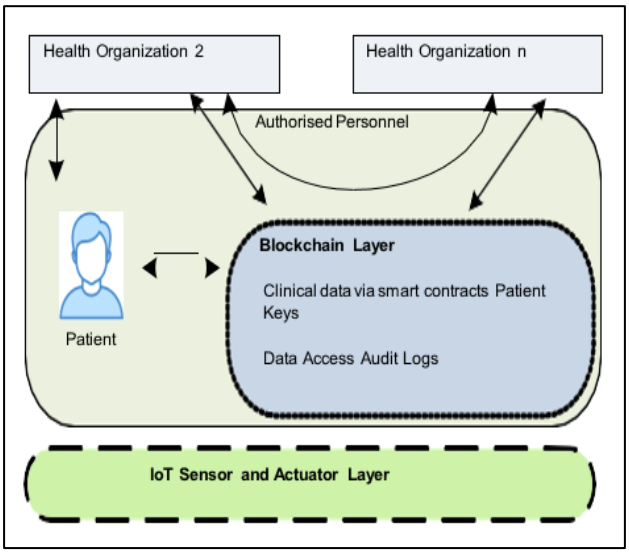

Figure 6. Process Flow in E-Healthcare(part 2)

8. Implementation of Blockchain in E-Healthcare

The main reason for the failure of the traditional medical services framework is the fact that people generally are unable to contact a specialist due to their busy schedules or for other reasons. Tele-medical services are quite like conventional methods of diagnosis and treatment, with a few key differences [19-25]. It has aided people who have a regressive background and lack the chances and advancements of clinical consideration. This framework creates an additional area and unlocks a layer of the structure that ably illustrates the management of health-related data throughout the computational phases and its beneficial transfer from the adviser to the victim. It also ensures a good nature of locating and guessing and aids in

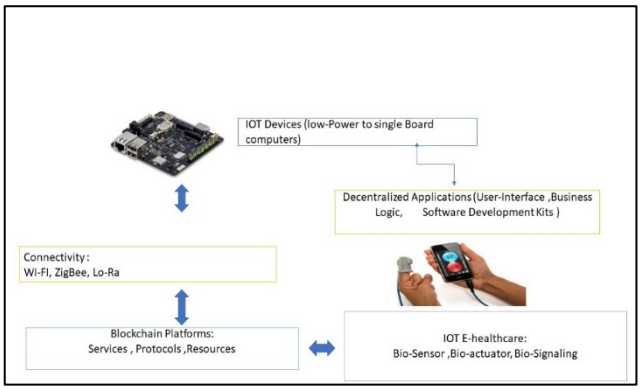

Figure 7. IoT Devices used in E-Healthcare

providing an experience. Access to medical records: The architecture can assist the patient by intervening in predefined commercial arrangements through local health groups or direct healthcare organizations. Entity interfacing takes place inside various healthcare organizations in which the IoT-based sensors, power supplies, wearables and cloud services are connected with patients' inseparability and blockchain smoothly. In the absence of existing commercial relationships, patients will also be assisted through intelligent contracts for authorization of Electronic Health Record (HER) sharing between different organizations. Assessment in Billing and claim in EHR: Fraudulent claims and accounts are the most serious e-health losses that need to be avoided and eradicated. The misrepresentation of unsupported e-health services is typically the source of claims over billing improper electronic-health services, an excessive charge of original electronic-health services and levying inefficient electronic-health services for the patient's medical condition. By automating the essential workflows and allowing parties to exchange information about the transaction and the contract, the IoT-based e-Health system can help to lowering the bulk of those problems while allowing fraudulent reclamation and payment procedures. Research in clinical: The consolidation procedure for detecting patient data requires great work, time and effort and thus expensive costs. Having big data set available and analysable characteristics to be determined is the main issue in achieving the accuracy of results of the underlying clinical studies. Hybrid key cryptography may be used to share the DLT with the community-based clinical research and study to provide safe clinical information. Supply chain management in drugs: Many individuals suffer or die from the use of counterfeit medicines every year. The supply chain procedure might include: transit, handling,

storage, redeployment and sale, starting with medicine manufacture and patient. A medicine may simply be added into the blockchain-DLT supply chain records which are permanent, unalterable and decentralised.

9. Application of Machine Learning and Blockchain in Healthcare

Machine Learning based algorithm are used by smart healthcare systems for disease prediction from a given patient dataset. Machine Learning model can be trained on a given medical dataset like dataset collected form Primary Healthcare Centers (PHC) of villages. The system will be trained for the patient of that rural area healthcare data. Using the same model a disease can be predicted by providing the health data for any unknown patient of the same rural area.

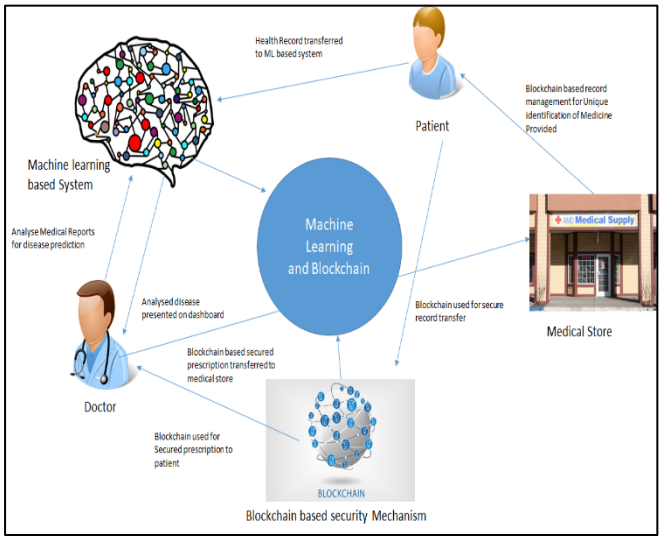

Figure 8. Significance of ML and Blockchain in E-Healthcare

Machine Learning can be helped in disease prediction for a unknown patient. But after prediction of a disease a detailed prescription should be provided by the doctor and the prescription should not be tempered by anyone. The medical store should also maintained the complete record in secured and un-tempered way for each medicine sold to the patient so that the complete flow of information in smart healthcare can be traced if needed. To overcome this security and privacy challenge Blockchain can be used with Machine Learning to make the complete healthcare system more accurate and more secure (figure 8).

10. Conclusion

Blockchain could be a most suitable security mechanism for provide required security features in Smart Healthcare and Tele-Medicine Systems. Although E-Healtcare or Tele-Medicine Systems are not the solution for all health issue but It can be utilized to address a number of them without requiring patients and doctors to move about physically. It will aid in reducing unneeded crowding in private and public hospitals. A patient who lives in a rural area can receive health consultation from a variety of available prominent hospitals and top-tier doctors throughout the world using these types of telemedicine platforms. This strategy improves the effectiveness and accessibility of qualified medical professionals whenever needed. These kinds of systems are essential, but they also call for quality and safety in the same way. These systems directly affect public health, hence a reliable and effective authentication mechanism is also required.

References

[1] Saha, Arijit & Amin, Ruhul & Kunal, Sourav & Vollala, Satyanarayana & Dwivedi, Sanjeev. (2019). Review on "Blockchain technology based medical healthcare system with privacy issues". Security and Privacy. 2. 10.1002/spy2.83.

[2] Kamdar, Nirav MD, MPP; Jalilian, Laleh MD Telemedicine: A Digital Interface for Perioperative Anesthetic Care, Anesthesia & Analgesia: February 2020 - Volume 130 - Issue 2 - p 272-275 doi: 10.1213/ANE.0000000000004513.

[3] Wang, R.C., Juang, W.S. and Lei, C.L. (2011) 'Provably secure and efficient identification and key agreement protocol with user anonymity', Journal of Computer and System Sciences, Vol. 77, No. 4, pp.790–798.

[4] Pu, Q., Wang, J. and Zhao, R. (2012) 'Strong authentication scheme for telecare medicine information systems', Journal of Medical Systems, Vol. 36, No. 4, pp.2609–2619.

[5] Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C. and Chung, Y. (2012) 'A secure authentication scheme for telecare medicine information systems', Journal of Medical Systems, Vol. 36, No. 3, pp.1529–1535.

[6] A. Shastri, R. Biswas "A Framework for Automated Database Tuning Using Dynamic SGA Parameters and Basic Operating System Utilities", Database Systems Journal vol. III, no. 4/2012.

[7] Gautam Srivastava, Jorge Crichigno, Shalini Dhar. "A Light and Secure Healthcare Blockchain for IoT Medical Devices", 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 2019.

[8] I Khanchi, E Ahmed "Automated Framework for Real-Time Sentiment Analysis", International Conference on Next Generation Computing Technologies (NGCT-2019).

[9] Singh, T., Kshitiz, K., Singh, H., Kukreja, P.: Detecting hate speech and insults on social commentary using nlp and machine learning. International Journal of Engineering Technology Science and Research 4(12), 279–285 (2017).

[10] Salman Shamshad, Muhammad Faizan Ayub, Khalid Mahmood, Saru Kumari, Shehzad Ashraf Chaudhry, Chien-

Ming Chen. "An enhanced scheme for mutual authentication for healthcare services", Digital Communications and Networks, 2021.
[11] Ahlawat, P., Biswas, S.S., “Sensors based smart healthcare framework using internet of things (IoT)”, International Journal of Scientific and Technology Research 9(2), pp. 1228-1234 (2020).
[12] Taneja, S., Ahmed, E., “I-Doctor: An IoT Based Self Patient's Health Monitoring System”, 2019 International Conference on Innovative Sustainable Computational Technologies, CISCT 2019 (2019). Ahmed H., K. Manender. K. Abdul“IoT based smart healthcare for future sustainability”, 2019 International Conference on Current and Future trends of IoT, (2019).
[13] Sharma, H.K., Khanchi, I., Agarwal, N., Seth, P., Ahlawat, P. , “Real time activity logger: A user activity detection system”, International Journal of Engineering and Advanced Technology 9(1), pp. 1991-1994 (2019).
[14] Bhushan, A., Rastogi, P., Ahmed, M.E., “I/O and memory management: Two keys for tuning RDBMS”, Proceedings on 2016 2nd International Conference on Next Generation Computing Technologies, NGCT 2016 7877416, pp. 208-214 (2017).
[15] Partha Pratim Ray, Dinesh Dash, Khaled Salah, Neeraj Kumar. "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases", IEEE Systems Journal, 2020.
[16] Nirav Kamdar, Laleh Jalilian. "Telemedicine", Anesthesia & Analgesia, 2020.
[17] Singh, Balpreet, Krishna Pal Sharma, and Nonita Sharma. "Blockchain applications, opportunities, challenges and risks: a survey." In Proceedings of the International Conference on Innovative Computing & Communications (ICICC). 2020.
[18] Yadav, Sourabh, Monika Mangla, Nonita Sharma, and Asmita Mahajan. "Blockchain framework for smart contract and distributive ledger for entity marketplace." International Journal of Blockchains and Cryptocurrencies 3, no. 2 (2022): 95-111.
[19] Sharma, Nonita, Monika Mangla, and Sachi Nandan Mohanty. "A Markov decision process-based secure consensus framework for leveraging blockchain technology in IoT applications." International Journal of Electronic Business 17, no. 3 (2022): 270-282.
[20] Singh, R., & Agarwal, B. B. “Abnormality detection and classification from brain MRI using machine learning”. International Journal of Health Sciences, (2022): 6(S3), 9170–9180.
[21] Singh, Ravendra, and Bharat Bhushan Agarwal. "An automated brain tumor classification in MR images using an enhanced convolutional neural network." International Journal of Information Technology (2022): 1-10.
[22] Yadav, Sourabh, Nonita Sharma, Monika Mangla, and Asmita Mahajan. "Blockchain and IPFS Based Framework for Secure Student Document Record Keeping." Journal of Educational Multimedia and Hypermedia 30, no. 2 (2021): 165-181.
[23] Georgios Tsaramirsis, Seyed M Buhari, Mohammed Basheri, Milos Stojmenovic."Navigating Virtual Environments Using Leg Poses and Smartphone Sensors".Multidisciplinary Digital Publishing Institute, Sensors.(2019): 299.
[24] Singh, Ravendra, and Bharat Bhushan Agarwal. "A Hybrid Approach for Detection of Brain Tumor with Levy Flight Cuckoo Search." Webology 19, no. 1 (2022).
[25] Georgios Tsaramirsis, Seyed M Buhari, Khalid Obaid Al-Shammari, Saud Ghazi, Mohd Saleem Nazmudeen, Kostandinos Tsaramirsis."Towards simulation of the classroom learning experience: Virtual reality approach”. 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom).(2016), 1343-1346.