IoT based health monitoring and record management using distributed ledger

Shanthi Makka¹, Gagandeep Arora ²and Bhargavi Mopuru³

¹,² Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology, Hyderabad, India-501301
³ Department of Computer Science and Engineering, Audisankara College of Engineering and Technology, Gudur, India

Email: dr.shanthimakka@gmail.com

Abstract. Frequent visit of doctors during pandemics is not recommended due to COVID-19 scenario. Internet of Things (IoT) based sensors can be used to measure and do certain tests at home. The blockchain-based strategy promises to aid in the delivery of health-care services while maintaining data privacy. To maintain transparency in the health record, medications, claim history, etc., up-to-date distributed ledger is required. Doctors have sometimes necessitate patients to undergo lab tests or buy drugs from those organisations merely in order to generate personal profit, even if the medical shop or pathology labs have a bad reputation. Therefore, blockchain technology provides trust among multiple parties so that any party could not be misguided. At times, the patient visits the hospital in critical condition and they may not be in situation to explain about medical history. In such scenario, the information stored in distributed ledger may be helpful to the doctors for further treatment. The medical emergencies such as cardiac arrest and breathing issues, the patient requires immediate treatment or medicine at his/her location, the intelligent drone is useful for faster delivery of medicines and needed medical accessories.

Keywords: Internet of Things (IoT), Blockchain, Internet of Medical Things (IoMT), Distributed ledger, Security, Drone.

1. Introduction

The current pandemic situation enforces the contact less service to the patients to decrease spread of COVID-19. We should also avoid visiting Hospitals so frequently. The doctors usually recommend basic tests such as blood pressure, temperature, blood oxygen, glucose, ECG, etc., according to the health problem. At the moment, body sensor devices can sense the physical condition in terms of numerical values. These sensor devices are also termed as Internet of Medical Things (IoMT) and the sensed data to be sent to the doctor who examines it and prescribes medicines. Sensor data is transmitted to the cloud server, with a smart contract blockchain structure.

Blockchain is an emerging technology [1], which provides a way for people around the world to collectively maintain a database without relying on a central authority. It's a new model for sharing and reconciling information without intervention of third party. The new blockchain technology facilitates peer-to-peer transactions without any intermediary such as a bank or governing body. Keeping the user's information anonymous, the blockchain validates [2] and keeps a permanent public ...
record of all transactions. Key concerns with blockchain applications in healthcare include: Network infrastructure security at all levels, Identity verification and authentication of all participants, Uniform patterns of authorization to access electronic health information. This suggested system could benefit the India and any country in the world because healthcare is a primary concern all over the world.

Patients can connect to any hospitals in the blockchain Network and collect their medical data [3] automatically without intervention of any external party in a secured way, timely medication delivery to home through drone and patients can discuss their problems or issues with the doctors of hospitals without any hesitation because doctor’s authenticity is already verified through miners in the network.

The Internet of Things (IoT) is a network of computing devices, mechanical and digital equipment, items, and people together with the intent of sharing data over the network without any interaction. A thing in IoT can be referred as a person or any object or any machine. All these objects connected to each other through Internet. The sensors can be used as a part of IoT devices to monitor basic health condition of a patient and can be shared with an available doctor in a blockchain network and interaction with the doctor can be done virtually to save time and not to get in to the crowd, which can lead to other diseases.

2. Proposed work

In the first phase of this work, a test bed can be prepared that includes various sensors, IoT devices, gateway, and cloud/server. The primary objective of IoT and sensors is to collect data and can create industry-ready blockchain architecture and send it to the gateway. The gateway will pre-process the data and send it to the cloud. This data is time-series data, and an intelligent method can be developed to pre-process it and determine the events from the data. With the inclusion of different IoMT sensors that detail health conditions such as temperature, blood pressure, blood sugar, heart rate, etc. Further, two types of entries can be maintained in the database: (i) routine test record (ii) extreme condition test record e.g., high/low BP, high/low blood sugar level and these details to be shared with patients and doctors. The data will store on the blockchain.

The second phase deals with creating a consortium network that will connect patients, doctors, hospitals, pathology labs, diagnostic centres, pharmacies and insurance companies. Define the roles and responsibilities along with accessibility permissions for each party. This work is extended in the third phase where it can deal with transaction logs and world state databases. Initially, dummy data to be created for testing the functionality of each party. Further, data to be taken from online sources to make the previous records of each party. It will be helpful in testing and debugging the functioning of the consortium network. In the third phase, the security aspects relevant to the IoT and Cloud will be managed using blockchain technology.

The fourth phase of this proposed work can be extended to work faster delivery of medicine or related clinical things. In this phase, drone’s prototype can be taken from the existing work, then implement the desired functionality and use it for medical purposes.

3. Underlying fundamentals of blockchain technology and IoT

Blockchain is based on a distributed ledger concept that is decentralised, digitalized, and distributed. This is more robust and secure by definition than the proprietary, centralised approaches now in use in the trade environment. The goal of blockchain is to make it possible to record and distribute digital data without the capacity to change it. The blockchain technology is proposed in 1991 with the intention of timestamp of the document could not be mitigated.

3.1 Features of blockchain

It is a repetitive practice for many organizations to fight with fraud, as per the surveys done by authorized deception investigator in each and every year a minimum of 5% of dividends are paid to the fraudsters. It is very difficult to identify the fraud or it may happen the fraud remains untouched for a longer time, timely getting hold of the fraud is very important. So, there are three features, which will help the business to put into frauds in a limited way.
Blockchain is distributed [4] A distributed digital ledger which can be classified as blockchain, this chain of blocks will adapt the data constantly and it also share it with in peer-to-peer network. As in this network there is no central authority so it will lead to no single point failure. If there is a fraud then there is no way to get the information about the fraud schemes what can be done is the endorsement mechanism to be implemented and moreover there is no proper way or place to investigate if there is a fraud in the network. As a deceiver the immoral task can be used such as deletion or modification of finance system of company by different methods. Changing the copy, which may be available in the soft or hard form of document to generate the crooked records. To improve the clarity in the digital ledger the use of shared or may be a common ledger, which will lead to decrease the frauds between different business or a network of businesses. The identification [5] in a network is easy because everyone in the network can see each and every transaction and moreover there are people from group only who are handling the network.

Blockchain is immutable, because there is no right with us to remove or change the digital ledger. As this process is defined in such a way the blocks, which are used for transaction, in turn, they are attached to the blockchain will be granted as the valid transaction if and only if it is approved by the associate members. The block is given a timestamp, which is encrypted, and it is linked to the block before it in the chain. It can, however, construct a new transaction to change the state of a service; it will be frankly added into the chain, and the file's primitive transcript [6] will remain available. This means by using the blockchain it can construct a transactional flow that will state from where these transactions are, where they are destined to and who is controlling these transactions.

![Figure1](image)

**Figure1.** Digital identity using blockchain [2]

The concept of immutability was first proposed by blockchain. It forbids the creation of anything written in a ledger, and you don't have to worry about your transaction information being protected because the blockchain works by attaching to multiple flaws to keep your data safe and secure. It can't be hacked by any hacker who wants to try due to the deception of blockchain.
Blockchain ledgers start with a single transaction or a series of transactions including funds, cryptocurrency [7], data, and agreement. The transaction is executed and the transaction is recorded once it has been validated. The produced object on blockchain is irreversible. Blockchain's immutability is enabled through the network effect. The frequency of utilisation determines a network's efficiency. The capacity to be immutable and safe is a crucial aspect of blockchain. The things are getting changed very rapidly in the area of cyber security. Permissions can be set up on a blockchain [8]. Permissions play a significant role in this scenario. However, unlike the other features can be covered, every blockchain network is not permissioned but a Permissioned network can be quite useful for deception prevention because they restrict who is allowed to participate and at what capacity, as well as their limitations. The permissioned network [9] member's contribution can begin once the network has been established.

Identity management and network access control play a big role in a permissioned network [10]. The blockchain framework is deployed in the Linux foundation, and all participants are issued with hyper ledger fabric and encrypted membership cards, they can prove their identity. They can use their designated membership card to access transactions that pertain to them as a part of digital identity shown in Figure 1. Even wise people are unable to add record and they can't damage any records because they're all encrypted, thus they can't add a record to the blockchain without consensus. As far as operational risks go in 2017, any type of fraud can be overlooked; it is highly costly, and it also lowers staff morale and creates an unclear business environment, as well as severing your business and customer ties.

![Figure 2. Properties of distributed ledger](image)

3.2 Security through blockchain

As its framework, a blockchain network [11] is more secure, and you must build out of stage for categorization. While establishing a private blockchain, despite the fact that the blockchain has built-in security feature depicted in Figure 2, by keeping data on the cloud, with malicious intent can exploit known flaws in your architecture. You must have a solid foundation with a unified security system. To put it another way, you need a solid foundation with unified security that can prevent anyone, including core users and supervisors, from accessing confidential data and defend against unwanted attempts to change data or network functionality. Encrypted keys [12] should be carefully escorted with high-level security measures to avoid misappropriation with multiple security layers as shown in Figure 3.
With this skill, your blockchain network will have the extra protection it needs to fend off attacks from within and beyond. An industry-ready blockchain architecture [13] can be created to aid in the advancement, administration, and practices of a multiorganizational business network. As stated in earlier sections, blockchain is nothing more than a chain of blocks, each of which contains a collection of records known as transactions, and each block is linked to the rest of the chain by a previous and next hash pointer. It is hard for hackers to damage [14] any record since they want the hash address of that block as well as all other blocks linked to it. This may not appear to be much of a deterrent on its own, but blockchain also has certain other important aspects that give further protection.

3.3 Blockchain Security with IoT
Consider an IoT network with centralised authority. It refers to devices as smart using sketches, and they are probably not allowed to make safeguarding decisions without the help of the central authority. The whole set of data, as well as each tool and 136 Security formations in digital transformation data as a result of blockchain, is accumulated in the blockchain model. Before inserting any data into the network, the hacker must gather all essential resources for a DNS attack, which must be confirmed and certified by each node in the network, because it allows deposits to be made without the use of a bank or a negotiator.

A blockchain can be used for a variety of financial purposes, including electronic assets, reimbursement, and online payment. In addition, it can be used in various domains such as IoT, smart investments [15], and public services. An IoT, it appears, is no longer limited to a single node. In the
world of IoT, an advanced and, as previously stated, amorphous stage of evolution that might be a
good idea for those who can see the capacity of combining blockchain security [16] with anchored
security. In fact, IoT poses a more serious warning than cryptocurrency, in which a distributed
network [17] is tasked with transferring money from one anonymous owner to another. To
authenticate, defend, and govern all the levels of a whole network, a complicated structure is required.

4. Proposed architecture
A private blockchain or permissioned blockchain is used to connect Hospitals, patients,
pharmaceutical companies, doctors and IoT based health-monitoring system into a single network. The
miners verify the authentication of all the components in blockchain and entry of new block in to
the network is permitted by the existing members of a network using Proof of Work (PoW) consensus
algorithm [18]. Whenever a request for a new block arises, the miners will be assigned with a puzzle
to solve and whoever solves first with maximum accuracy will be given a chance to add block in to
network.

Figure 4. Proposed architecture of healthcare blockchain
Hash address for the new block will be generated once the miner got an opportunity to insert block and permission by the existing blocks in network is achieved and through this hash address new block will be connected with the existing block in the network. All the records or blocks are stored in ledger; whenever a block is added or any transaction or activity took place will dynamically reflect in all the blocks in the network. Thereafter entry of malicious users can be 100% restricted, but if any block in existing network will turn as a malicious user, then a voting from all the blocks to be taken before consideration of any block or decision in the network. We have to make sure that malicious activity users should not be more than 2/3 of blocks in the network. Distributed ledger is Immutable, Distributed, Time stamped, secured, anonymous, and programmable which lead to the easy identification of malicious activities in the network. A distributed ledger is basically a database connected multiple nodes and it can also represent the data in different ways in each ledger.

In proposed model in Figure 4, the people who are healthy or unhealthy can contact the doctors in the blockchain or they can contact the hospitals in the network for their treatment or to avail the medicine delivery at footstep without visiting anywhere. The reason for choosing such architecture is to decrease spread of diseases from one to other and also current pandemic situation expects the same from us.

User can self-measure simple tests at home by using IoT based kit which has different sensors for making blood tests, oxygen levels, hearth beat levels and etc., then these reports can be shared to the hospitals or the doctors in the network for further suggestions. If a doctors can suggest certain medicines without calling the patients to the hospitals, they would suggest medicines and will be provided at doorstep. In many countries to lose our family members due to non-availability of medicines at right time. Due to traffic or any other technical issue, there may delay in delivery of medicines, to overcome such situations, the proposed drone-based delivery of medication to the patients is benefitted. Patients will not bother about the authenticity of doctors and hospitals because all these people are already authenticated or verified by the miners and other members in the network.

Patient has to bother about their illness not about doctors and hospitals.

5. Anticipated outcomes
The proposed work guarantees an effective and safer mode for delivery of medication to the patients in remote locations. A low-cost testing kit will be available for monitoring the patient’s condition. Each party of consortium network could track and verify the segments of information such as patient’s health condition, medical history, test reports, doctors’ profile and treatment history, hospitals’ profile and history, facilities available in hospitals, patient’s recovery rate in specific hospital, doctors’ prescriptions, diagnostic centre’s profile and facilities, supply chain of medicines, insurance companies’ profile and trustability on claims, insurance plan and claim records. Further, drone-based delivery of medicines and other required materials would provide a faster and safer way of treatment.

6. Applications of a healthcare blockchain
This work can be beneficial for all the parties related to the healthcare system[19],[20] such as patients, hospitals, doctors, diagnostic centres, insurance companies and government to get updated information and maintaining the trust between them and also guarantees transparency in treatment of patients. Blockchain technology is distributed in nature, hence, safe from a single point of failure. The patient could start his/her treatment from a remote location without visiting the hospitals. It may reduce the patient’s expenses. The distributed ledger [21] contains medical history of patients, so quick treatment can be provided even though the patient is not in a condition to speak. As distributed ledger gets updates in a dynamic manner, so the record updating can be monitored and accessed by the hospitals at any point of time and doctors could track the current condition of patients and categorize them as high priority (critical condition) and low priority patients.

The proposed idea based on blockchain technology [22],[23] gives assurance to the secure transfer of data received from IoT-based sensors used for monitoring of remote patient by the healthcare
professionals. Further, they can use data for research and analysis purposes. Pharmaceutical companies and pharmacies can track the medicine requirement at different locations. If it seems that any location is having a scarcity of medicine or other medical accessories they can decide on quick supply for the same. Internet of Things companies can get authentic data to research and development of new devices which may beneficial for patients, hospitals, doctors, diagnostic centres and insurance companies [25],[26]. The government can get a single view of all data and monitor hospitals, doctors, pharmacies, diagnostic centres, insurance companies and some diseases in a specific area. The Government can get quick reference [27] to the data about the areas which are getting affected by any virus, any specific diseases and any pandemic situations. As patient’s information is updated on distributed ledger dynamically, the organizations can take quick decisions [28] or implement policies specific to those affected areas instead of getting in to the complete shut down situations. Blockchain offers the ability to create a single system for securely storing and retrieving health records by authorised users in a timely and safe manner. By avoiding miscommunication between different healthcare [29],[30] staff involved in caring for the same patient, many mistakes can be prevented, faster diagnosis and interventions can be performed, and care can be tailored to each patient.

7. Conclusion and future Scope
The Proposed architecture can use the Internet of Medical Things sensor devices and test in the real environment and design a consortium network by connecting patients, hospitals, pathology labs, diagnostic centres, pharmacies and insurance companies. Maintaining distributed hyper ledger to keep transactions log and world state databases and maintenance of cloud security and IoT security aspects. Setup drone’s functionality for medicines delivery. Web platform for GUI can be developed and also further phases can deal with creating interactive easy to use web and android applications to facilitate the maximum number of patients. The people tremendously increase the usage of mobile phones, so app developments for the various operating systems can facilitate most of the users.

References
[1] Hölbl, M., Kompara, M., Kamišalić, A., & NemečZlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. Symmetry, 10(10), 470.
[2] Makka, S., Arora, G., & Sagar, B. B. (2020). Consequent Formation in Security With blockchain in Digital Transformation. In S. Goundar, S. Bhusan, & V. Thukare (Ed.), Impact of Digital Transformation on Security Policies and Standards (pp. 122-144). IGI Global. http://doi:10.4018/978-1-7998-2367-4.ch008.
[3] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016, August). A Case Study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data. In Proceedings of IEEE open & big data conference (Vol. 13, p. 13).
[4] McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62-75.
[5] Bell, L., Buchanan, W. J., Cameron, J., & Lo, O. (2018). Applications of blockchain within healthcare. blockchain in healthcare today, 1(8).
[6] Rathee, G., Sharma, A., Saini, H., Kumar, R. and Iqbal, R., 2020. A hybrid framework for multimedia data processing in Internet of Things (IoT)-healthcare using blockchain technology. Multimedia Tools and Applications, 79(15), pp.9711-9733.
[7] Yazdinejad, A., Srivastava, G., Parizi, R. M., Delghanthanta, A., Choo, K. K. R. and Aledhari, M., 2020. Decentralized authentication of distributed patients in hospital networks using blockchain. IEEE journal of biomedical and health informatics, 24(8), pp.2146-2156.
[8] Khezr, S., Moniruzzaman, M., Yassine, A. and Benlami, R., 2019. blockchain technology in healthcare: A comprehensive review and directions for future research. Applied sciences, 9(9).p.1736.
[9] Kumar, R., Marchang, N. and Tripathi, R., 2020, January. Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and blockchain. In 2020 International Conference on Communication Systems & Networks (COMSNETS) (pp. 1-5). IEEE.
[10] Kumar, R. and Tripathi, R., 2021. Towards design and implementation of security and privacy framework for Internet of Medical Things (Internet of Medical Things (IoMT)) by leveraging blockchain and IPFSTechnology. The Journal of Supercomputing, pp.1-40.
[11] Ni, W., Huang, X., Zhang, J. and Yu, R., 2019, July. HealChain: A Decentralized Data Management System for Mobile
9

healthcare Using Consortium blockchain. In 2019 Chinese Control Conference (CCC) (pp. 6333-6338). IEEE.

[12] Scott, J.E. and Scott, C.H., 2019. Models for drone delivery of medications and other healthcare items. *Unmanned aerial vehicles: Breakthroughs in research and practice*, pp.376-392.

[13] Scott, J. and Scott, C., 2017, January. Drone delivery models for healthcare. In *Proceedings of The 50th Hawaii international conference on system sciences*. pp. 3297-3304, doi: 10.24251/HICSS.2017.399

[14] Chen, H., Hu, Z. and Solak, S., 2021. Improved delivery policies for future drone-based delivery systems. *European Journal of Operational Research*.

[15] Hasselgren, A., Kraljevska, K., Gigoroski, D., Pedersen, S. A., &Faxvaag, A. (2020). blockchaininhealthcare and health sciences—A scoping review. *International Journal of Medical Informatics, 134*, 104040.

[16] Kassab, M. H., DeFranco, J., Malas, T., Laplante, P., &Neto, V. V. G. (2019). Exploring researchin blockchain for healthcare and a roadmap for the future. *IEEE Transactions on Emerging Topics in Computing*, 1, 91-101.

[17] Katuwal, G. J., Pandey, S., Hennessey, M., &Lamichhane, B. (2018). Applications of blockchainin healthcare: current landscape & challenges. arXiv preprint arXiv:1812.02776.

[18] Zhang, M., &Ji, Y. (2018).blockchain for healthcare records: A data perspective. *PeerJ Preprints*, 6, e2694v1.

[19] Dhillon, V., Metcalf, D., & Hooper, M. (2021).blockchain in healthcare. In *blockchain enabled applications* (pp. 201-220). Apress, Berkeley, CA.

[20] K. Verma, S. Bhardwaj, R. Arya, M.S.U. Islam, M. Bhushan, A. Kumar, and P. Samant, “Latest tools for data mining and machine learning”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 8, no. 9S, pp. 18-23, ISSN: 2278-3075, 2019. Available https://doi.org/10.35940/ijitee.I1003.0789S19

[21] ReshamArya, Ashok Kumar, and MeghaBhushan, Affect Recognition using Brain Signals: A Survey. In: Singh V., Asari V.K., Kumar S., Patel R.B. (eds) Computational Methods and Data Engineering. Advances in Intelligent Systems and Computing, vol 1257, 2021.Springer, Singapore. https://doi.org/10.1007/978-981-15-7907-3_40

[22] MonikaMangla, Ashok Kumar, Vaishali Mehta, MeghaBhushan and SachiNandanMohanty, Real-Life Applications of the Internet of Things: Challenges, Applications, and Advances, CRC Press, Taylor&FrancisGroup, 9781774638477, January 2022. Available at:https://www.appleacademicpress.com/real-life-applications-of-internet-of-thingschallenges-applications-and-advances/9781774638477

[23] Shagun Sharma, Ashok Kumar, MeghaBhushan, NitinGoyal, SaileshSuryanarayanyer, “Is Blockchain Technology Secure to Work On? In Blockchain and AI Technology in the Industrial Internet of Things. edited by Subhendu Kumar Pani , Sian Lun Lau , and Xingcheng Liu, 66-80. Hershey, PA: IGI Global, 2021. http://doi:10.4018/978-1-7998-6694-7.ch005

[24] SayeedAkhunumPathan, MeghaBhushan, Anita Bai, A Study on Health Care using Data Mining Techniques. *Journal of Critical Reviews*, 7 (19), 7877-7890, 2020. doi:10.31838/jcr.07.19.896

[25] VikramJeet Singh, MeghaBhushan, Vikram Kumar, KishoriLalBansal, Optimization of Segment Size Assuring Application Perceived QoS in Healthcare, *Lecture Notes in Engineering and Computer Science, World Congress on Engineering 2015, London, United Kingdom, volume 2217, no. 1, 2015*, pp. 274-278.

[26] Shkaraputa Alexander, P., Alekseev, A., Erakhtina, O., Kondratyeva, K., &Nikitin, T. (1794). Peer review declaration. In *Journal of Physics: Conference Series* (Vol. 2021, p. 011002).

[27] Wang, Y., Huang, W., Yu, J., Chen, K., & Wang, F. (2020, October). Data privacy protection method of internet of things based on blockchain technology. In *Journal of Physics: Conference Series* (Vol. 1651, No. 1, p. 012068). IOP Publishing.

[28] Liang, N. (2020, June). Data Sharing Model of Internet of Things Based on Blockchain. In *Journal of Physics: Conference Series* (Vol. 1574, No. 5, p. 052064). IOP Publishing.

[29] Sun, Y., Chen, W., Chen, L., & Li, M. (2021). Research on Clustering Management of Power Distribution Internet of Things Based on Trusted Blockchain. In *Journal of Physics: Conference Series* (Vol. 1748, No. 5, p. 052064). IOP Publishing.