International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

ODBFT: An Optimal Derivative based Byzantine Fault Tolerance of Blockchain Consensus Algorithm with Smart Digital Contract for Health Monitoring System

V. Sarala Devi[1], Dr. S. Radha Rammohan[2], Dr. Sheela K.[3] , Dr. V. Vaidehi[4] , Dr. N. Jayashri[5]

Submitted: 25/12/2023 **Revised**: 27/02/2024 **Accepted**: 05/02/2024

Abstract: Blockchain technology starts with crypto currency called Bitcoin. Followed by Smart contract is called digital contract, which is defined as pieces of decentralized code. It performs self-sufficient operation are executed automatically to meet certain conditions. Compared with Bitcoin application, Blockchain technology is more powerful. Overall opportunity of Blockchain technology is increasing and applicable in industry, financial transaction and healthcare system. Consensus is a digital agreement or procedure to make a common decision or agreement in a decentralized network. Different methods of consensus are used in Blockchain environment and Bitcoin network. In decentralized environment, multiple nodes can take own decision whereas some nodes act as a malicious node or faulty node. Blockchain and the Internet of Things (IoT) are fast-growing technologies this can be easily integrated and applied in various services, especially for Health Monitoring System (HMS) applications. In smart HMS, IoT devices have the functionality to store, process, and analyze sensed data collected from end user data. Storage of data is also challenging because it must consider legitimate elements, a single point of failure, data manipulation, tampering, and security. To mitigate such problems, integrate Blockchain technology and store of patient sensed data for decentralized computation. In this research, concentrate on consensus mechanism and cognitive smart digital contract in Blockchain network. Propose a decentralized Cognitive Blockchain-based HMS (CBC-HMS). Cognitive blockchain framework is combination of Cognitive Consensus Algorithm with Design a Optimal Derivative based Byzantine Fault Tolerance (ODBFT) consensus technique for a blockchain with IoT technology.Through this research work, two Byzantine Fault Tolerance (BFT) consensus algorithms are proposed for improving the consensus process, reduces fault and improve the lifetime of the network with energy efficiency. Detailed review of PBFT, Paxos, RAFT, PoA, PoAh consensus algorithms is discussed. Also to improve the decision making skill for blockchain introduced cognitive smart digital contract which creates high potential action aggrement. Proposed ODBFT algorithm compared the faulty rate, security, scalability and throughput of consensus mechanism with existing models. Finally, the advantages and disadvantages of the consensus algorithms are compared.The results show that proposed ODBFT solves the problem of Byzantine faults and guarantees stable performance.

Keywords: *Block chain, Health Monitoring System, Consensus Algorithm, Transactions, Byzantine Fault Tolerance, Cloud Storage.*

1. Introduction

An intelligent self-organizing network called the self-organizing node is a component of the wireless sensor clustering network that gathers data from the environmental monitoring region. Longer network lifespans and balanced network usage are crucial design considerations for wireless sensor clustering networks. It should be noted that sensor nodes are only powered by vital batteries. [1]. Wireless Sensor Networks (WSN) come in three varieties: multi-hop communication, many-to-one traffic patterns, and centralized data collection. Packet loss, packet collisions, and network congestion can result from these traits. high energy requirement, which results in the network and its nodes dying too soon [2]. In this WSN, by using a multi-hop path, each sensor node serves as a router to transmit or relay data to the sink node. However, each sensor node is powered by a battery and lacks the ability to be recharged. [3]. Here, the communication procedure uses less energy from the sensor node. The lack of energy in the sensor node causes it to malfunction or die. Thus, the data packet forwarding process is lost, which shortens the network's lifespan.[4]. The Internet of Things (IoT) is made up of many types of sensor nodes that generate, process, store, and exchange vast amounts of sensitive and security-related data. Thus, privacy-sensitive data is communicated between nodes, between nodes and humans, and between sensor nodes and Cluster Heads (CH), making them vulnerable to many types of

[1] *Research Scholar, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Chennai, Mail id - saraladevi.mca@drmgrdu.ac.in*

[2] *Professor, Department of Computer Applications, Dr.M.G.R Educational and Research Institute, Chennai.*
Mail id- radharammohan.mca@drmgrdu.ac.in

[3] *Assistant Professor, Department of Computer Science, St. Anne's Arts and Science College, Madhavaram, Chennai. Mail id- drksheela.research@gmail.com*

[4] *Assistant Professor, Department of Computer Applications, Dr.M.G.R Educational and Research Institute, Chennai. Mail id- vaidehi.mca@drmgrdu.ac.in*

[5] *Associate Professor, Department of Computer Applications, Dr.M.G.R Educational and Research Institute,Chennai. Mail id - jayashrichandrasekar@yahoo.co.in*

communication attacks. [4]. Numerous recently developed wearable and networkable devices, or Internet of Things (IoT) sensor nodes, are low-power and lightweight. IoT technology has a significant impact on network communication in WSN. Internet of Things technology is communicated via centralized systems. IoT devices also raise the possibility of communication with different privacy and security risks. This is counter to security and privacy norms in communication. An essential aspect of human life and networks is communication. The need for dependable, uninterrupted, and secure connectivity cannot be fully met by these IoT devices.

In order to address the crucial problems with secure communication and information exchange in WSN and IoT, blockchain technology has been introduced. In WSN peer-to-peer networks and the Internet of Things, it offers security. Blockchain technology facilitates decentralized, distributed, transparent, and secure communication. Because any node may access the history of data in the public Blockchain, IoT and the Blockchain can be utilized in the context of WSN to govern the truth of information for nodes. The goal of the system is to assess the WSN and IoT node and information truth worthiness. Subsequently, a blockchain is focused on information sharing between nodes or Internet of Things devices. uses a public Blockchain to store the trustworthiness of nodes and information in a distributed ledger suitable for safe communication after that. also presents various Blockchain consensus mechanisms that enhance a Blockchain's scalability and security.A lot of scholars have focused on Blockchain consensus algorithms in the past few years. The consensus algorithm provides the answer to problems in making decisions in a distributed context. [5]. Why does a distributed ecosystem require consensus? There is no requirement for an agreement (decision) if there is only one node in the network. However, in a distributed setting with more nodes, there are multiple decision-makers, hence consensus is required. [6]. Consensus techniques have been a major issue in distributed systems. Consensus algorithm design and deployment are crucial tasks because they require careful consideration of a number of important factors, including network segmentation, node failure, incorrect or out-of-order input, and network latency. [7]. Additionally, in Blockchain networks, the consensus mechanism is employed to prevent forks. Two miners in the same transaction block define the forking problem in the Blockchain network concurrently. [8]. The key issues with consensus algorithms are fault tolerance, availability, and consistency. However, in an asynchronous setting, the consensus mechanism as a whole is unable to meet all three requirements. These algorithms often offer safety and liveliness over fault tolerance in distributed systems. Crash fault and Byzantine fault are two common fault-tolerant issues in distributed settings. [9]. When a node malfunctions as a result of hardware or software issues, a crash fault occurs. It could happen at any time and without prior notice. The failed nodes continue to be unresponsive after that, and the network is unable to take any more action. Byzantine Fault Tolerance (BFT) assesses a distributed system's dependability in the event that any node fails and produces faulty data as the result. The Blockchain network tackles many important problems, including byzantine fault tolerance. When two sensor nodes are reporting comparable information, BFT allows the sensor nodes to communicate safety throughout the system. A node experiencing a Byzantine failure may malfunction occasionally, but it may also exhibit distinct symptoms each time. [10]. In this scenario, in order to avoid the system failure altogether, active nodes must agree on a sign. BFT is also called as error avalanche congruency.

IoT and Blockchain are fast-emerging technologies that can be easily integrated and applied in various services, especially for HMS applications. With smart health monitoring systems, IoT devices have the functionality to store, process, and analyze sensed data collected from patients, and the data are transferred to centralized storage for further computation. Storage can be challenging because it must consider trust elements, a single point of failure, data manipulation, tampering, and security. To mitigate such problems, integrate Blockchain technology and store patients‟ sensed data for decentralized computation. Propose an HMS with a combination of Blockchain and IoT technologies. It can provide secure operations for adecentralized Cognitive Blockchain-based HMS (CBC-HMS). Then design a optimal derivative Byzantine fault tolerance (ODBFT) consensus algorithm for a Blockchain-based IoT HMS. Also summarize a Blockchain network platform. Our results show that ODBFT solves the problem of Byzantine faults and guarantees stable performance.

Challenges Of Pbft Algorithm

Without BFT, a node might propagate fake information throughout the network, rendering Blockchain data unreliable. Make sure that every node prevents the Practical Byzantine Fault Tolerance (PBFT) when implementing the BFT. Every Blockchain network node takes part in the PBFT voting process to add a new block to the system. Here, the blockchain network's two nodes work together to improve a new block. The PBFT approach is more cost-effective and works well with blockchain technology. Fault tolerance would be used to protect against malevolent nodes. Here, consensus is essential because every node generates a verified block, which is subsequently approved by all of the nodes in the blockchain. Permission-less blockchain consensus algorithms are known as Proof-of-Work, Proof-of-Stack, and Proof-of-Burn algorithms. More communication within the Blockchain network is required for these algorithms. Permission-based blockchain consensus algorithms include RAFT, Paxos, Byzantine Fault Tolerance, and Practical Byzantine Fault Tolerance..The Major Contribution of the proposed work is

- Three parameters are used in an adaptive consensus algorithm to choose a Master Node (Chain Head).
- Among the client nodes, identify the Legitimate Node (Cognitive Node) based on their legitimate transaction. Next, permit voting through the Legitimate Node and eliminate the concept of perspective.
- Based on their erroneous transaction, identify the malicious or defective node among the client nodes. Once the defective nodes are identified, their reputation value drops and they are eliminated from the voting process.
- The Master Node (CH) rotates with an equal chance when the threshold measure is determined at a given time interval..

2. Literature Review

[11] described a message-passing system that has general behavior as maliciously. For example, Think of General A, General B, General C, and General D as the Four Generals. Via the phone call, all of the generals are speaking with one another. As an attack, General B sent his own message. The troops are prepared to launch an assault. At this point, General C calls A and B and delivers his personal judgment as an attack. Subsequently, General A notifies General B of the attack while General D receives the retreat communication. In this instance, General A behaves malevolently. General D is now perplexed when he decides. Reaching a consensus in a decentralized or distributed message passing system is exceedingly challenging. Malicious nodes are those that behave in a malicious manner. The term "byzantine fault" refers to the failure and the malicious node that is causing it. It is simple to get to an agreement if there are no systemic failures.

Castro & Liskov (1999) proposed PBFT consensus algorithm. The protocol used to support the synchronous environment is called Byzantine Fault-Tolerance. However, we use an asynchronous environment in our real-time system. The system has low overhead and can withstand byzantine failure. The authors refer to a system as an asynchronous technique for this reason. One can use the PBFT algorithm in a permission-based blockchain network. The techniques require 3f+1 replica(), and the model has 3f+1 replica in an asynchronous environment. [12] created Federated Byzantine Agreement (FBA) algorithm, which has quorum slice-achieved resilience. Decisions made by each node are based on the quorum of the system. The Steller consensus algorithm has also been suggested by the author. Every network node in FBA is aware of the state of every other node. Thus, it waits for another node consent before completing the node transaction. Subsequently, the FBA guarantees the Blockchain transaction's integrity. The BFT algorithm demands higher performance, complexity, and resource costs. Because there are too many attackers present, BFT is unable to control the malfunctioning node and does not support the message delivery scheduling method. [13] has suggested XFT, or Cross Fault Tolerance. This strategy aims to improve security and dependability. In an asynchronous setting, safety is provided by the XFT SMR algorithm. It can also be used in an asynchronous network with byzantine fault tolerance. strategy for delivery schedule since there are too many attackers.

[14] presented the Honey Badger BFT, a unique atomic broadcast technique that adds life. It offers maximum efficiency as well. It is the first atomic broadcasting algorithm that contributes to the asymptotic efficiency being as high as possible. There are designated nodes in this method, and every node consents to every other node's transaction. The bottom bound for broadcast protocol is $3f+1 \leq N$. Three steps make up this Honey Badger algorithm: trusted setup, static byzantine defect, and totally asynchronous network. This strategy is employed to increase the network's scalability. The primary node is frequently the target of attacks, although the author has explained how to identify problematic nodes using the PBFT method. It can be challenging to remove bad nodes in a timely manner.

[15] The Blockchain consensus process makes use of a novel collective decision mechanism. This method is used to identify the problematic node and, even in the presence of the problematic node, it makes recommendations for correction. This technique can detect fraudulent data and creates a peer-to-peer network of PMUs. [16] proposed PMU is used to provide the consensus of nodes. Master node selection is one of the major issues where communication overhead must be increased, as the PBFT algorithm explains. The main node selection procedure is eliminated in the Egalitarian PBFT algorithm that is suggested. As a result, the nodes build a block, and through broadcast requests, more nodes are built, broadcast to the network, and the system's present status is broadcast. Every node in the network is handled equally and efficiently using the same techniques. Here, there is an increase in consensus efficiency and a halving of communication complexity due to fewer viewpoint changes. When comparing this

technique to PBFT, throughput rises while communication costs and delay decrease.

In a large Blockchain network, the PBFT algorithm is unable to meet the scalability requirements. [17] suggested an Eigen Trust model-based Practical Byzantine Fault Tolerance consensus clustering technique. The ODBFT algorithm has multiple stages. Nodes in PBFT are separated into two categories: transaction nodes and non-transaction nodes. Calculating the global trust value and the cognitive node value between nodes would then be possible. The consensus group can be built by nodes with the greatest trust scores. This approach replaces the single valid node with a collection of core nodes, reducing the need for the view change method. The communication overhead is decreased by using the suggested approach. Because PBFT algorithms are unable to successfully excite positive nodes, a significant amount of communication resources are required.

Table 1: Communication complexity of permission Blockchain consensus algorithms

Byzantinefault	PBFT	Honey Badger BFT	XFT	FBFT	RBFT	ODBFT
Legitimate NetworkNode	One	One	One	One	One	Many
Computational Communication	Avg	*O (N²+ N³Log N)*	O(N)	Avg	Avg	Avg
Viewchangeprobability	High	High	Nil	High	Nil	Low

[18] provides Credit Delegated Byzantine Fault Tolerance (CDBFT), a system that operates using two methods. The first is the credit evaluation scheme's voting rewards and punishments. The purpose of the scheme is to enhance dependable node simulation and decrease the number of defective nodes in the shared decision process. The second one increases the system's flexibility and efficiency and is based on consistency and checkpoint protocol. By lowering the number of malfunctioning nodes to 5%, the CDBFT algorithm increases the network's stability and efficacy. [19] proposed Delegated Adaptive BFT algorithm is an empowered approach, whereby a more adaptable DABFT can choose BFT flavors appropriate for concurrent activities. DABFT is extended by an adaptive-ness idea. A task validator creates the new block based on the validator. The suggested approach lowers system complexity and increases efficiency. A decentralized and scalable trust infrastructure is provided by SBFT. BFT operates in a cluster of hundreds of replicas, particularly when deployed globally. [20] suggested SBFT work in a global geo-replicated deployment using a 209 model with a f=64 byzantine fault. SBFT improves the network's scalability and performance. With 1.5 × latency and 2 x higher throughputs than PBFT, SBFT is a highly efficient network. This four-step SBFT technique lowers client communication, employs an optimistic fast path, uses redundant servers for speed, and collects data.presents the Delegated BFT method as well. The DBFT algorithm is used to increase the scalability and efficiency of networks. Node selection in this suggested method is left to other nodes.The idea of distributed structure serves as the foundation for this method. It is employed to lessen the complexity of central storage and the problems associated with single node attacks. In order to increase consensus efficiency and decrease PBFT consensus overhead, SG-PBFT includes a score grouping technique. The geographic PBFT algorithm is used to get around the low scalability and high computing cost of the Sybil node attack. For IoT-Blockchain applications, a novel scalable consensus protocol and location-based algorithm are created. After then, the stationary node shortens consensus times and requires more processing power than mobile work overhead.

The Dynamic Reputation PBFT algorithm functions similarly to a credit-based method for selecting consortium nodes. As a monitoring node, Chain Head is chosen to separate the remaining participating nodes into consensus and secondary nodes according to each node's standing value. These nodes take part in the process of creating blocks [12]. The transaction speed is accelerated using this protocol. It is appropriate for the blockchain energy sector as well.Voting results from internal nodes can be efficiently gathered

MBFT: The algorithm for Mixed Byzantine Fault Tolerance utilizes sharing and layered technologies. In order to increase fault tolerance and security, the MBFT algorithm incorporates a credit system and a random node election technique. The nodes are separated into three categories: verification, backup, and client. Every node transaction is validated, and the transaction list is stored on the verifying node. The Blockchain network is then informed of the malicious node details by the verification node [21].

High throughput, scalability, and strong security are offered by MBFT. It primarily focuses on enhancing the Blockchain's fault tolerance while also increasing throughput and scalability.

Berdik et al. (2022) surveyed the potential of blockchain in maintaining security in applications used nowadays.

The survey throws light on blockchain as a service used for applications in recent ages. It outlines different uses of blockchain studies in securing applications. The findings throw light on using blockchain technology in full potential for global markets. Proposed a blockchain model for code copyright protection in order to avoid plagiarism. This is achieved through developing a blockchain based verification model while the nodes in the blockchain are responsible for storing and validating through the verification model. This model claims to guarantee code protection with efficiency in storage, which uses irreversible sha 256 algorithm, and betterment in speed.

Kouhizadeh et al. (2023) carried out exploration study for the barriers in acceptance and adaptation of blockchain technology in the field of supply chain management. The extensive study has been carried out from various experts from relevant industries including academics, which is further analyzed with specialized tools. The results outline critical technology and supply chain barriers including comparisons from academics and industrial experts. Proposed a blockchain framework model in the smart vehicle industry, which is resilient to malicious attacks. The proposed framework throws light in secured communication using blockchain technology with authentic smart data exchange between vehicles. The model intends to provide a new approach of security in the smart vehicle industry using the underlying blockchain technology such as trust and security.Ahmad et al. (2021) using blockchain technology in port logistics for data security. The transparency and security of data is a perennial challenge in this category. The traceability is scarce and integrity is at stake. The paper intends to solve challenges in introducing permissioned blockchain to improvise the operation, services and deployments. The paper outlines the issues hindering the adaptation.The security solutions provided are expert advice involving various security professionals from the relevant fields. The solutions drawn are the result of extensive blockchain research and includes suggestions, technical artifacts and best practices to follow while designing applications.

Xu et al. (2022) provides a performance analytical model of permissioned blockchain. The model tends to quantify and measure the performance of fabric blockchain in a more accurate manner with its effectiveness. The insights provided are beneficial for developers with various accurate measuring parameters like size and interval of the block.The focus of the infographic is to look at the technology's development and how it gained acceptance in many industries via step-by-step means. The ledger, smart contracts, and the excellent data security and protection capabilities of the network were described.

Bisogni et al. (2023) prepared an encryption methodology to sign smart contracts in blockchain technology. The encryption encoding uses face as the key encoding which is combined with the RSA key using a hybrid information algorithm. The result proves authenticity of the execution without compromising the privacy including a better performance and accuracy while signing.

3. Blockchain Technology Used in Health Monitoring System

In centralized cloud storage everyone edits on their local copy of the patient sensitive data and treatment, medicine.

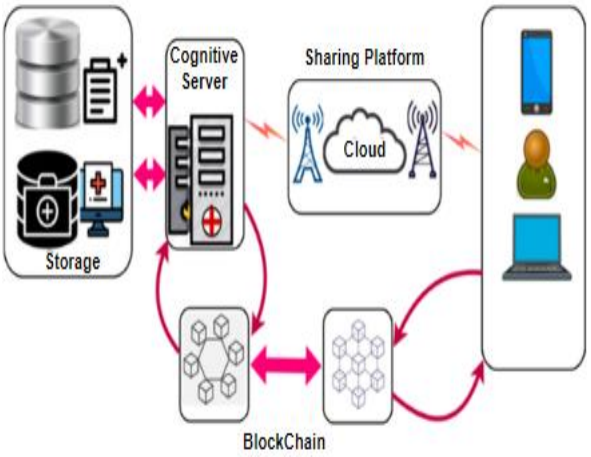


Fig 1: An Advanced Health Monitoring System with Cloud Storage

The Internet of Things (IoT) is an emerging technology and is a core building block in the development of smart homes and smart cities, with the increasing number of devices connected to the internet (Saha et al. 2017). The main IoT components are sensing, heterogeneous access, information accxess, and services. Other important components are security and privacy. With the effective implementation of those components, IoT is now being applied in many of CBC-HMS. Issues arise in devices when adopting IoT technology in an HMS. The main concerns are devices that have low consumption of energy and computation power (Namasudra et al. 2021). This study concerns an HMS that combines IoT and Blockchain to overcome many problems in IoT technology. Blockchain technology solves consensus problems in networks. To achieve this aim, review Blockchain operations and their implementation in medical domains in different areas on various platforms.Propose a ODBFT consensus algorithm that can operate with patient, health provider, transaction, and consensus nodes. The algorithm provides the consensus of Cognitive Blockchain-based IoT HMS. Devise an efficient structure of dataflow, smart contracts, and Blockchain-based HMS blocks. Due to their importance, diverse consensus algorithms are used in the Blockchain network. Blockchain networks include permission networks and permission less networks, and these use different algorithms. So,suggest a consensus algorithm for IoT-based CBC-HMS.Blockchain technique is decentralized database which supports the strong consistency.

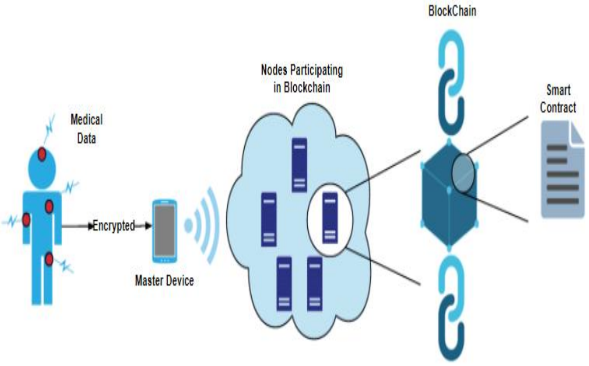
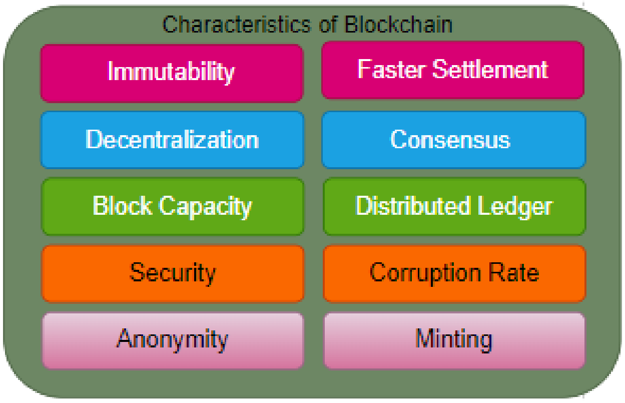


Fig 2: Blockchain for IoT Health Monitoring System

In Blockchain network, public ledger is a database, which maintains the historical information of every patient. The historical information might have been utilized for future treatment. In Health Monitoring System, the old treatment is used to update the new treatment. Public ledger is used to store 500 patient's information.

BLOCKCHAIN FEATURE FOR HMS

The Blockchain has many interesting and attractive characteristics, which is useful for the IoT application to solve major issues of IoT.



Characteristics of Blockchain

Immutability	Faster Settlement
Decentralization	Consensus
Block Capacity	Distributed Ledger
Security	Corruption Rate
Anonymity	Minting

Fig 3: Blockchain features for HMS

Immutability: All the centralized data is modified or corrupted by third parties or hackers, so need the integrity to keep information. In Blockchain once node have recorded the transaction then it cannot be modified or never changed by any other node.

Decentralization: In IoT, all devices in a Blockchain network is a decentralized network, it supports the peer-to-peer communication of transactions. Bitcoin eliminates a single point of failure, traffic flow.

Security: Single point of failure may break down the entire network in IoT applications. In Blockchain technology there is no single point of failure, so it provides better security. The concept of one-way hashing, tamper proof attacker cannot find the input of hash value. Byzantine Fault Tolerance, PBFT protocol algorithms are used to provide security.

Increased Capacity: Blockchain is a decentralized database which contains thousands of computers working together to perform transactions. Compared to centralized servers, Blockchain increases network capacity. The concepts of mining any node let to add to the network and leave the network at any time.

Anonymity: In a Blockchain network, a user's private information is kept secret that means hiding the user identity. Zero Knowledge Protocol is used to support anonymity.

Two types of nodes used for Blockchain based applications. First one is Full node and second one is lightweight node. Blockchain network nodes are responsible for performing creation of blocks, data storing, mining, validation of blocks and distributing data among other nodes.

Full Nodes: In a decentralized network, full nodes act as a server, creates, validate the blocks and store a copy of Blockchain. Full node is divided into 2 types such as pruned node & archival node.

Pruned Nodes: From the beginning, it downloads the blocks and when it reaches the limited, the older block is deleted.

Archival node: It acts as a database which stores full Blockchain. There are four types of archival nodes such as master, mining, staking, and authority.

Master node: Maintains the record of transaction and validates the transaction. It cannot add blocks to the network.

Mining node: This type of node adds block to the network

Staking node: It is used to hold and buy crypto coins.

Authority node: Such types of nodes are used to broadcast data to other nodes.

Lightweight node: It cannot store a copy of the block in the network. It performs the payment operation and verification and the major function of lightweight node is to query the current status of blocks transactions which block broadcasts transaction and last. List of main contributions,

- This research work describes the basic Blockchain network background.

- This research discusses Blockchain consensus algorithm in the HMS field.
- This research compares Blockchain platforms and their potential uses in an CBC-HMS.
- This research discusses uses of cognitive blockchain and IoT-enabled HMS services.
- This research proposes a consensus algorithm for cognitive blockchain-based HMS that calculates global trust values for the consensus process.

4. Cognitive Blockchain Based Health Monitoring System

Blockchain network, the public ledger is a database maintaining the historical information of every patient, and this information may be utilized for future treatment. In HMS, the old treatment is used to update the new treatment. The consensus of the system ensures that the patient's sensitive data are consistent and updated.

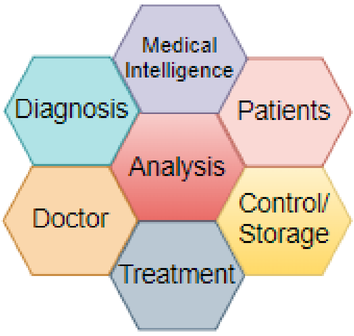


Fig 4: General Blockchain Architecture for CBC-HMS

The patient's data must tamper-proof to avoid malicious acts and compromised information. A patient's sensitive medical information belongs to various clients, and Blockchain can guarantee privacy and authenticity. A hash function makes a timestamp of a patient's medical data. When a patient accesses medical information, it constructs a block with the sequence number of access, patient ID, timestamp, and a hash value. All the data are hashed and communicated to the previous block. The public ledger stores the information of diverse patients, as shown in Figure 4.

A smart contract is a fast, cheap, and secure digital contract. It provides a legal contract with a computerized technique used for digital facilitation and verification. It supports the improvement of legal contracts byeliminating intermediates. It directly validates a contract over the decentralized platform. A smart contract can provide the complete medical data of patients for implementing a health monitoring system. It constructs a block with the sequence number of access, patient ID, timestamp, a hash value from the previous request, and all data. All data are hashed and communicated to the previous block and the shared patient's records.

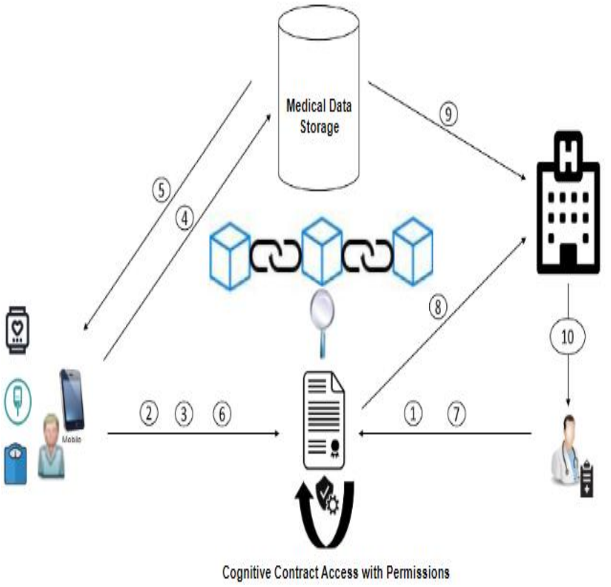
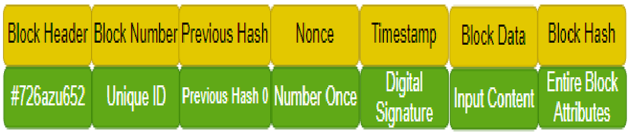


Fig 5: Smart Contracts for CBC-HMS



Block Header	Block Number	Previous Hash	Nonce	Timestamp	Block Data	Block Hash
#726azu652	Unique ID	Previous Hash 0	Number Once	Digital Signature	Input Content	Entire Block Attributes

Fig 6: Block item description

Smart contracts are computed through the system to produce a group of blocks. Every block is constructed for the patient to identify a specific transaction. The patient information is stored in the smart contracts using the patient ID. Whenever patient health records are included in the system, the patient can access his or her information and communicate through the Blockchain network regularly with the healthcare provider. The block item description is illustrated in Figure 6. The block items include the block number, id, height, group, previous block, nonce, timestamp, block data, and block hash.

Cognitive Smart Digital Contract

```
Start Contract
Input: Nodes Group, Client Request Message
User: End user, medical intakes
        Unlock time, $Private_{key}$
Output: Consensus Outcomes
Assign
        Lock time, $Public_{key}$
        Hash Value of Message Request ← SHA256($Req_{msg}$)
        N←Total node length
```

Main()

```
1.  When time is active
2.  Gather signature to private
3.  Accept the contract
4.  Request(Time, block_id, Client$_{Sig}$)
5.  Wrap ([Primary_Node], [Master_Node])
6.  Communication_build (Pre_Prepare, Primary_Node, Current_View, Block_Height,Req$_{msg}$)
7.  Broadcast (Step 6)
8.  Loop: Condition 1: Approve → Pre-Prepare
9.        Condition 2: Send →Check
10.       Iteration Node 1 to N
11. Master_Node_Check (receives same and correct)
12. Master_Node Broadcast (Req$_{msg}$, block height, view, Master_Node)
13. Otherwise reject the contract
14. If user data are matched
15. Approve(Commit)
16. Primary_Node Send(Reply, block_height, current_view, requested hash value, signature_check)
17. Unlock signature Lock time, $Publickey$
18. Client receives the same and correct(reply(f+2))
19. Retrieve the patient's documents in the network
20. Accept the contract
21. Continue the process until the entire patient's documents are retrived
```

Stop Contract

A patient who has a disease may want to take treatment in a multi-specialist hospital but may lack sufficient money for treatment. In that case, a Blockchain smart contract submits a proposal to a crowd funding agency. Multiple agencies commit to support medical treatment with small funds. Two types of the Blockchain nodes are used for Blockchain-based applications. These are the full node and lightweight node. Blockchain network nodes are responsible for the creation of blocks, data storage, mining, validation of blocks, and distribution of data among nodes.

In a decentralized network, full nodes act as servers that create and validate blocks. After that, they store a copy of the Blockchain. Full nodes are divided into two types of nodes, such as a pruned node and an archival node. Pruned nodes have been downloading blocks and have reached the limit, in such case, the older blocks are deleted. An archival node acts as a database that stores the full Blockchain. There are four types of archival nodes. A master node maintains the record of a transaction and validates it. It cannot add blocks to the network. A mining node adds a block to the network. A staking node is used to hold and buy crypto coins. An authority node broadcasts data to other nodes. A lightweight node cannot store a copy of a block in the network. It performs payment operations and verification. Its major function is to query the current status of block transactions.

A blockchain-based IoT (BIoT) healthcare system uses sensors to monitor a patient's health. Figure7 illustrates the architecture of CBC-HMS. Body sensors may include sensors for blood pressure, body movement, temperature, blood sugar, ECG, and heartbeat, which measure a patient's physiological condition. Body sensors measure pulse, body temperature, respiratory rate, and vital signs. These data are essential to determine a patient's critical health. Special-purpose sensors such as fall detection and blood-glucose can be implemented for specific conditions. Other important sensors measureblood oxygen and blood pressure. Central nodes act as a database, receiving and storing data from body sensors. A central node processes this information, analyzes the data, and implements a decision-making Blockchain network.

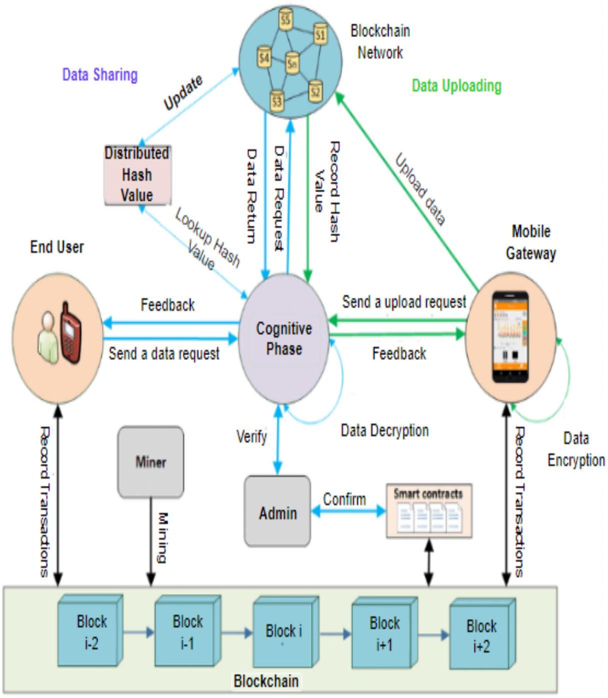


Fig 7: Overall Processing Model of CBC-HMS

Short-range communication is required for sensors to communicate with the central node. For this, consider the standard, security, latency, and effect on the body. It might provide a strong security mechanism for sensitive data. Sensitive data must not be attacked.

Data of central nodes should be forwarded to a database where doctors can securely access it. Long-range communication is implemented and messages are transferred. When a message is sent by the central node, the same message is received by the doctor. It supports high availability, which means message delivery anytime and anywhere. This is important in time-critical applications. Medical information received from a patient through a body sensor must be stored securely for continuous and future use. Doctors benefit from identifying a patient's medical history. The Blockchain provides security for patient data through smart contracts. The Blockchain provides cryptography algorithms and hash functions to securely store data.

5. Optimal Derived Pbft Consensus Algorithm For Cbc-Hms

The ODBFT consensus algorithm is most suitable for Blockchain-based IoT HMS. This algorithm uses four steps to achieve the consensus process of CBC-HMS: calculation of a patient node, trust evaluation, construction of a health provider consensus group, and a consensus process. It has four types of nodes: health provider, patient, transaction, and consensus. In Blockchain-based IoT HMS, the consensus is important for making decisions in the health provider nodes, i.e., the primary and master nodes. ODBFT is a multistage algorithm. The node trust value is calculated between the patient's nodes. It is divided into a cognitive node and faulty node. In addition, the high trust value of the node allows active participation in the consensus process. The health provider (primary) node is replaced by the health provider group.

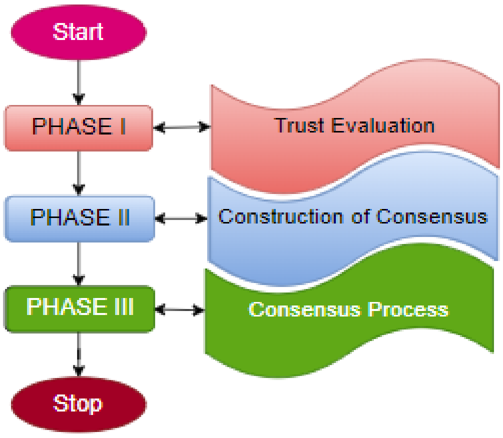


Fig 8: Optimal Derivative Byzantine Fault Tolerence Consensus Algorithm

In peer-to-peer network application, Blockchain provides a decentralized approach. Due to this characteristic, Blockchain-based IoT HMS is attacked by many malicious nodes. It tries to reduce malicious nodes and hasan impact of dishonest nodes in the CBC-HMS of the consensus field. The entire process of the proposed optimal derivative based-BFT algorithm is shown in Figure 8.

PHASE I–NODE TRUST EVALUATION

Trust process generates a key-pair when a user logs into the server with a unique identifier, and the attribute set is forwarded to the authentication system to generate the health provider group. When the generated attributes are valid, a secret key is computed for the Blockchain health provider group.

Thekeyinitializationprocessfor$K$apublickeyuser(PuK_{End_User})iscomputedusingthegeneratedkeys(gen_K)intheblockchainelements($generate_K^{\alpha}$)fortheusers ($End\_User_1, \ldots\ldots, End\_User_n$)inEquation(1),

$$PuK_{End\_User} = (generate_k, End\_User_1, \ldots\ldots, End\_User_n, generate_K^{\alpha})$$

The master key for the End_user (MaK_{End_User}) is computed as

$$MaK_{End\_User} = generate_K^{\alpha}$$

The group of attributes for the End_user (Att_{user}) is identified within the attributes set (Att) as

$$Att_{user} \subseteq Att$$

The secret key for the End_user ($SecK_{End\_user}$) is computed as

$$SecK_{End\_user} = generate_K^{\alpha} \cup generate_k$$

Algorithm 1: Calculate Patient's Node Trust Evaluation

```
Threshold_i= 0;
For (patient's node_j∈ Health Provider Nodes)
{
    $Threshold_i = \sum_{n}^{C_{ji}} Thershold_j$
}
```

Procedure: Health provider nodes may act as primary or master nodes.The patient's information is inserted and stored in the health provider node.Patient nodes participate in the CBC-HMS. Patients send requests to the health provider node.Any new patients added are included in the CBC-HMS.Some patient's nodes may behave like malicious nodes that continuously send invalid votes.Patient nodes are divided into faulty and cognitive nodes. Legitimate or cognitive nodes send valid transactions.This consensus algorithm finds the faulty node and legitimate node.In the consensus process the high voting value may make a decision.Health provider or primary nodes are selected as the rotation basis.The consensus node constructs the consensus group based on their global trust values.

PHASE II–CONSENSUS GROUP CONSTRUCTION

Consensus group construction is used to provide the solution for scalability issues. The nodes having high threshold values are elected as members of the consensus group. Consensus group construction of Blockchain is performed as the find patient node optimal evaluations to determine universal trust rate of the end user nodes in the blockchain network. The consensus nodes provide the accelerated progress of Blockchain consistency. They set the global trust threshold value, and then a node can elect to hypothesis the consensus cluster for blockchain. However, this consensus process have limited time and power.

Algorithm 2: Consensus Group

```
Consensus group=ф;
Arrange patient nodes by threshold;
For (patient's node $_i \in$ health provider nNodes)
{
    if (threshold $_i$into consensus group) then
    {
        Add patient's node$_i$ into consensus group;
        else
        Exclude consensus group;
    }
}
```

PHASE III–CONSENSUS PROCESS

The proposed ODBFT algorithm improves the fault-tolerant rate with the consensus group with which the faulty node is identified. A new patient node is added to the network by a voting process within the consensus group. When a health provider node or primary node fails, the faulty patient node behaves arbitrarily or the network fails. At that time, end user nodes execute peak cognitive rate which get improves enhancement of consensus clusters. Thus, a health provider or primary node is replaced by a health provider group. Algorithm 3 describes the operations.

Algorithm 3: Form Health Provider Group (Primary Group)

```
Let m = message
Consensus group, fixed value m (0<m<=1)
Health provider group =Φ;
for (node$_i \in$ consensus group)
{
    if(node$_i$> with global optimal value in top m)
    then
    {
        add node$_i$ to health provider group;
        else
        exclude node$_i$ from health provider group;
    }
}
```

Encryption process is initiated by a uniquely computed identifier from the user to implement the encryption of the file to be delivered in the cognitive blockchain-based ODBFT model. The threshold value is used to implement the encryption with the captured attributes as the master key and public key. It is transmitted to every user. The server side is responsible for encryption. Everyattribute is assigned a parity-related authority value. The encryption process generates the cipher text as

$$Cipher_{Data} = \{Cipher_{\delta 1}, Cipher_{\delta 2}\}$$

The cipher data for the particular end user ($Cipher_{\delta 1}$) is computed as

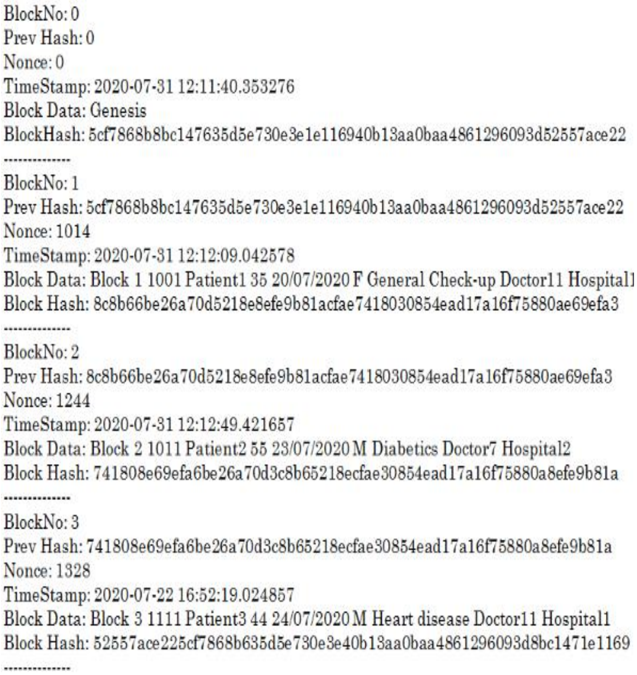
$$Cipher_{\delta 1} = generate^{\alpha\delta}$$

The decrypted message files are received by the server. The cipher text creates global optimal values based on the priority and attribute level. Whenever the receiver decrypts a file with an invalid user, it is assumed that hackers are trying to hack a message. If the user is valid, the decryption technique converts cipher text into regular plaintext. If authorized user has secret key$SecK_{End_user}$, then the decryption process for the cipher text is

$$SecK_{End\_user} = Decrypt(Cipher_{Data})$$

Smart contracts using Blockchain.

The proposed system has a Blockchain-based management process to identify authorized users who can view blocks, and nodes can generate smart contracts to verify the included nodes. The limitation of the users has to identify the service providers to execute the application. To identify authorized users, nodes in the Blockchain with a valid block have signatures from a reduced number of members. False transactions are restricted using an efficient secured framework with a Proof-of-Work concept. The smart contract has a portable format for every patient-related record to be structured using the Blockchain framework, the output of the smart contract is illustrated in Figure 14. The proposed technique has improved encryption time, decryption time, key strength, and throughput. It produces scalability to an advanced blockchain-based HMS. The communication complexity for an advanced blockchain-based HMS is $(M2)$ for the initial formation, and is $(M2 + M3 \log M)$. Then the total numbers of users increase rapidly.



```
BlockNo: 0
Prev Hash: 0
Nonce: 0
TimeStamp: 2020-07-31 12:11:40.353276
Block Data: Genesis
BlockHash: 5cf7868b8bc147635d5e730e3e1e116940b13aa0baa4861296093d52557ace22
--------------
BlockNo: 1
Prev Hash: 5cf7868b8bc147635d5e730e3e1e116940b13aa0baa4861296093d52557ace22
Nonce: 1014
TimeStamp: 2020-07-31 12:12:09.042578
Block Data: Block 1 1001 Patient1 35 20/07/2020 F General Check-up Doctor11 Hospital1
Block Hash: 8c8b66be26a70d5218e8efe9b81acfae7418030854ead17a16f75880ae69efa3
--------------
BlockNo: 2
Prev Hash: 8c8b66be26a70d5218e8efe9b81acfae7418030854ead17a16f75880ae69efa3
Nonce: 1244
TimeStamp: 2020-07-31 12:12:49.421657
Block Data: Block 2 1011 Patient2 55 23/07/2020 M Diabetics Doctor7 Hospital2
Block Hash: 741808e69efa6be26a70d3c8b65218ecfae30854ead17a16f75880a8efe9b81a
--------------
BlockNo: 3
Prev Hash: 741808e69efa6be26a70d3c8b65218ecfae30854ead17a16f75880a8efe9b81a
Nonce: 1328
TimeStamp: 2020-07-22 16:52:19.024857
Block Data: Block 3 1111 Patient3 44 24/07/2020 M Heart disease Doctor11 Hospital1
Block Hash: 52557ace225cf7868b635d5e730e3e40b13aa0baa4861296093d8bc1471e1169
--------------
```

Fig 14: Smart contracts using Blockchain

Table 2: Comparison of Proposed Consensus Algorithm with Existing Models

Features	RAFT	TPBFT	ODBFT
Anti majority attacker Node	3.5	5.5	5
Minimal Comn Complexity	3.75	2.5	4.75
Fault Tolerence Rate	3.5	3.5	5
Transactions per Second (1000 nodes)	5	3	4.5
System Utilization Level	5	4	**4.5**

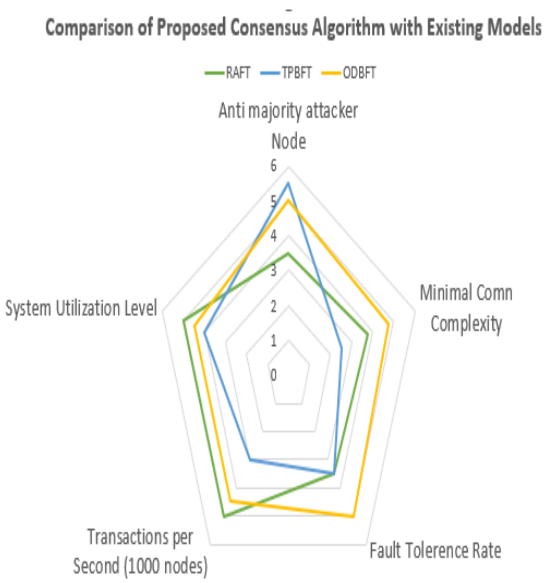


Fig 15: Radar Chart Comparison for Various Consensus Algorithms

6. Performance Evaluations

The ODBFT algorithm reduces encryption time, efficiently generates cipher text, and enhances the performance of the decryption process. The proposed algorithm was compared with the related RAFT (CJC & Ercole 1998), XFT (Liu et al. 2016), CDBFT (Wang et al. 2019) methods was proposed. The experimental setup was initialized by the testing machines, which were controlled by the master machine. Every slave machine continuously forwards requests within the load balancing application. The testing machine has more than 500 users within one minute of time to provide the results. The Blockchain validated nodes were divided into geographic regions. The efficiency of the proposed technique was analyzed by active communication in the Blockchain. The proposed technique was implemented using Python 3.8.4. The coding created blocks through hashing. Chains of blocks were stored on a databaseserver using the block data. Smart contracts were created using the IoT-based healthcare monitoring system. Based on the literature survey and to suit with real time scenario, appropriate algorithms are chosen to work with Blockchain consensus algorithm.

Encryption Time

In Health Monitoring system, an RSA encryption algorithm is used. The size of the key is 512 bits, the file contains the patient's records. The encryption time was measured as the time taken to convert plaintext into cipher text. The experimental results for the encryption time are portrayswith Figure9. ODBFT proposed model used less encryption time than the other techniques.

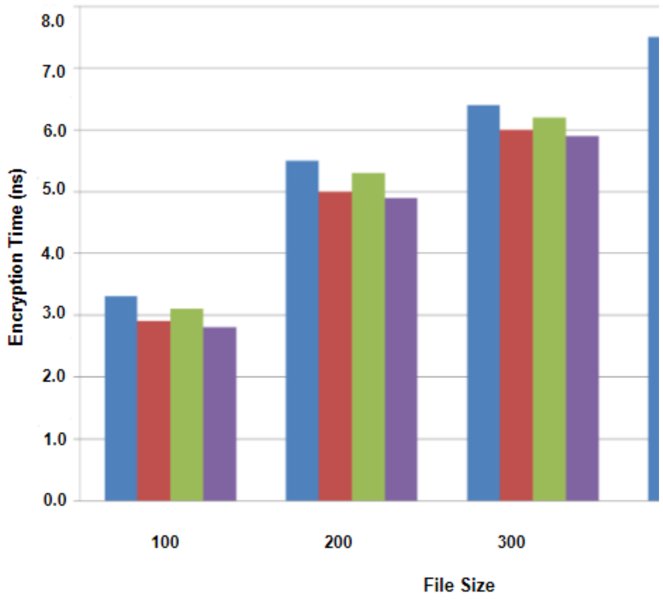


Fig 9: Encryption time

Decryption Time

The decryption time was measured by converting the cipher text to plain text regardless of the file size. Decryption time is increased with file size. Figure10 compares decryption process of proposed CDBFT method with various existing methods.

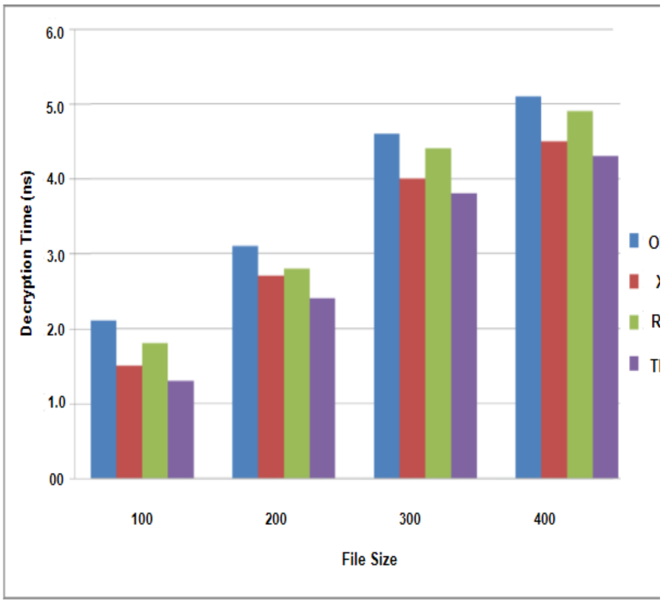


Fig 10: Decryption time

Key strength of proposed technique

The avalanche effect is an important parameter in hash-based cryptographic method computation. A small change in a cipher can cause huge changes in the output. The avalanche effect is reduced as the key strength increases, as described in Figure11.

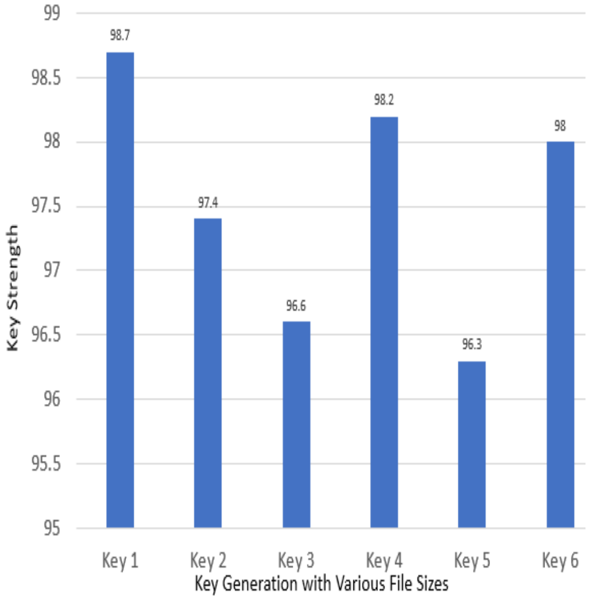


Fig 11: Key strength of proposed technique

Transactions per Seconds

Throughput calculated with overall transactions per second. Figure 12 illustrates the throughput for different numbers of users. Throughput calculated with overall transaction per second (sec). The proposed system minimizes the time and improves efficiency compared with related techniques during transactions between users.

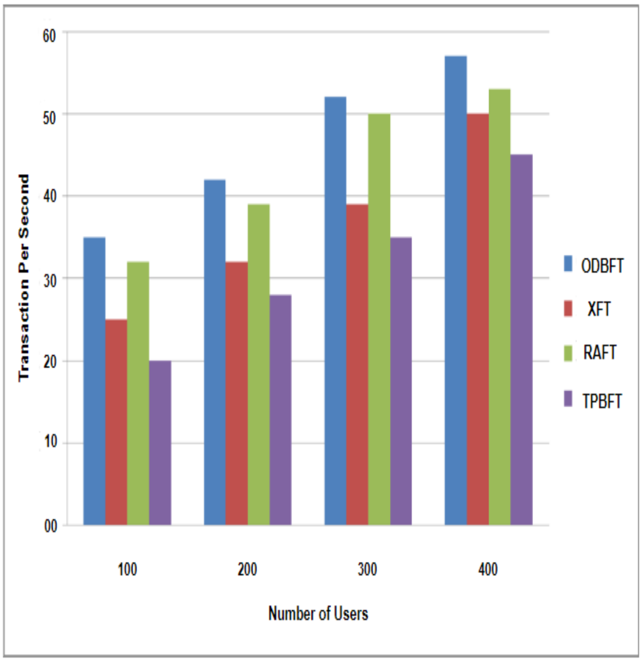


Fig 12: Transactions per seconds

Throughput comparisons of disk and network

Smart contracts are used to store the details about the permission for accessing IoT-based healthcare system. The proposed approach provides privacy and security for health-related records. The huge number of healthcare-related records will affect the response time, and the throughput is used to measure the performance, which is illustrated in Figure13.

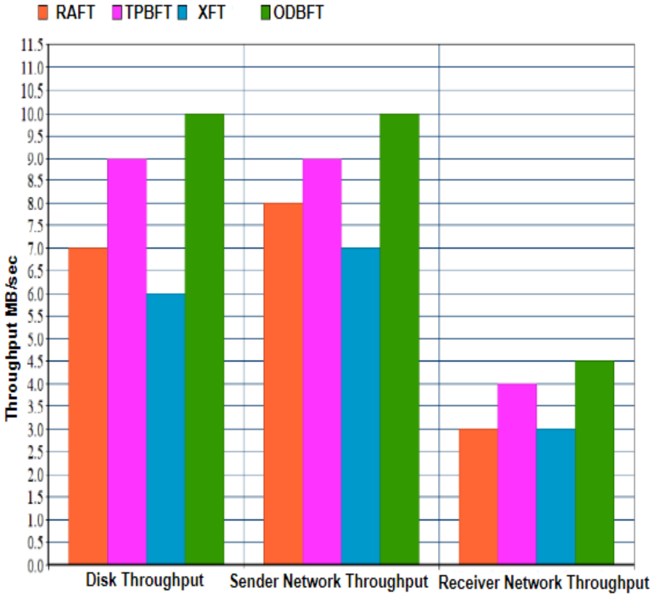


Fig 13: Throughput comparisons of disk and network

ODBFT Communication Complexity Analysis

Overall nodes of this byzantine fault tolerance algorithm is N, process of ODBFT has six difference stages are Request, Pre-Prepare,Prepare, Broadcast, Commit and Reply. Computational complxity can evaluated with $1 + (no.of\ bc\ nodes - 1) + (no.of\ bc\ nodes - 1)(no.of\ bc\ nodes - 1) + no.of\ bc\ nodes(no.of\ bc\ nodes - 1) + no.of\ bc\ nodes$. Attained communication complexity of existing BFT algorithm is,

$$Complex_{comn} = 2N^2 - N + 1$$

ODBFT algorithm also has N number of nodes, k is node's cluster domain, it will divids into (N/k)cluster domains. Communication complexity of ODBFT is $1 + 2(k(k-1)) + (k+1)$, which is simplified form of $2(k+1)^2$. Attained communication complexity of the proposed consensus algorithm is,

$$Complex_{ODBFT} = 2(k+1)^2/k$$

Ratio of complexity of proposed ODFBT consensus algorithm is $C = Complex_{ODBFT}/Complex_{comn}$. From the expression,

$$C = [2(k+1)^2/k]/[2N^2 - N + 1]$$

Evaluating complexiy with k =4, 10 and 16 using number of blockchain network nodes N greater than or equal to 1200. ODBFT consensus algorithm experimental results portrays comparison of existing models and proposed algorithm has significantly minimal. Network size also playing vital role on complexity, minimal k value process obtained low complexity. However, minimal k value that proposed model needs to be divid into more layers. It shows more layers and iterations leads to minimal security and computational time also higher.

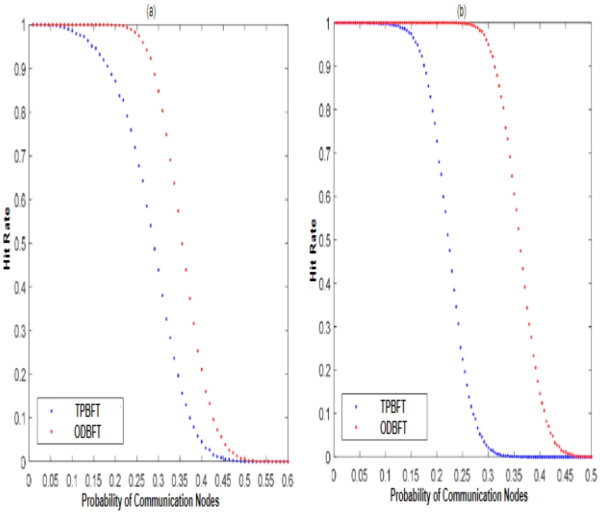


Fig 16: Analysis of hit rate various k, N values for the ODBFT and existing model. a) k=10 and N=100 b) k=15 and N=250

7. Conclusion and Future Enhancement

The proposed Cognitive Blockchain-based IoT HMS (CBC-HMS) is highly optimal, transparent, secure, and efficient. This research work uses cognitive smart digital contract which improved decision making, access permission of block, efficiency and accuracy of health monitoring system. The introduced the ODBFT consensus algorithm is to overcome Byzantine faults or malicious node problems. The ODBFT consensus algorithm is support to isolate cognitive nodes. By doing nodes isolation process classifies different nodes through that provides service to improve the impact on the blockchain consortium. ODBFT is efficient, and it improves scalability and reduces communication overhead. Evaluated through experimental analysis, ODBFT has O(n) network and communicational complexity. The comparison on transaction per second portrays that ODBFT algorithm is more comfortable for adoption and it can manage around 1800 transactions per second with communicational complexity low. Further work is focused on the implementation of the ODBFT consensus algorithm in a Blockchain-based IoT, HMS uses cost-effective, feasible, reliable, and resource-constrained protocols. After the investigation a more compact system with the best Blockchain platform more efficiently provides CBC-HMS. The proposed algorithm is feasible for providing security in a Blockchain-based IoT HMS.

References

[1] Alfandi, O, Otoum, S & Jararweh, Y 2020, "Blockchain solution for iot-based critical

infrastructures: Byzantine fault tolerance", In NOMS IEEE/IFIP Network Operations and Management Symposium, pp. 1-4.

[2] Anisi, MH, Abdullah, AH, Razak, SA & Ngadi, MA 2012, "An overview of data routing approaches for wireless sensor net-works", Sensors, vol. 12, no. 4, pp. 3964-3996.

[3] Cai, W, Jiang, W, Xie, K, Zhu, Y, Liu, Y & Shen, T 2020, "Dynamic reputation–based consensus mechanism: Real-time transactions for energy blockchain", International Journal of Distributed Sensor Networks, vol. 16, no. 3, pp. 1550147720907335.

[4] Chatterjee, P, Ghosh, SC & Das, N 2017, "Load balanced coverage with graded node deployment in wireless sensor networks", IEEE Transactions on Multi-Scale Computing Systems, vol. 3, no. 2, pp. 100-112.

[5] Feng, L, Zhang, H, Chen, Y & Lou, L 2018, "Scalable dynamic multi- agent practical byzantine fault-tolerant consensus in permissioned blockchain, Applied Sciences, vol. 8, no. 10, p. 1919.

[6] Nakamoto, S 2008, "Bitcoin: A peer-to-peer electronic cash system", Decentralized Business Review, p. 21260.

[7] Dinh, TTA, Liu, R & Zhang, M 2018, "Untangling blockchain: A data processing view of block - chain systems," IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366– 1385.

[8] Puthal, D, Mohanty, SP, Yanambaka, VP & Kougianos, E 2020, Poah: A novel consensus algorithm for fast scalable private blockchain for large-scale iot frameworks. arXiv preprint arXiv:2001.07297.

[9] Baliga, A 2017, "Understanding Blockchain Consensus Models", April, [Online] Available: https: //www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf.

[10] Sankar, LS, Sindhu, M & Sethumadhavan, M 2017, "Survey of consensus protocols on blockchain applications", 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, pp. 1-5.

[11] Cachin, C & Vukolic, M 2017, "Blockchain consensus protocols in the wild", arXiv preprint arXiv:1707.01873.

[12] Bano, S, Sonnino, A, Al-Bassam, M, Azouvi, S, McCorry, P, Meiklejohn, S & Danezis, G 2017, "Consensus in the age of blockchains", arXiv preprint arXiv:1711.03936.

[13] Lamport, L, Shostak, R & Pease, M 2019, "The Byzantine generals problem",In Concurrency: the Works of Leslie Lamport, pp. 203-226.

[14] Castro, M & Liskov, B 1999, „Practical byzantine fault tolerance", In OSDI, vol. 99, no. 1999, pp. 173-186.

[15] Mazieres, D 2015, „The stellar consensus protocol: A federated model for internet-level consensus", Stellar Development Foundation, p. 32.

[16] Liu, S, Viotti, P, Cachin, C, Quema, V & Vukolic, M 2016, „{XFT}: Practical fault tolerance beyond crashes", 12th {USENIX} Symposium on Operating Systems Design and Implementation ({OSDI}) pp. 485-500.

[17] Miller, D 2018, „Blockchain and the internet of things in the industrial sector", IT Professional, vol. 20, no. 3, pp. 15-18.

[18] Iyer, S, Thakur, S, Dixit, M, Agrawal, A, Katkam, R & Kazi, F 2019, „Blockchain based Distributed Consensus for Byzantine Fault Tolerance in PMU Network", 10th International Conference onComputing, Communication and Networking Technologies (ICCCNT), IEEE, pp. 1-7.

[19] He, L & Hou, Z 2019, „An Improvement of Consensus Fault Tolerant Algorithm Applied to Alliance Chain", IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), IEEE, pp. 1-4.

[20] Gao, S, Yu, T, Zhu, J & Cai, W 2019, „T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm", China Communications, vol. 16, no. 12, pp. 111-123.

[21] Wang, Y, Cai, S, Lin, C, Chen, Z, Wang, T, Gao, Z & Zhou, C 2019,„Study of blockchain's consensus mechanism 8 based on credit", IEEE Access, vol. 7, no. 1, pp. 10224-10231.

[22] Deng, Q 2019, „Blockchain Economical Models, Delegated Proof of Economic Value and Delegated Adaptive Byzantine Fault Tolerance and their implementation in Artificial Intelligence BlockCloud", Journal of Risk and Financial Management, vol. 12, no. 4, p. 177.

[23] Gueta, GG, Abraham, I, Grossman, S, Malkhi, D, Pinkas, B, Reiter, M & Tomescu, A 2019, „SBFT: a scalable and decentralized trust infrastructure", 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), IEEE, pp. 568-580.

[24] Ray, PP, Dash, D, Salah, K & Kumar, N 2020, „Blockchain for IoT- Based Healthcare: Background, Consensus, Platforms, and use Cases", IEEE Systems Journal.

[25] Saha, HN, Auddy, S, Pal, S, Kumar, S, Pandey, S, Singh, R & Saha, S 2017, „Health monitoring using internet of things (IoT)", 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), IEEE, pp. 69-73.

[26] Namasudra, S., Deka, G.C., Johri, P., Hosseinpour, M. and Gandomi, A.H., 2021. „The revolution of blockchain: State-of-the-art and research challenges". Archives of Computational Methods in Engineering, 28(3), pp.1497-1515.

[27] YK, CJC & Ercole, F 1998, „Living free-radical polymerization by reversible addition−fragmentation chain transfer: the RAFT process", Macromolecules, vol. 31, PP. 5559-5562.