BLOCKCHAIN ARCHITECTURE TO MEET CHALLENGES IN MANAGEMENT OF ELECTRONIC HEALTH RECORDS IN IOT BASED HEALTHCARE SYSTEMS

Maria Arif, Megha Kuliha and Sunita Varma

Department of Information Technology, S.G.S.I.T.S., Indore, M.P., India

ABSTRACT

Secure, immutable and transparent feature of blockchain has led researchers to find ways to harness its potential in sectors other than financial services. Blockchain is emerging as a popular tool to help solve some of the healthcare industry's age-old problems that have resulted in delayed treatments, inaccessible health records in emergency, wasteful spending and higher costs for doctors, health care providers, insurers and patients. Applying blockchain in healthcare brings a new challenge of integrating blockchain with Internet of Things (IoT) networks as sensor based medical and wearable devices are now used to gather information about the health of a patient and provide it to medical applications using wireless networking. This paper proposes an architecture that would provide a decentralized, secure, immutable, transparent, scalable and traceable system for management and access control of electronic health records (EHRs) through the use of consortium blockchain, smart contracts, proof-of-authentication (PoAh) consensus protocol and decentralized cloud.

KEYWORDS

Blockchain, Proof of Authentication, Smart Contracts, Internet of Things, Healthcare

1. INTRODUCTION

Safe and effective healthcare require good quality, complete, up-to-date and accurate medical records for doctors and hospital staff to make timely decisions, to improve quality of care, to develop new ways of predicting and diagnosing illness. At present, many healthcare systems still use papers and files to maintain records that often lead to delays in accessing data and hence, in providing treatment. Even where records are stored digitally as electronic health records (EHR), they mostly have server/client centralized model where server has huge pressure in terms of storage and computing, and also poses a single point of failure.

In 2019, it was reported that approximately 18 % of patient health records are duplicates and roughly one in five patients have mismatched health records, providing doctors an imperfect view of their medical history, thus resulting in delayed, improper treatment and unnecessary repeated testing. Another major concern is that though bulk of data repositories are owned by healthcare providers, pharmaceutical companies, and other stakeholders in the health and medical ecosystem, yet they do not interact with one another. This leads to non-availability of a patient’s medical history to health providers in emergency cases. Sharing data between hospitals can allow for reduced costs and improved patient outcomes across hospital systems but presently, organizations and researchers cannot benefit from data sharing as patient’s privacy is at stake.

David C. Wyld et al. (Eds): MLIOB, SIPO, NET, DNLP, SOEA, AISCA - 2021
Pp.49-63, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.111204

The world is witnessing an increasing number of medical records breach every year, with over 20 million breaches records in 2019 alone. The term “Medical Theft” was introduced by the World Privacy Forum (WPF) in 2006 for the illegal access and use of a patient's personally identifiable information to obtain medical treatment, services or goods. In most cases, name or health insurance numbers were used to see a doctor or get prescription drugs and in others, medical providers submitted false insurance claims for services not provided. Blockchain, if used in a well-planned architecture, can prove to be a boon to address the above issues.

Blockchain is an open, distributed, append-only public ledger technology. It consists of a chain of blocks that maintains the digitally signed transactions of the users in a verifiable and permanent way[1]. It doesn’t require the need of any central authority as the participating nodes in the network are themselves responsible for its maintenance through the use of consensus protocol which ensures that a block is added only after it has been validated by the majority of nodes. Each node in the network keeps an updated copy of the whole blockchain, ensuring consistency of the data among all nodes and protection against malicious attacks. A block once added to the blockchain cannot be altered and any changes to be made it are stored as new transactions in a new block added at the end of the blockchain, keeping the original copy intact. Hence, it ensures traceability and accountability. All the blocks are interconnected using hash values, so that any tampering with the data is easily reflected in the consequent blocks. An important feature of blockchain is the user’s anonymity which is achieved by concealing their true identity as each user is identified by their public addresses. This provides transparency in the network and allows data to be viewed and shared by all the nodes in the network.

The most common consensus protocols used today, ex. Proof of Work (PoW), have high latency in creation of a new block. Such protocols are infeasible to be used in healthcare system as IoT devices, that require fast data processing, have become an indispensable part of every healthcare system today. Others introduce some centralization, defeating the whole purpose of using a blockchain. For example, Proof of Stake (PoS) where more the number of tokens, more the power to create a block.

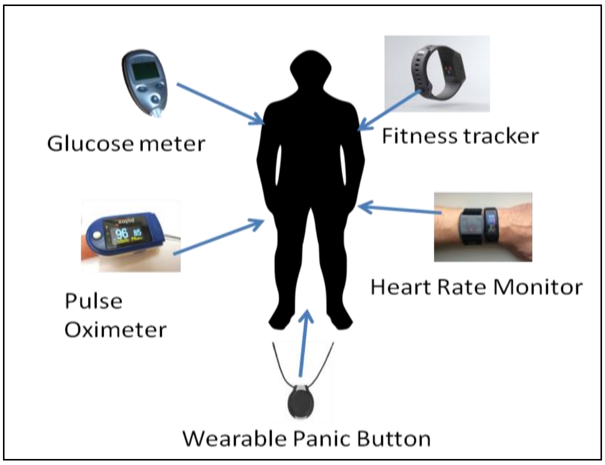


Figure 1. Role of IoT in Healthcare

The Internet of things refers to the network of physical entities that are embedded with sensors, software, and other technologies for collecting and exchanging data with other devices and systems over the internet. IoT has provided a great opportunity to build powerful industrial systems and applications by using the growing ubiquity of radio-frequency Identification (RFID) and wireless, mobile, and sensor devices [2]. Medical care and health care represent one of the most attractive application areas for the IoT. IoT devices are used for tracking various medical issues such as electrocardiogram, blood pressure, asthma, blood sugar and so on as shown in Figure 1. The IoT has the potential to give rise to many medical applications such as remote health monitoring, fitness programs, chronic diseases, and elderly care. IoT-based healthcare services would reduce cost and increase the quality of life. But integrating the blockchain with IoT devices, which are constrained in terms of storage and computational power, brings new set of challenges.

This paper discusses these challenges and how the proposed architecture overcomes them. The remainder of this paper is organized as follows:

Section 2 discusses the related work done in this area. Section 3 discusses the structure and working of a block chain along with the benefits and challenges of integrating it with IoT in healthcare systems. Section 4 describes the architecture and workflow of the proposed model. Section 5 discusses how two blockchains were implemented based on two different consensus protocols to justify the use of proposed protocol. Section 6 presents the observed results which are discussed further in section 7. Section 8 concludes the paper by specifying the features of the proposed model that makes it fit for a secure and transparent healthcare system.

2. RELATED WORK

There have been many researches on blockchian recently. Ref. [3] surveys advances in IoT-based health care technologies and reviews the state-of-the-art network architectures/platforms, applications, and industrial trends in IoT-based health care systems. In [4] authors propose a blockchain based IoT model for medical device transactions and communication using Inter Planetary File System for storing and sharing data but they don’t take into account the cost incurred by energy and time requirements of PoW protocol used for mining. Ref. [5] discuss the opportunities that blockchain offers in the field of healthcare e.g., in public health management, user-oriented medical research based on personal patient data as well as drug counterfeiting. A systematic review of the usual consensus algorithms used in the blockchain and analysis of their performance with respect to verification speed, throughput, scalability and fault tolerance has been made in [6]. In [7], authors have outlined and mapped 66 consensus protocols for private and public blockchains. The authors in [8] propose a decentralized healthcare blockchain for IoT using light weight digital signature scheme but no implementation of the same exists ensuring the low latency desired in IoT. We use the decentralized cloud model in our model inspired by them. In [9,10] authors present a novel consensus algorithm called Proof-of-Authentication (PoAh) for resource-constrained distributed systems such as the Internet of Things (IoT), edge computing and fog computing to make the blockchain application-specific. They implemented and proved that PoAh, while running in limited computer resources, has latency in the order of few seconds and is faster than PoW which is used in traditional blockchain. After considering many consensus protocols, we found PoAh to be the most apt protocol for a secure and fast data processing.

3. INTEGRATION OF BLOCKCHAIN WITH IOT

3.1. Structure and Working of Blockchain

Blockchain is a chain of interconnected blocks where each block contains data in form of multiple transactions between the nodes that are part of the network. Each block contains the transactions that occurred after the last block was added to the blockchain. The data of a particular block, when fed as input to a hashing algorithm, produces a hash that is unique to that block. This hash is also stored as a part of the block. SHA-256 is the mostly used cryptographic hash function as it produces a 256- bit(32 bytes) one-way hash i.e. if the hash is known it is practically impossible to know the original data. And even a minute change in the input produces a totally different output hash. Thus, the hash serves as the fingerprint of the block.

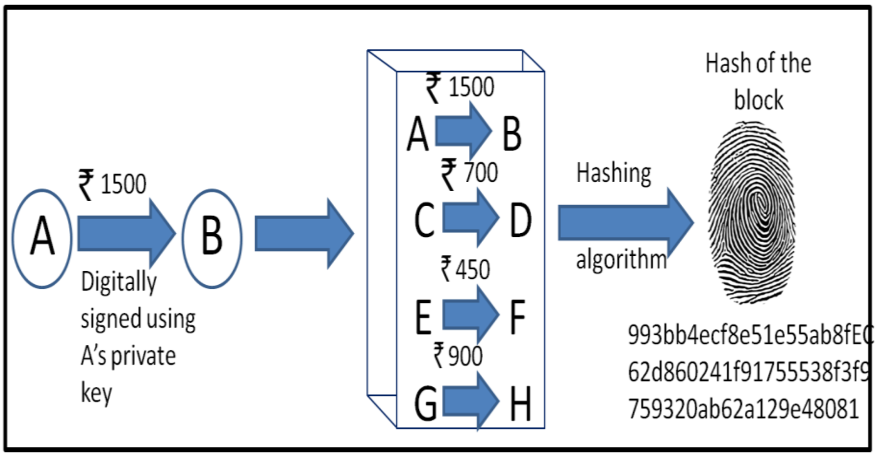


Figure 2. Pending transactions to be added to next block

Fig 2 shows how a transaction between two parties A and B is recorded in a block. Apart from data and hash, each block also contains a unique index, timestamp when it was created/ mined, a random integer nonce, and the hash of the previous block. Thus, all the blocks are connected via the hashes such that, any tampering with data in a block causes the hash to change. This renders the hash of that block stored in subsequent block, as the hash of the previous block, invalid. This provides immutability of data once stored in the blockchain and protects it against any malicious attack.

Fig 3 shows the structure of a blockchain. Each user in the network also has a unique pair of his private key (PrK) and public key (PuK). The PrK is kept as a secret whereas the PuK is known to all and also serves as the unique address of the user, hiding his true identity. The sender digitally signs (encrypts) the transaction with his PrK. The transaction is broadcasted to all the nodes in the network to be stored as pending transaction. The receivers use the PuK of the sender to authenticate the transaction. Multiple such transactions form data for the next block to be added to the blockchain.

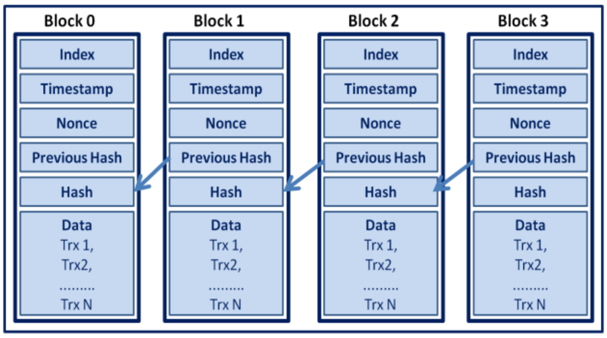


Figure 3. Structure of a blockchain

Every block needs to get consensus from majority of nodes in network before it is added to the blockchain. The process by which the nodes come at consensus at validity of the block to be added is called consensus protocol. Different such protocols exist, the most commonly used being

PoW in which all the participants of the network compete to create a block. This process is called mining, where miners (competing nodes) try to solve a computationally extensive mathematical puzzle. The puzzle is to guess a random number, nonce, such that hash obtained by sha256 (sha256 (data + nonce)) begins with a number of 0s (say seventeen, ex:000000000000000001422882355385290563fe84da5f0a5aa4832e8 5f68b1b5), according to the difficulty level. The only way a miner can find the number is by guessing, *i.e.* trying millions of random numbers. The one who solves the puzzle first, gets to mine (create) the block. The winner creates the block by adding the pending transactions, index, hash, timestamp, nonce and the hash of the previous block. The newly mined block is then broadcasted to all other nodes to be validated. All the nodes then check the index of the block with the one they expect, calculate and check the hash of the block, and also match the hash in the hash of the previous block field in the new block with the hash of the last block stored in their blockchain. If the block is validated by the majority of the nodes, consensus is reached and the block is added by all the nodes to their respective blockchains. This way same updated copy of blockchain is stored at all nodes, ensuring consistency. The winner who mines the block gets rewarded (with cryptocurrency in bitcoin network) for devoting its computational energy and time. If any node goes down for any reason, it broadcasts the request for the latest blockchain and stores the one which is the longest.

The consensus protocol safeguards the blockchain from malicious activity of the hacker as he may be required to devote a huge computational power and time to solve the puzzle to be able to mine the block. Apart from that he would require majority of nodes to validate his block, which would be practically infeasible for him. The protocol explained above is called Proof of Work (PoW), and is the mostly used consensus protocol in blockchains. Typically, it takes around 10 minutes for a new block to be added to the blockchain with consent from majority of the nodes.

3.2. Benefits of Blockchain Based IoT Systems

The IoT still remains in its infancy in the healthcare field due to various challenges that it imposes, the most significant being the security risk that comes with large amount of sensitive data stored in a single centralized database. Others being the issues of interoperability, scalability, flexibility, and energy efficiency [11], [12]. To address such concerns, blockchain can be a boon for IoT [13]. If IoT network is combined with the blockchain, it would provide a secure, fault tolerant, consistent healthcare system that would:

- allow storing and sharing health data securely and transparently
- enhance the accessibility of patient information in real-time
- allow secure data sharing
- ensure data integrity i.e. not changed, destroyed, or removed.
- Provide patients the control to access their data; however, they themselves won't be able to alter it either.
- ensure consistency in the patient records and increase their availability across the institutional boundaries as they may provide vital information to healthcare professionals, medical practitioners and researchers.
- guarantee medical care in emergency situations resulting in reduced suffering and medical expenses.
- aid in secure management and analysis of healthcare big data.

3.3. Challenges

Implementing blockchain with IOT may seem to be a perfect solution for healthcare systems to store highly private patient's data. But combining the two technologies brings lots of new challenges as IOT devices have very limited storage capacity, computational power and bandwidth, whereas blockchain is computationally expensive, demands high bandwidth and storage capacity. These challenges are discussed below:

- *Scalability Issue*: IoT systems usually contain a large number of nodes. But with increasing nodes the blockchain would require more time for transaction verification and block validation.
- *Computational Capacity*: Computationally intensive Proof of Work consensus protocol in blockchain is a challenge for resource restricted IoT devices.
- *Time Consumption*: While low latency is highly desirable in most of the IoT devices that generate new data about patient’s health at high frequency, mining process is highly time consuming. If this data takes too long to appear on blockchain and become available for healthcare providers, it may lead to a critical situation for the patient in emergency situations.
- *Storage Requirements*: Ever-increasing blockchain ledger has to be stored on the nodes themselves. On the contrary, IoT devices are storage constraint and usually use cloud services to extend their storage requirements. Cloud computing is based on a centralized structure whereas the whole purpose of using a blockchain is to provide a decentralized network without any central authority.
- *Access Control of Data*: Most blockchains implemented today are public/open, where anyone can join the network without the need of any permission and can access all the data stored. An important question arises here - how to provide access control to highly-classified and sensitive medical data where anyone can come in and become a part of it? Moreover, each patient may wish to share different part of his/her data with different organizations. For example, he/she may wish to make all of his/her data available to hospitals or health care providers, but only some fraction of it to insurance company or researchers.

The proposed model takes into account all the above challenges to the integrate blockchain with IoT for a healthcare network.

4. The Proposed Model

4.1. Meeting the Challenges

To resolve the challenges discussed in the last section, the proposed model uses consortium blockchain, Proof of Authentication consensus protocol, decentralized cloud and smart contracts. Each of these is discussed in detail in this section.

4.1.1. Consortium Blockchain for Scalability

There are three main types of blockchains [14]:

- *Public/Permissionless blockchain* networks like bitcoin are completely open. These networks allow anyone to join the network without the need of any permission. Everyone in the network has full right to access all the stored data and to take part in transaction verification and consensus protocol for block validation. However, they are not the best candidate for storage and transmission of sensitive information such as healthcare records because the sole purpose of public blockchains is not to provide confidentiality but rather to allow for a publicly accessible, verifiable and unforgeable storage of data [15]. Large number of nodes taking part in consensus would result in delay in addition of blocks to blockchain.

- *Private Blockchains* are blockchains where write permissions are kept centralized to one organization/entity whereas read permissions may be public or restricted to an arbitrary extent. It is equipped with the lowest degree of openness, with a high level of access control and authority management. But the healthcare systems require openness and data sharing among multiple organizations like hospitals, researchers and insurance companies.
- C*onsortium Blockchains* are less open than the public blockchains. Only authenticated members can join the network and get access to the data recorded on the ledger. It may be apt for use in application across multiple organizations in terms of suitable degree of openness and high security. Using consortium blockchain for healthcare systems can ensure that only medical related organizations can be a part of the network and that patient's records will be in safe hands. Limiting the number of participants would result in fast transactions, privacy and high security.

4.1.2. Proof of Authentication for Time and Computational Constraint

The consensus protocol should be chosen after considering the sector requirements and deployment environment. The consensus in public environment needs to be complex and must include incentives and severe penalties for the participant nodes to ensure integrity of the network and to prevent the network from fraudulent nodes as the environment here is untrusted. Therefore, security in public blockchains is achieved at the cost of speed and scalability. On the other hand, in a private environment with trusted participating nodes, the consensus protocols can be simple and also do not require a reward mechanism as the participating nodes have business interests to protect and secure the network, therefore can focus more on speed and scalability.

The proposed model uses PoAh as a consensus protocol. Authentication uses fewer resources and less energy than other mechanisms, which can be highly advantageous in case of a resource-constrained environment like IoT architectures. PoAh utilizes minimal resources for block validation, minimal time compared to PoW without compromising security threats and it provides substantial security while integrating a blockchain based decentralized security solution to the IoT [16,17]. The working of the same is described below:

- Every participating node generates a for public-private key pair (PuK-PrK)
- There are some predetermined trusted nodes known as validators. These are initialized during the network deployment with a minimum threshold trust value, th and other network nodes with a zero trust value, tr = 0
- Network participants generate transactions with the sensed or collected data from IoT devices to form a block.
- The network users broadcast their public key, PuK, to the network and sign the block using their own private key PrK
- The nodes broadcast the blocks to the validators for validation.
- Upon receiving the block for validation, the validators authenticate the block using PuK of the sender, check the *hash of the previous block* field against the *hash* of the last block in the blockchain stored at their end and check the index expected.
- After successful authentication, validated blocks are broadcasted back to the network with the PoAh id of the validator.
- On receiving the block, the network nodes verify the PoAh information to add blocks into the chain.
- To avoid centralization of power in hands of validators, with every successful block authentication, a validator's trust value is increased by 1. Each fake block authentication decreases the trust value by 1.

- Thus, a trusted node can be out of the validation process when its trust value drops below the threshold trust value, and a normal node can be a part of the authentication process.

4.1.3. Decentralized Cloud for Storage Constraint

Most of the storage constraint IoT devices use cloud services to store the massive amount of high frequency data they generate in real time. Cloud computing is centralized as the cloud providers allow users to access the applications and computing power of their servers while also retaining complete control over those resources and their data. 80% of organizations suffered at least one cloud data breach in the past 18 months, while 43% of companies reported 10 or more cloud data breaches [18]. This may raise a question about the privacy of patient's health data. Instead of storing data directly over cloud, using blockchain at cloud level to store encrypted data may result in a decentralized cloud. The intermediate layers like patient's laptop, doctor'scomputer etc., connected with the IoT devices need not store the whole blockchain but only the hashes of the block stored at the cloud. After a block is added to the blockchain on cloud, its hash is sent back to the intermediate layer. This way any change or deletion in data would result in change of hashes which would be easily reflected at the intermediate layer, which keeps a record of hashes of all the blocks. This eliminates the need of any third party trust, because any changes in data could be easily traceable. Use of such a decentralized cloud has been proposed in this paper to overcome storage constraint and provide additional data securityas on cloud, data files are broken into fragments, encrypted and stored at multiple nodes.

4.1.4. Smart Contracts for Access Control

Access control is an essential part of the EHR and provides confidentiality by checking if a user has the required rights to access the requested resources. To assure access control of data in blockchain, which otherwise is open to all its participants, the proposed model uses smart contracts. These are lines of code (if/then statements) that are stored on a blockchain and are automatically executed when predetermined terms and conditions are met. Participants to a blockchain determine how transactions and their data are represented to other participants, agree on the rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes. Each participant (patient, healthcare provider, etc.) defines it smart contract when it registers with the network. This includes stating which part of the data would be visible to others and also states the events to be triggered in case of exceptions. As it is too stored in the blockchain, any attempt to malicious access by tampering the smart contract would be immediately visible to all. Thus, smart contracts would provide access control without the need of any central authority.

4.2. Architecture of the Proposed Model

Figure 4 shows the architecture of the proposed model.

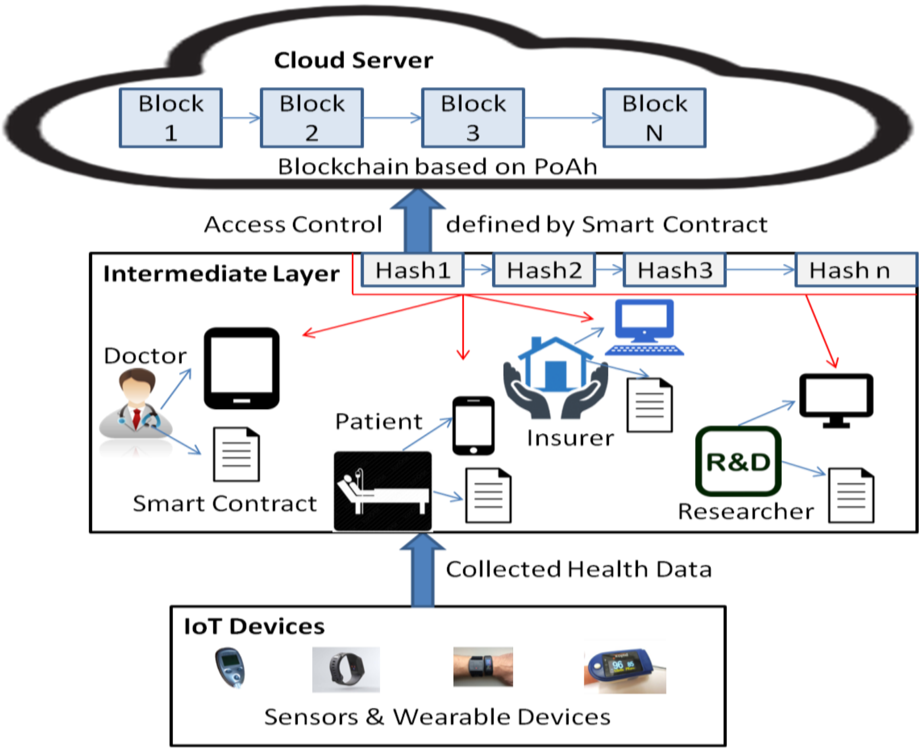


Figure 4. Architecture of the proposed model

The first layer comprises of the wearable IoT devices that collect data about the patient's health using various sensors. These may include blood pressure, heart rate or glucose monitor. The collected data is personal to the patient and can be stored on his smartphone, tablet or laptop. Each patient defines a smart contract at the time of registration. The next layer includes all the registered nodes that are the part of the network i.e. the patient, doctor, insurance provider or researcher. This layer stores only the hashes of all the blocks in the blockchain. Data from IoT devices are matched against the values specified in the smart contract and the specified event is triggered. The patient may also decide to share data with the others nodes. These actions would result in new transactions that would be broadcasted to all. The new block created would be sent and stored at the cloud. The cloud forms the next layer. This is where the whole blockchain is kept. After a new block is stored, its hash is sent back to all the nodes at the intermediate layer. The next layer comprises of the healthcare application, which is used by all the nodes to register themselves to the network, initiate various transactions and to access the blockchain data which they are authorized to. Figure 5 shows the design of the proposed model.

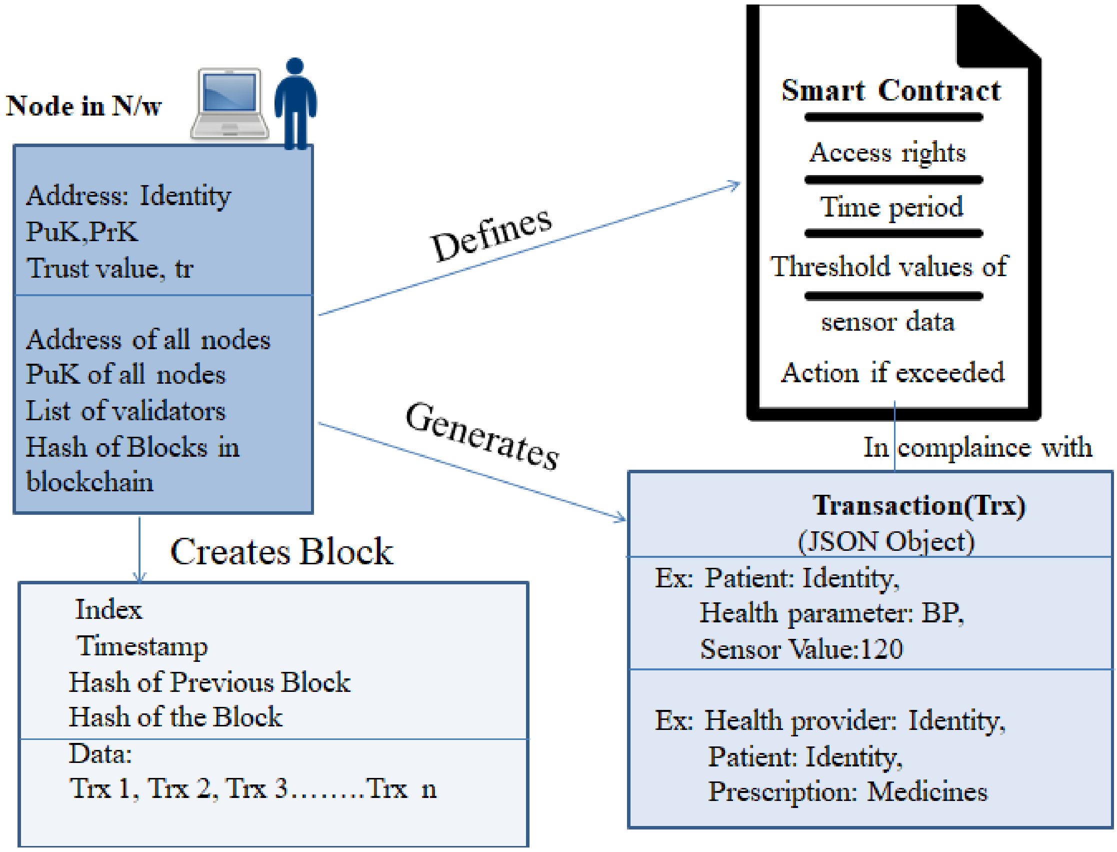


Figure 5. Design of the proposed model

4.3. Workflow of the Proposed Model

Figure 6 and 7 shows the workflow of the proposed model. It is described below in detail:

- The patient is equipped with wearable sensor devices such as a blood pressure monitor, insulin pump, temperature monitor or other known devices.
- Patients, Health providers, insurers or researchers can use the healthcare application to register to the consortium blockchain network. They can only make an account once they provide identity verification documents.

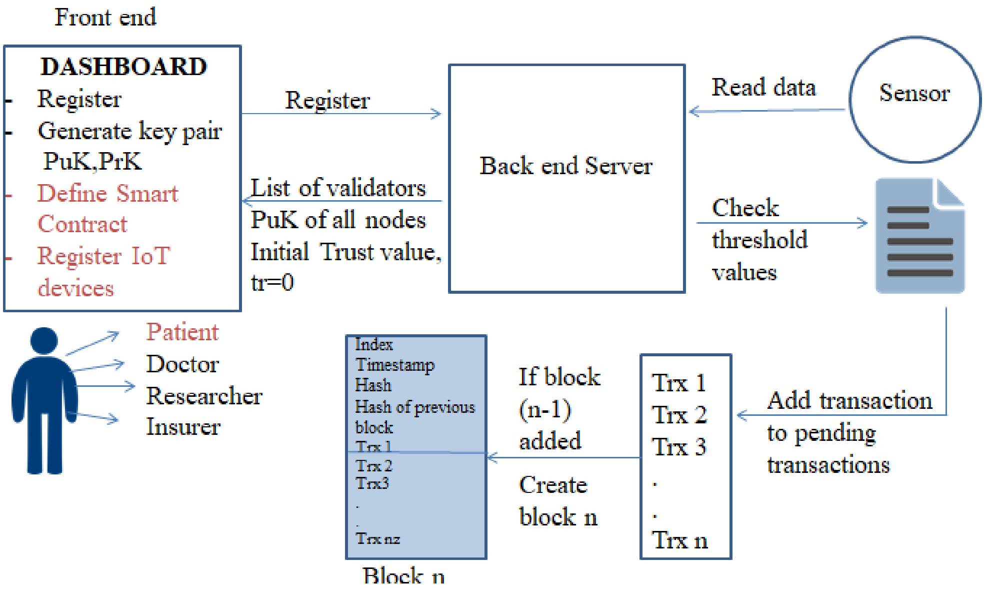
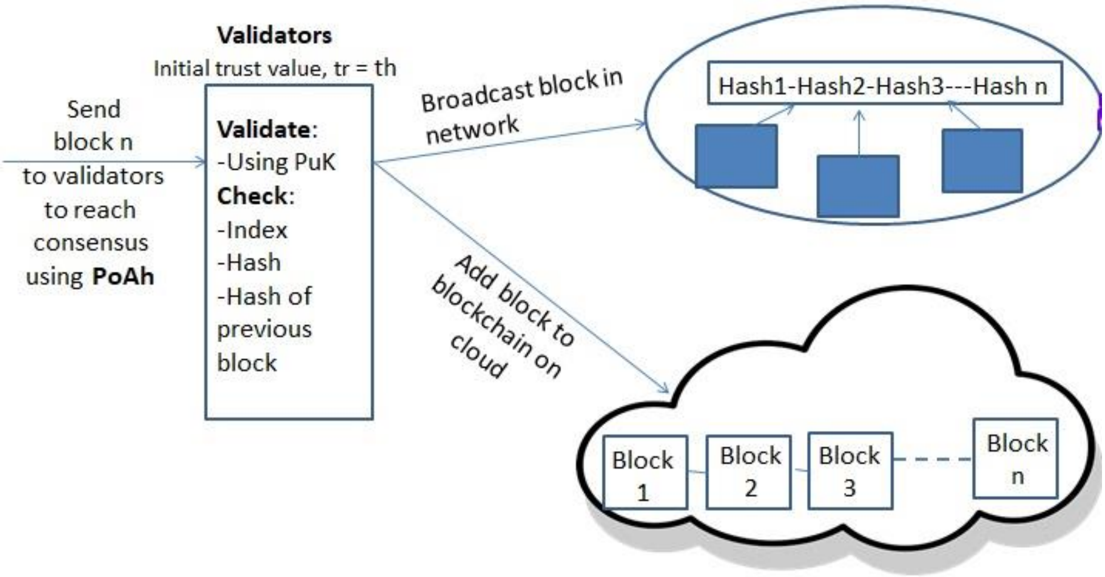


Figure 6. Workflow of block creation by a node


Validators
Initial trust value, tr = th
Send block n to validators to reach consensus using PoAh
Validate:
-Using PuK
Check:
-Index
-Hash
-Hash of previous block
Broadcast block in network
Hash1-Hash2-Hash3---Hash n
Add block to blockchain on cloud
Block 1
Block 2
Block 3
Block n

- **Successful validation**: tr =tr+1
- **Fake validation**: tr = tr-1
- If tr < th, Validator = Normal node
- New Validator appointed

Figure 7. Workflow (continued) of addition of block to blockchain after PoAh consensus

- Each participant creates his own private key i.e. a 256- bit number. The key is kept as a secret and a public key is generated as the hash of the private key using SHA-256 algorithm. Finally, the hash of the public key provides the address of the participant node to which all the transactions are addressed.
- Each participant has his own personal dashboard.

- The patients first define their smart contract, stating the access rights to their data and the events to be triggered in case of any violation or exceptions. The insurer and researchers can access the data according to the smart contract
- Some nodes are selected as authorized nodes and are provided an authentication id and minimum trust value. Only these validators are allowed to validate the blocks. Trust value of all other nodes is zero. All nodes in the network have information of the address of the validators.
- The health information is sent from sensors to the smart devices such as a smartphone/tablet/personal computer
- Information received is sent to the corresponding smart contract for full analysis along with the threshold values as required.
- The threshold value in the smart contract decides whether the health reading is normal as per standard readings or not.
- If the health reading is abnormal, then the smart contract would execute specified action and send an alert to the health providers in intermediate layer.
- The patient or Health provider may initiate a transaction to get treatment, pay fees or send prescription. Each transaction is signed with the private key so that it can be verified at the other end using the corresponding public key.
- All such transactions are broadcasted to all the nodes. One of the authorized nodes, creates a block with all the pending transactions and sends it to other authorized nodes with its authorization id. The block is validated by all other authorized nodes.
- Once validated the block is sent to the cloud server for storage, where it is added to the blockchain.
- The hash of the recently added block is sent back by the cloud to all nodes in the intermediate layer. Each node at this layer keeps a chronological list of hashes of all the blocks stored in blockchain on the cloud server.

5. IMPLEMENTATION OF BLOCKCHAIN

The consensus protocol is the backbone of any blockchain. To prove that PoAh is a faster and more efficient consensus protocol than the most commonly used Proof-of-Work, for the proposed architecture, two healthcare blockchain models were implemented. One used PoW as the consensus algorithm and the other PoAh. Both the models were run on the same machine, with Windows 10 operating system and 8 GB RAM, one at a time. Transactions for both were simulated using the Postman simulator. The post calls were made through Postman to simulate the registration of block and creation and broadcasting of transaction. Node js and Visual Code editor was used to write the code and to run different nodes at different ports. Node js provides many features and is very popular for javascript programs with its rich built-in libraries. HTML, CSS, Javascript, Jquery and Angular js were used to design the front end where user can register and view the data of the blockchain.

First, 15 nodes were simulated for both the models. 50 transactions were simulated to be added to the block to be created. The time taken for execution of the consensus protocol and addition of a newly created block to the blockchain was noted for the blockchains. Then, 25 nodes were simulated for both the models. 50 transactions were simulated to be added to the new block. The time was recorded in this too case. Lastly, 50 nodes were simulated and time was again noted for the block addition to the blockchain after the consensus. On an attempt to create note for further testing, a warning was shown on the system depicting overuse of resources as all the nodes were running on the same machine and PoW protocol uses a lot of computational power and memory to solve the mathematical puzzle. More computers were not available and labs were not accessible due to the covid 19 pandemic lockdown. Thus, observations were made and results were recorded to make a comparison between the PoW and PoAh based blockchains.

6. RESULT

The two blockchain models, based on PoW and PoAh were successfully executed. Different number of nodes were simulated each time with fifty transactions. the time taken for execution of the consensus protocol in both the cases with different number of nodes was recorded. The results are produced in the table1 given below.

Table 1 Time taken to execute PoW and PoAh protocols

Number of Nodes	**No. of Transactions**	**Time Taken in sec (PoW)**	**Time Taken in sec (PoAh)**
15	50	29.252	0.656
25	50	67.313	1.503
50	50	888.777	2.583

7. DISCUSSION

The results clearly show that PoAh consensus protocol is faster than PoW with respect to validation and addition of a newly created block to the blockchain. With less number of nodes, it is approximately 45 times faster than PoW protocol. With the increase in the number of nodes, PoW takes more time which is approximately 14 min to mine a block whereas PoAh takes few seconds to do so. Thus, while the latency of PoW increases with the expansion of the network, PoAh remains low latent and is approximately 300 times faster. This proves that PoAh is highly scalable and can update the blockchain with the new blocks at a faster rate. Hence, PoAh would be an apt protocol to be used in a healthcare blockchain that requires low latency in addition of a newly created block to the existing blockchain.

8. CONCLUSION

An efficient model for access control and secure management of EHRs has been proposed and described in detail in this paper. The use of PoAh protocol for consensus has been justified by implementation and the observed results. Using the blockchain technology with IoT networks along with proof of authentication protocol, decentralized cloud and smart contract, would allow tamper proof medical data storage, quick reporting, data sharing and lowering the cost of medical services. Such a healthcare system is the need of the hour, especially in this pandemic of covid-19.

REFERENCES

[1] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun," A Review on Consensus Algorithm of Blockchain", 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC) Banff Center, Banff, Canada, October 5-8, 2017

[2] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Das, G. (2018). Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems. IEEE Consumer Electronics Magazine, 7(4), 6–14. doi:10.1109/mce.2018.2816299

[3] Li Da Xu, Senior Member, IEEE, Wu He, and Shancang," Internet of Things in Industries: A Survey", IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 10, NO. 4, NOVEMBER 2014

[4] Tushar Dey , Shweta Sunderkrishnan , Shaurya Jaiswal and Prof. Neha Katre ,"HealthSense: A Medical Use Case of Internet of Things and Blockchain" in Proceedings of the International Conference on Intelligent Sustainable Systems (ICISS 2017) IEEE Xplore Compliant - Part Number:CFP17M19-ART, ISBN:978-1-5386-1959-9

[5] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 618–623.

[6] Matthias Mettler," Blockchain Technology in Healthcare The Revolution Starts Here", 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)

[7] Wan, S., Li, M., Liu, G., & Wang, C. (2019), "Recent advances in consensus protocols for blockchain: a survey. Wireless Networks". doi:10.1007/s11276-019-02195-0

[8] Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar and Rajani Singh ,"A Decentralized Privacy-Preserving Healthcare Blockchain for IoT", MDPI Article, 15 January 2019

[9] Deepak Puthal, Saraju P. Mohanty, Priyadarsi Nanda, Elias Kougianos, and Gautam Das," Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems", 2019 IEEE International Conference on Consumer Electronics(ICCE), doi:10.1109/icce.2019.8662009

[10] Deepak Puthal, Saraju P. Mohanty, Venkata P. Yanambaka, Elias Kougianos "PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for Large-scale IoT Frameworks"

[11] Riazul Islam, S. M., Daehan Kwak, Humaun Kabir, M., Hossain, M., & Kyung-Sup Kwak. (2015). "The Internet of Things for Health Care: A Comprehensive Survey", IEEE Access, 3, 678–708.

[12] Stephanie Baker, Wei Xiang, Senior Member, IEEE, and Ian Atkinson," Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities", IEEE Access, 5, 26521–26544. doi:10.1109/access.2017.2775180

[13] Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wireless Communications", 24(3), 10–16.

[14] Kumar, N. M., & Mallick, P. K. (2018), "Blockchain technology for security issues and challenges in IoT.", Procedia Computer Science, 132, 1815–1823. doi:10.1016/j.procs.2018.05.140

[15] Alhadhrami, Z., Alghfeli, S., Alghfeli, M., Abedlla, J. A., & Shuaib, K. (2017). "Introducing blockchains for healthcare." 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA). doi:10.1109/icecta.2017.8252043

[16] Shahaab, A., Lidgey, B., Hewage, C., & Khan, I. (2019). "Applicability and Appropriateness of Distributed Ledgers Consensus Protocols in Public and Private Sectors: A Systematic Review". IEEE Access, 7, 43622–43636. doi:10.1109/access.2019.2904181

[17] Maitra, S., Yanambaka, V. P., Abdelgawad, A., Puthal, D., & Yelamarthi, K. (2020), "Proof-of-Authentication Consensus Algorithm: Blockchain-based IoT Implementation", 2020 IEEE 6th World Forum on Internet of Things (WF-IoT). doi:10.1109/wf-iot48130.2020.9221187

[18] "80% of Organizations Suffered a Cloud Data Breach in the Past 18 Months" article by CISOMAG, June 4,2020

AUTHORS

Maria Arif Pursuing Masters of Engineering in Information Technology from Shri G.S. Institute of Technology and Science, Indore (M.P.), she has an experience as a software developer in Impetus Infotech. Her fields of interest include IoT networks, Blockchain and full stack web development.

Megha Kuliha Working as Senior Assistant Professor in Information Technology Department of Shri G.S. Institute of Technology & Science, Indore, he has 14 Years of experience in academics. She is currently pursuing her PhD from RGPV Bhopal. Her research areas are Blockchain, Network Security & Cloud Computing.

Sunita Varma Born in 1969 at Indore in Madhya Pradesh, Dr. Sunita obtained B.E. (Electronics & Telecommunication, 1991) and M.E. (Computer Engineering, 1998) from Shri. G.S. Institute of Technology and Science, Indore. She had been awarded Doctoral degree from Devi Ahilya University, Indore in 2013.At present she is working as Professor and head in the Department of Information Technology at Shri. G.S. Institute of Technology and science, Indore. Her fields of interest are Mobile Computing and Communication, Cloud Computing, Big Data etc. She is professional member of several international bodies like IEEE and life member of Institute of Engineers.