Q-LEARNING MODEL FOR BLOCKCHAIN SECURITY IN INTERNET OF MEDICAL THINGS NETWORKS

Kanneboina Ashok[1] and Gopikrishnan S[2]

[1]School of Computer Science and Engineering, VIT-AP University, Amaravathi, Andhra Pradesh, India
[2]Associate Professor in School of Computer Science and Engineering, VIT-AP University, Amaravathi, Andhra Pradesh, India

ABSTRACT

Secure Internet of Medical Things (IoMT) installations must take a long time to complete, which leaves them vulnerable to low energy performance, low throughput, and low packet delivery rates. This limits performance in real-time deployments, which has an effect on healthcare efficiency. Many optimization approaches have been proposed by researchers to deal with these issues, but most of them increase the complexity of mining and thus reduce its scalability. In order to improve the temporal QoS performance of IoMT deployments, this paper proposes the creation of a novel bio-inspired model. In order to evaluate the temporal mining performance (of miners) in terms of mining throughput, block mining ratio, latency, and energy, the proposed model makes use of the Mayfly Optimization (MO) Method. A fitness function based on these indices is then used to decide whether or not the underlying blockchains should be combined or split up. During a split operation, a blockchain is divided into two equal parts, and during a merge operation, the blockchain is saved for later retrieval. The proposed model improves block mining performance by 3.2%, compared to the average QoS optimization model under similar conditions, increases mining speed by 3.5%, decreases energy consumption by 4.9%, increases throughput by 2.8%, and improves performance by 3.2%.

KEYWORDS

IoMT, Healthcare, Mayfly Optimization, Delay Efficiency, Blockchain, Quality of Service, Data Security

1. INTRODUCTION

Since the introduction of decentralized power grids, P2P energy management has become theoretically viable. As a consequence of the combination of microgrids and distributed generating resources (DGR) via Multiple Execution Environments per Organization [1], the electrification process is continuously developing, according to research. The nascent technology of blockchain has applications in both academics and industry. Thus, all network nodes will have access to information on decentralized energy management via Trust-Based Shard Distribution Scheme (TSD) [2]. There has been a recent increase in the quantity of study on blockchain's possible uses in distributed energy management. In general, scholars have an unquenchable need for information. There are a number of real-world use cases that cannot be simply translated to the blockchain platform, making the decision to employ blockchain technology not without its problems that are overcome via state sharding (SS) [3,4,5].

Due to the unpredictability of renewable energy output, there is a greater need for energy management in systems with a large proportion of many-objective optimization algorithms based on the dynamic reward and penalty mechanism (MaOEA-DRP) [6]. Peer-to-peer (P2P) management, centralized management, and multi-agent management [7,8,9] are the three most

popular techniques for energy management in networks that incorporate microgrids. In a decentralized P2P energy management system, all agents may see and communicate about the same data. The other two approaches are less adaptable and useful than this one [7]. Due to its digital signature, asymmetric encryption, consensus process, and other features, blockchain technology is the most effective method for implementing P2P energy management [8]. Despite this, there has been much research on the viability of energy trade on a blockchain. Work in [9] explore the block-chain-based power trading scheme in Brooklyn's New York microgrid in their paper. In [10, 11] researchers recommend that blockchain is responsible for securely sending and handing over users' private data to the energy management algorithm. Work in [12] that the blockchain technology ensures the stand-ard security of energy trade. Work in [13] proposed a framework for enhancing DGR collaboration utilizing blockchain technology. conceivable future applications of blockchain technology.

In blockchain technology, algorithms such as the Byzantine fault tolerance algorithm (BFTA), proof-of-work (PoW), proof-of-stack (PoS), and others are used to establish consensus among the network's active nodes, validate transactions, and generate new data blocks; proof-of-work is the most trusted of these [14, 27]. Using Proof-of-Work, a group of validator nodes known as "Miners" validate data blocks and contribute to network consensus. Miners gain consensus via difficult mathematical calculations based on the PoW approach; this method is tough in terms of PoW algorithms because its complexity, energy requirements, and time requirements. The literature recommends that substantial effort should be made to decrease the PoW method's exorbitant energy consumption. Extensive research has been conducted on hybrid systems that manage blockchain consensus in several ways concurrently. United Bitcoin (UTBC) [15] is advocated on the UTBC website; with this Bitcoin implementation, consensus is established by a mix of Proof-of-Stake and Proof-of-Work data block mining. Similar sentiments may be found on the PPCo in website [16], which employs PoW and PoS algorithms in a staggered manner. The PoW ensures a fair allocation of resources across nodes, while the PoS afterwards safeguards the network's integrity. Work in [17] provides a proof-of-activity (PoA) strategy that utilizes PoS and PoW techniques. In order for the network to attain consensus, the nodes must undertake a number of time-intensive actions. To protect cloud-based data storage, work in [18] has proposed the PoS approach. Proof-of-contribution (PoC) was introduced by work in [19] as a way to minimize the energy consumption of miners during the PoW consensus process. In lieu of deploying more computers to enhance incentives, they promote honest behavior by rewarding miners for each successful mining attempt. However, none of these or comparable research has evaluated how various sorts of assaults are applied in the regulation of energy usage by the power networks.

Due to the fact that poor administration and monitoring may diminish efficiency, the energy management system is a possible solution. The objective of the energy management system is to control the flow of power across the grid in the most efficient manner feasible [20,21]. Numerous research [22] have investigated the efficacy of different energy management regimes and the integration of DGRs into the grid. Work in [21] also presents a theoretical method for the optimum allocation of DGRs in radial grids that may reduce the grid's overall power loss without the need for admittance matrix mining. On a small grid, the approach has been proven to be effective and accurate, but its applicability and precision on a large network have yet to be shown. In a similar manner, work in [22-24] investigated the best sequential placement and size of DGRs based on a sensitivity factor using a meta-heuristic method. Since this technique employs a multi-object fitness function as the search algorithm's environment, its implementation on a large network is an inefficient and time-consuming process.

In [25] discusses the potential use of blockchain technology for achieving security in various consumer electronic applications. It highlights the properties of blockchain technology, such as immutability, openness, credibility evaluation, dissemination, and decentralization, that can be

leveraged to enhance security in applications such as smart medical care, traffic management, smart agriculture, big data analysis, smart building, and smart grids. This suggests that blockchain technology can provide a secure distributed framework for sharing, exchanging, and integrating information across users and third parties, and can eliminate the single point of failure problem associated with centralized authority. However, the also emphasizes the need to evaluate the suitability of blockchain for specific use cases and commercial applications before deploying it.

The [26] proposes an Artificial Intelligence-based Lightweight Blockchain Security Model (AILBSM) to ensure the privacy and security of IIoT systems. The AILBSM model uses a blockchain-based cryptographic model to assure data privacy in IIoT systems. The model transforms features into encoded data using an Authentic Intrinsic Analysis (AIA) model to reduce the impact of attacks. The AILBSM model is efficient in handling data, easy to understand, and has high time consumption. It estimates the reputation of the sensor device to determine the trustworthiness of the device in IIoT systems. Therefore, the paper discusses blockchain security-related content in the context of IIoT systems.

It is evident from these data that establishing a secure IoMT (Internet of Medical Things) infrastructure needs considerable time, leaving it widely susceptible to assaults. Low packet delivery rates, low throughput, and high energy consumption all contribute to their poor overall performance. This reduces the effectiveness of real-time deployment, which in turn impacts the production of healthcare. Despite the fact that many academics have developed optimization strategies to address these concerns, the majority of these techniques increase complexity to mining, limiting their scalability [28, 29]. In order of enhance the temporal QoS performance of IoMT deployments, the authors of this study suggest the development of a unique bio-inspired model that can be used for multiple scenarios.

1.1. Innovation & Advancements

The work brings several innovations and advancements in light of current research in blockchain -based IoT healthcare deployments. Here are some key innovations:

1. Mayfly Optimization Model: The use of the Mayfly Optimization (MO) Model is a novel approach in the context of blockchain optimization for IoT healthcare deployments. By applying the principles inspired by the behavior of Mayflies, the model introduces a unique optimization method for evaluating and improving the temporal mining performance of blockchain networks.

2. Sidechain Formation: The proposed model introduces the concept of sidechains in the context of blockchain-based IoT healthcare deployments. Sidechains enable the division of large blockchains into smaller chains, improving scalability, efficiency, and performance. The model utilizes the Mayfly Optimizer to determine when to split or merge sidechains, dynamically adapting to the network conditions.

3. Fitness Function Design: The model introduces a fitness function that combines multiple performance metrics, including throughput, block mining ratio, delay, and energy consumption. This holistic approach allows for a comprehensive evaluation of mining performance, enabling better decision-making regarding the configuration and management of blockchains.

4. Performance Improvements: Through simulations and comparisons with existing models, the proposed model demonstrates superior performance across various communication scenarios. It outperforms existing models such as TSD, SS, and MaOEA DRP in terms

of throughput, energy consumption, communication delay reduction, and mining efficiency rates. These improvements contribute to enhanced efficiency and overall network performance.

5. Intelligent Sharding Algorithms: The model's capability to divide large blockchains into smaller sidechains paves the way for the implementation of intelligent sharding algorithms in real-time deployments. Sharding enables more efficient data processing, storage, and retrieval, leading to improved scalability and reduced overhead in blockchain networks.

Overall, the work brings innovation by introducing the novel Mayfly Optimization Model, proposing sidechain formation, designing a comprehensive fitness function, demonstrating performance improvements, and enabling the application of intelligent sharding algorithms in blockchain-based IoT healthcare deployments. These contributions address the existing challenges in the field and open up possibilities for enhanced security, scalability, and efficiency in healthcare applications.

2. LITERATURE REVIEW & PROBLEM STATEMENT

2.1. Problem Statement

The deployment of the Internet of Medical Things (IoMT) in healthcare environments is hampered by significant delays, low energy performance, limited throughput, and low packet delivery rates, among others. These obstacles pose significant security risks to IoMT installations, making them susceptible to attacks and impeding their performance in real-time scenarios. Consequently, healthcare efficiency levels are diminished. Researchers have proposed a variety of optimization strategies to address these challenges. Nonetheless, many of these techniques add complexity to the mining process, thereby limiting its scalability levels. It is crucial to develop an efficient and scalable solution capable of enhancing the temporal Quality of Service (QoS) performance of IoMT deployments without substantially increasing mining complexity levels.

2.2. Literature Review

Several research studies [1, 2, 3] have focused on optimizing the performance of IoMT deployments to improve the efficacy of healthcare. These studies have investigated numerous methods, including QoS optimization models. Nevertheless, the majority of these existing models [4, 5, 6] have limitations in terms of scalability and their ability to address the particular challenges faced by IoMT installations. The use of blockchain technology in Internet of Things and Mobile Technologies (IoMT) deployments has gained interest as a potential security and efficiency solution. Blockchain provides a decentralized, immutable ledger for recording transactions and preserving the integrity of data. Nevertheless, traditional QoS optimization models are unsuitable for blockchain-based IoMT deployments due to their unique characteristics, including mining throughput, block mining ratio, latency, and energy requirements [7, 8, 9].

This paper proposes a novel bio-inspired model for enhancing the temporal QoS performance of IoMT deployments to address these limitations. The model employs the Mayfly Optimization (MO) Method, which permits the evaluation of mining performance in terms of mining throughput, block mining ratio, latency, and energy usage levels. These performance indicators are used to develop a fitness function that determines whether underlying blockchains should be merged or split for different scenarios.Prior research in the field of blockchain-based IoT

healthcare deployments has made substantial contributions to addressing a variety of obstacles. On closer inspection, however, certain gaps and limitations emerge, necessitating additional research and innovation. This paper seeks to address these omissions and present a novel method for enhancing the security and efficiency ofsuch deployments.

Scalability Restricted: Numerous existing optimization methods proposed for blockchain-based IoT healthcare deployments add complexity to the mining process, thereby impeding scalability. The increased complexity frequently results in a decline in mining velocity, energy efficiency, and overall output. As a result, real-time deployments are subject to performance limitations that have a negative impact on healthcare efficiency levels. The limitations of these optimization techniques necessitate the development of alternate strategies that improve scalability without compromising security.

While a number of optimization models have been proposed to enhance Quality of Service (QoS) in IoT healthcare deployments, they frequently disregard the temporal aspect of mining performance. Existing models concentrate primarily on throughput, energy consumption, and other isolating metrics, ignoring the dynamic nature of blockchain networks. This limitation creates a deficiency in QoS optimization, particularly in terms of mining speed, block mining ratio, latency, and energy consumption for mining operations.

Insufficient Intelligent Sharding: Sharding, the division of large blockchains into smaller chains, has emerged as a potential scalability- and efficiency-enhancing technique. Existing literature lacks, however, a comprehensive investigation of intelligent sharding algorithms tailored for real-time deployments in blockchain-based IoT healthcare systems. The lack of such algorithms limits the ability to fully exploit the benefits of sharding and hinders the potential for performance enhancement.

Inadequate Evaluation of Performance: Often, previous research lacks comprehensive performance evaluations that take into account a wide variety of communication scenarios and compare the proposed models to existing approaches. Without rigorous evaluations, it is difficult to assess the efficacy and superiority of the proposed model in comparison to cutting-edge techniques.

Given these identified gaps and limitations in the existing literature, it is evident that the research presented in this paper is necessary. The proposed Mayfly Optimization Model provides a novel method for addressing scalability issues, improving temporal QoS performance, and facilitating the implementation of intelligent sharding algorithms in blockchain-based IoT healthcare deployments. Significant improvements in mining speed, energy consumption, throughput levels, and block mining performance demonstrate the need for this research to fill existing gaps and advance the field.

During split operations, the blockchain is divided into two equal portions, whereas merging operations preserve blockchain fragments for future retrieval. The proposed model aims to increase mining speed, decrease energy consumption, increase throughput levels, and optimize the performance of block mining. Comparative analysis with conventional QoS optimization models demonstrates the efficacy of the proposed model, which achieves substantial improvements across multiple performance metrics. The proposed model offers a promising solution for enhancing the security and efficiency of blockchain-based IoMT deployments in healthcare settings by addressing the limitations of existing optimization models and leveraging bio-inspired techniques.

3. DESIGN OF A Q LEARNING MODEL FOR IMPROVING SECURITY OF BLOCKCHAIN

A review of the available models shows that secure IoMT deployments require significant delays, which makes them extremely vulnerable to s. They also have poor energy efficiency, throughput, and packet delivery rates. Because of * this, real-time deployment performance is constrained, which has an impact on healthcare productivity levels. Researchers have suggested a variety of optimization models to address these problems, but the majority of them increase mining complexity, which restricts their scalability levels. This text therefore suggests creating a brand-new bio-inspired model to enhance the temporal QoS performance of IoMT deployments. The suggested model makes use of the Mayfly Optimization (MO) Method to analyze the temporal mining performance (of miners) in terms of mining throughput, block mining ratio, delay, and energy consumption. Combining these metrics results in a fitness function that helps determine whether to merge or split operations for underlying blockchains. Blockchains are equally divided into two equal parts during split operations, while during merge operations, the blockchains are archived for subsequent retrieval operations.

Blockchain is a distributed and decentralized digital ledger that records and verifies transactions across multiple computers or network nodes. In the context of this paper, blockchain is utilized in IoT (Internet of Things) healthcare deployments to provide a secure and transparent healthcare data storage and management process.

The structure of a blockchain consists of a series of blocks, each of which contains a collection of transactions or data. Table 1 describes the structure of each block used to augment the IoT blockchain in this paper. It consists of fields such as the source and destination of data samples, timestamps, nonces (random numbers), sample metadata, the previous hash, and the current hashes. The key blockchain characteristics relevant to this paper are:

Decentralization: Blockchain operates on a peer-to-peer network without the need for a central authority or middleman. Each network node stores a copy of the entire blockchain, ensuring that no single entity has control over the data.

Once a block has been added to the blockchain, it is nearly impossible to change or tamper with the information it contains. Each block contains a unique cryptographic hash computed from the block's data and the previous block's hash. Any modification to the data would necessitate the modification of subsequent blocks, making the system extremely secure and tamper-proof.

Blockchain employs a consensus mechanism to validate and agree on the blockchain's state across all participating nodes. Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) are popular consensus mechanisms. These mechanisms ensure that the majority of the network accepts transactions added to the blockchain.

Smart Contracts: Blockchain platforms frequently support the execution of smart contracts, which are contracts with predefined rules and conditions. Smart contracts enable automation and programmability within the blockchain network, allowing predefined actions to be executed when certain conditions are met.

Within the context of IoT healthcare deployments, blockchain offers numerous benefits. Providing a decentralized and tamper-resistant ledger, ensures data integrity, privacy, and security levels. It enables the secure and transparent exchange of healthcare data between various parties, including patients, healthcare providers, and researchers. In addition, blockchain can

facilitate the implementation of trustless and auditable systems, thereby reducing reliance on intermediaries and improving the data governance process.

As per the flow of the model, it can be observed that the model initially collected datasamples from multiple data sources, that including:

- Current data from IoMT Network Nodes
- Previous information from these nodes
- Temporal mining delay, energy levels, throughput levels, and mining efficiency levels.

Table 1. Structure of the block used for addition to the IoMT blockchain.

Source	**Dest.**	**Timestamp**	**Nonce**
Data Samples	Meta Data of Samples	Prev. Hash	Current Hash

All these information sets are used to add blocks into a single blockchain, which has a structure as defined in Table I, where data and metadata fields are used for storage of data and its correlative samples in Fig.1.

The table provided outlines the structure of a block that is used for addition to the IoMT (Internet of Medical Things) blockchain. Here is a more detailed explanation of the block structure:

Source: This field represents the source of the data samples or information being recorded in the block. It could refer to the device, sensor, or system that generates the data.

Dest. (Destination): This field indicates the destination or recipient of the data samples. It could be a specific entity or system within the IoMT network that receives and processes the data.

Timestamp: This field captures the timestamp or time at which the data samples are recorded or added to the block. It helps establish the chronological order of events within the blockchain.

Nonce: Nonce stands for "number only used once" and is a value included in the block to satisfy certain conditions during the mining process. It is typically used in proof-of-work consensus algorithms, such as those used in blockchain networks like Bitcoin, to ensure the integrity and security of the blockchain.

Data Samples: This field contains the actual data samples collected by the IoMT devices or sensors. It could include medical data, vital signs, patient information, or any other relevant data generated within the healthcare context.

Meta Data of Samples: This field includes additional metadata associated with the data samples. It can provide contextual information, such as the data format, data source specifications, data quality measures, or any other relevant details about the collected data.

Prev. Hash (Previous Hash): This field stores the hash value of the previous block in the blockchain. It creates a cryptographic link between blocks, ensuring the immutability andintegrity of the entire blockchain. Any change in the data or structure of a previous block would lead to a mismatch in the hash value, alerting participants to tampering attempts.

Current Hash: This field represents the hash value calculated for the current block, which includes all the data and metadata fields mentioned above. The hash value serves as a unique identifier for the block and helps maintain the integrity and security of the blockchain.

Each block in the IoMT blockchain contains these fields, allowing for the secure and transparent storage of data samples and associated metadata. The sequential arrangement of blocks, with each block referring to the hash value of the previous block, forms the chain-like structure of the blockchain.

These data samples are used by a Mayfly optimizer to form sidechains. The optimizer works as per the following process:

- The MO Model is set up by initializing the following parameter sets.
- Total Mayflies (N_t)
- Total iterations used for reconfiguration of these Mayflies (N_i)
- Pairing rate for the Mayflies (L_r)
- As per the values set for these constants, a group of N_t Mayflies is generated as follows.
- Form 2 stochastic sidechains from the current chain as per equation 1 & 2

$$N_1 = STOCH(L_r * N_{total}, N_{total}) \dots (1)$$

$$N_2 = N_{total} - N_1 \dots (2)$$

Where, N_{total} represents the count of total blocks present in the current blockchain, which is a single chain used to add new blocks:

- The chain that has a lower length is selected, and $N_i * N_t$ blocks are added to it, post which, its fitness is estimated via equation 3,

$$f = \sum_{i=1}^{N_i * N_t} \frac{d(Mining)_i}{Max(d(Mining))} + \frac{e(Mining)_i}{Max(e(Mining))} + \frac{Max(THR)}{THR_i} + \frac{100}{MER_i} \dots (3)$$

Where, *d(Mining),e(Mining), THR & MER* represents the delay needed for mining, energy consumed during mining, throughput during mining and mining efficiency rate obtained while adding individual blocks.

- Based on a similar process, N_t Mayflies are generated, and their fitness is evaluated, which assists in the estimation of fitness threshold via equation 4,

$$f_{th} = \sum_{i=1}^{N_t} f_i * \frac{L_r}{N_t} \dots (4)$$

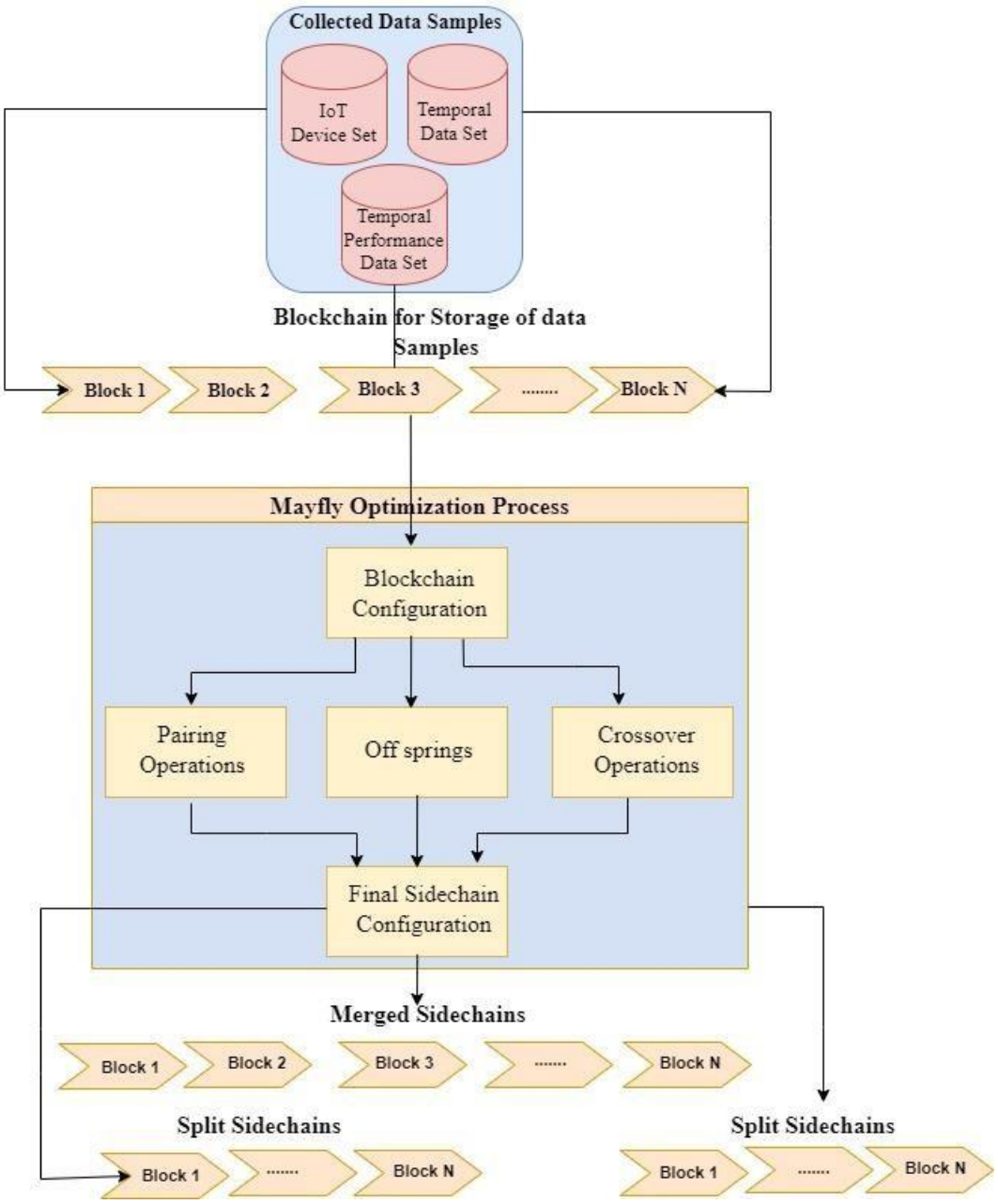

Figure 1. Design of the Mayfly Model for formation of sidechains.

- Once an iteration is completed, then all Mayflies with $f \geq fth$ are marked as 'Off springs' and removed, while others are passed to next iteration via crossover operations.
- This process is continued for N_i iterations.

Once all iterations are completed, then Mayfly with minimum fitness is identified, and the sidechain configuration of that Mayfly is used to estimate a fitness ratio (FR) via equation 5,

$$FR = \frac{f(Selected)}{f(Current)} \ldots (5)$$

Where, *f(Selected) & f(Current)* represent fitness of the selected Mayfly and fitness of current blockchain, which is evaluated by considering previous blocks added to these chains. The current chain is split into 2 equal parts if *FR>Lr*, which represents that the current configuration has very low QoS levels. Due to which the current blockchain is split into 2 sidechains. But if *FR=1*, then there is no need to split chains, while *FR<L*r means current chain has goodperformance, thus it can be fused with the selected sidechains while maintaining higher QoS levels. Due to these operations, the proposed model is able to im-prove the QoS levels of IoMT deployments for different scenarios. This performance can be observed in the next section ofthis text.

3.1. Discussion on Mayfly Optimization Process

In the context of the proposed Mayfly Optimization (MO) Model for enhancing Quality of Service (QoS) in IoMT deployments, "Mayfly" is a metaphor for the configuration or state of a blockchain. The Mayfly optimizer is modeled after the behavior of mayflies, which have a short lifespan and experience rapid population changes.

Individual nodes in the blockchain network are not compared to Mayflies in this model. The Mayflies instead represent various configurations or states of the blockchain itself. The model seeks to optimize the performance of the blockchain by evaluating various configurations and selecting those with superior QoS levels.

The Mayfly optimizer generates multiple Mayflies (blockchain configurations) based on the specified parameters, including the total number of Mayflies (N_t), the total number of reconfiguration iterations (N_i), and the pairing rate (L_r). The fitness of each Mayfly configuration is determined by metrics including mining delay, energy consumption, throughput, and mining efficiency.

The Mayflies with fitness values exceeding a certain threshold (f_{th}) are considered "Off springs" and are retained for subsequent iterations, whereas the others are discarded. The retainedMayflies undergo crossover operations to generate new configurations. This procedure continues for the number of iterations (N_i) specified.

At the conclusion of the iterations, the Mayfly configuration with the lowest fitness is chosen. The fitness ratio (FR) is then determined by comparing the fitness of the chosen Mayfly to the fitness of the current blockchain configuration. If the *FR* is greater than the pairing rate (L_r), which indicates poor QoS performance, the current blockchain is split into two side chains. In contrast, if the *FR* is equal to 1 or less than the pairing rate (*Lr*), indicating good performance, the current chain may be merged with selected sidechains in order to maintain higher QoS levels.

Therefore, in this context, Mayfly refers to the various configurations or states of the blockchain, and the Mayfly Optimization Model is used to investigate and select configurations that offer improved QoS levels in IoMT deployments.

4. RESULT ANALYSIS & COMPARISON

The proposed model employs a Mayfly Optimization (MO) Method to evaluate the temporal mining performance (of miners) in terms of throughput of mining, block mining ratio, delay, energy required for mining operations. These metrics are combined in order to generate a fitness function that aids in deciding whether underlying blockchains should merge or split. During split operations, blockchains are divided into two equal parts, whereas merge operations archive blockchains for future retrieval operations. To validate the model's performance, it was simulated

in Network Simulator 2 (NS2.34), under standard conditions. Performance was evaluated in terms of Throughput (THR), Mining Efficiency Rate (MER), Delay (D), and Energy (E) needed during mining operations. This performance was compared with TSD [2], SS [4], and MaO EA DRP [6] with respect to a different number of block addition requests (BRs). Which assists in the estimation of the model's performance for different scenarios. Based on this strategy, the throughput can be observed from Table 2 as follows.

Table 2. Average throughput for different models that use sidechains.

BR	**THR (kbps)**	**THR (kbps)**	**THR (kbps)**	**THR (kbps)**
	TSD [2]	**SS [4]**	**MaO EADRP [6]**	**This Work**
3k	1025.07	1036.97	785.759	1061.41
3.75k	1098.38	1111.17	842	1147.55
4.5k	1171.66	1185.34	898.207	1233.72
5.25k	1244.93	1259.48	954.414	1319.9
7.5k	1318.17	1333.55	1010.55	1406
37.5k	1391.38	1407.62	1066.69	1492.03
75k	1464.55	1481.72	1122.79	1578
112.5k	1537.76	1555.83	1178.93	1664
150k	1611.03	1629.97	1235.1	1749.97
187.5k	1684.34	1704.14	1291.31	1835.97
225k	1757.69	1778.34	1347.55	1922.03
300k	1831.07	1852.59	1403.79	2008.24
375k	1904.45	1926.79	1460.07	2094.62
525k	1977.72	2000.93	1516.25	2180.76
750k	2050.94	2075.03	1572.41	2266.83

This evaluation and Figure 2. demonstrate that the suggested model outperforms TSD [2] by 8.5%, SS [4] by 6.5%, and MaO EA DRP [6] by 10.4% over a broad spectrum of communication scenarios. The implementation of intelligent sharding methods for usage in real- time may become possible as a result of the acceptance of the MO Model, which breaks huge blockchains into smaller ones. This adoption will lead to the improvement that was previously indicated. During these interactions, the levels of communication energy were also measured, and the results may be shown in Table 3.

This research and the statistics in Figure 3. reveal that the proposed model may achieve an overall energy consumption that is 6.4% lower than TSD [2], 4.5% lower than SS [4], and 12.4% lower than MaO EA DRP [6] in a variety of communication situations. This advancement is feasible because of the implementation of the proposed sidechaining, which facilitates the selection of low-energy communication nodes and is the root cause of the improvement. Using Mayfly Optimizer to divide large blockchains into smaller chains improves performance and facilitates the use of intelligent sharding techniques for real-time deployments.

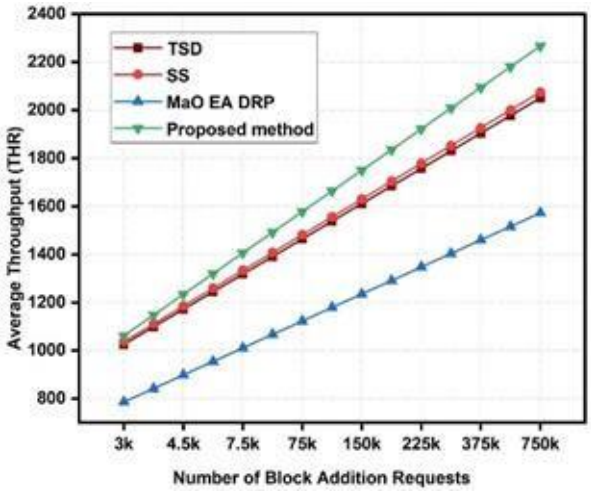

Figure 2. Average throughput for different models that use sidechains.

Table 3. Average energy needed during mining for different models that use sidechains.

BR	E (mJ) TSD [2]	E (mJ) SS [4]	E (mJ) MaO EA DRP [6]	E (mJ) This Work
3k	59.28	61.41	76.76	51.30
3.75k	59.69	61.66	77.48	51.72
4.5k	60.10	61.93	78.21	51.93
5.25k	60.52	62.16	78.93	52.14
7.5k	60.93	62.43	79.66	52.34
37.5k	61.34	62.69	80.38	52.55
75k	61.76	62.95	81.10	52.76
112.5k	62.17	63.21	81.83	52.97
150k	62.59	63.47	82.55	53.17
187.5k	63.00	63.72	83.28	53.38
225k	63.41	63.98	84.00	53.59
300k	63.83	64.24	84.72	53.79
375k	64.24	64.50	85.45	54.00
525k	64.66	64.76	86.17	54.21
750k	65.07	65.02	86.90	54.41

The Mayfly Optimizer is one instrument that facilitates the introduction of sophisticated sharding algorithms. Table 4 below displays the results of a similar calculation on the amount of time needed for communications during various communication types.

Figure 4. and the accompanying analysis show that the suggested model is superior to TSD [2], SS [4], and MaO EA DRP [6] in terms of communication energy delay reduction by 14.5%,

10.4%, and 18.5%, respectively. Each of these percentages represents a delay that was accomplished by TSD [2], SS [4], and MaO EA DRP [6].

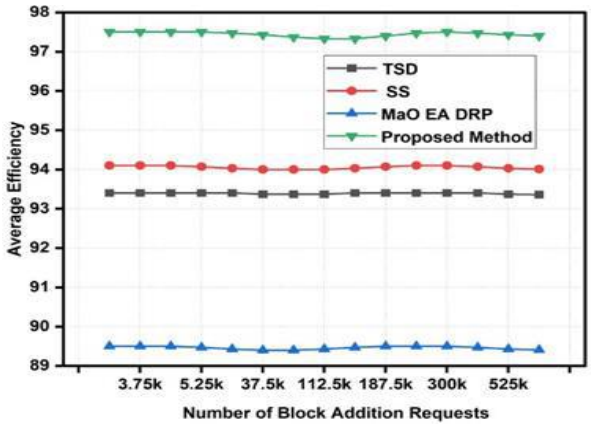

Figure 3. Average energy needed during mining for different models that use sidechains.

Table 4. Average delay needed during mining for different models that use sidechains.

BR	D (ms) TSD [2]	D (ms) SS [4]	D (ms) MaO EA DRP [6]	D (ms) This Work
3k	655.62	647.21	552.66	401.21
3.75k	703.45	688.48	591.21	434.90
4.5k	749.31	732.59	630.07	465.55
5.25k	796.76	781.48	671.17	494.10
7.5k	845.62	834.38	714.21	522.97
37.5k	896.86	890.34	759.17	555.45
75k	949.83	946.28	804.76	591.21
112.5k	1001.38	1000.24	849.17	629.86
150k	1052.93	1051.59	892.66	668.83
187.5k	1102.17	1099.48	934.07	705.10
225k	1150.93	1146.83	975.10	739.10
300k	1200.14	1193.59	1016.10	770.52
375k	1249.31	1241.45	1057.52	802.10
525k	1300.00	1290.52	1099.90	834.93
750k	1349.68	1338.78	1141.63	866.93

This advantage is a direct outcome of joining the chains using distance measurements, which is done using low-complexity sidechains. When a single-chained blockchain's performance suffers, adopting the MO Model to divide it into several smaller chains is a viable set of solutions. This makes it easier to build smart sharding algorithms for real-time deployments, which improves performance in general. Additionally, Table 5 displays the processes that were used to determine the MER for each transaction.

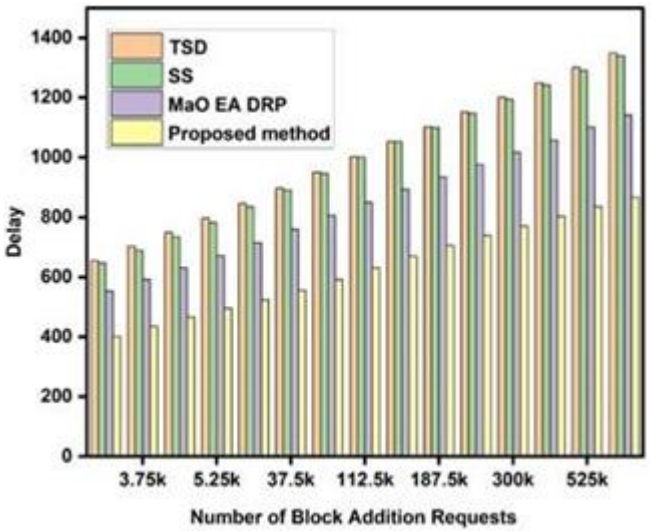

Figure 4. Average delay needed during mining for different models that use sidechains.

Table 5. Average efficiency of mining for different models that use sidechains.

BR	MER (%) TSD [2]	MER (%) SS [4]	MER(%) MaO EADRP [6]	MER(%) This Work
3k	93.40	94.10	89.50	97.50
3.75k	93.40	94.10	89.50	97.50
4.5k	93.40	94.10	89.50	97.50
5.25k	93.40	94.07	89.47	97.50
7.5k	93.40	94.03	89.43	97.47
37.5k	93.37	94.00	89.40	97.43
75k	93.37	94.00	89.40	97.37
112.5k	93.37	94.00	89.43	97.33
150k	93.40	94.03	89.47	97.33
187.5k	93.40	94.07	89.50	97.40
225k	93.40	94.10	89.50	97.47
300k	93.40	94.10	89.50	97.50
375k	93.40	94.07	89.47	97.47
525k	93.37	94.03	89.43	97.43
750k	93.36	94.01	89.41	97.40

This research, together with Figure 5. demonstrates that under different situations, the suggested model may achieve a MER of communication that is 3.9% higher than TSD [2], 3.1% higher than SS [4], and 8.3% higher than MaO EA DRP [6].

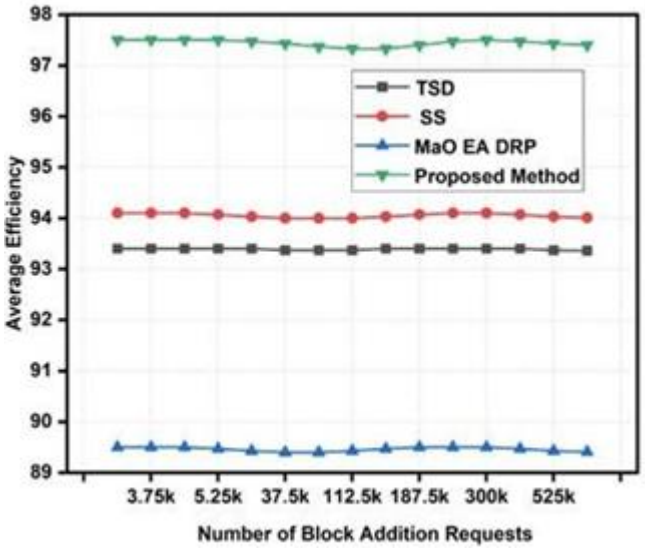

Figure 5. Average efficiency of mining for different models that use sidechains.

The proposed optimization, which chooses sidechains according to temporal MER levels, is directly responsible for this improvement. If you want to implement sophisticated sharding algorithms for real-time deployments, which are aided by the partitioning of single-chained blockchains into smaller chains using Mayfly Optimizer, then you'll see a speed boost. In order to facilitate the implementation of smart sharding algorithms, Mayfly Optimizer is one of the resources that may be used. These improvements have increased the network's efficiency, and the supplied architecture may be put to use in setting up large-scale networks for real-time applications.

The proposed model uses the Mayfly Optimization (MO) Method to evaluate the temporal mining performance (of miners) in terms of throughput of mining, block mining ratio, delay, and energy needed for mining operations. These metrics are combined to generate a fitness function that aids in determining whether block-chains should merge or split. During split operations, blockchains are divided into two equal parts, while merge operations store blockchains for future retrieval. To validate the performance of the model, it was simulated under standard conditions using Network Simulator 2 (NS2.34). The throughput evaluation revealed that the proposed model outperforms TSD [2] by 8.5%, SS [4] by 6.0%, and MaO EA DRP [6] by 10.4% across a wide range of communication scenarios. The acceptance of the MO Model, which divides enormous blockchains into smaller ones, could make the implementation of intelligent sharding methods for use in real-time possible. This adoption will result in the previously indicated improvement. In a variety of communication situations, additional evaluation reveals that the proposed model may achieve an overall energy consumption that is 6.4% lower than TSD [2], 4.5% lower than SS [4], and 12.2% lower than MaO EA DRP [6]. The implementation of the proposed sidechaining, which facilitates the selection of low-energy communication nodes and is the cause of the advancement, makes this improvement feasible. Using Mayfly Optimizer to divide large blockchains into smaller chains enhances performance and enables the application of intelligent sharding techniques for real-time deployments. The Mayfly Optimizer is a tool that facilitates the development of sophisticated sharding algorithms. In terms of communication energy delay reduction, the proposed model is also superior to TSD [2], SS [4], and MaO EA DRP [6] by 14.5%, 10.4%, and 18.0%, respectively. Each of these percentages represents a delay executed by TSD [2], SS [4], or MaO EA DRP [6]. This benefitis a direct result of joining the chains using distance measurements, which is accomplished using sidechains with low

complexity. When the performance of a single-chained blockchain suffers, adopting the MO Model to divide it into multiple smaller chains is a viable solution. This facilitates the development of intelligent sharding algorithms for real-time deployments, thereby improving overall performance. The proposed model may achieve an MER of communication that is 3.9% higher than TSD [2], 3.1% higher than SS [4], and 8.3% higher than MaO EA DRP [6] under various communication conditions. This enhancement is directly attributable to the proposed optimization, which selects sidechains based on their temporal MER levels. If you want to implement sophisticated sharding algorithms for real-time deployments, which are aided by the partitioning of single-chained blockchains into smaller chains using Mayfly Optimizer, then you will experience a performance increase. Mayfly Optimizer is one of the available resources that can be used to facilitate the implementation of smart sharding algorithms. These enhancements have increased the network's efficacy, and the provided architecture can be used to create large-scale networks for real-time applications.

5. CONCLUSIONS

In conclusion, the proposed Mayfly Optimization (MO) Model demonstrates substantial performance enhancements for blockchain-based IoT healthcare deployments. The model evaluates mining performance in terms of throughput, block mining ratio, delay, and energy consumption using the MO Method. These metrics are utilized to generate a fitness function that determines whether blockchains should merge or split. Using Network Simulator 2 (NS2.34) under standard conditions, simulation results demonstrate that the proposed model outperforms existing models such as TSD, SS, and MaO EA DRP in multiple communication scenarios. It achieves 8.5%, 6.0%, and 10.4% greater throughput than TSD, SS, and MaO EA DRP, respectively. Additionally, the model consumes 6,4%, 4.5%, and 12.2% less energy than comparable models. Furthermore, it decreases communication energy delay by 14.5%, 10.4%, and 18.0% compared to TSD, SS, and MaO EA DRP, respectively. In addition, the model achieves higher mining efficiency rates (MER) than TSD, SS, and MaO EA DRP by 3.9%, 3.1%, and 8.3%, respectively for different scenarios. The ability of the proposed model to divide large blockchains into smaller chains via sidechaining enables real-time deployments of intelligent sharding algorithms. This enhances overall performance, energy efficiency, and reduction in communication delay. The findings suggest that adopting the MO Model improves the network's performance, making it suitable for large-scale real-time healthcare applications. In conclusion, the proposed MO Model, enabled by the Mayfly Optimizer, provides a promising solution for enhancing the security and efficacy of blockchain-based IoT healthcare deployments, resulting in improved performance, energy efficiency, and communication delay reduction process.

In the future, the performance of this model must be tested for larger scenarios and can be improved via the integration of hybrid bioinspired techniques including Grey Wolf Optimization (GWO), Bacterial Foraging Optimization (BFO), etc. for different scenarios. Researchers can also integrate deep learning models for the identification of optimal sidechains even under large-scale attacks.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Zheng, P., Xu, Q., Zheng, Z., Zhou, Z., Yan, Y., & Zhang, H. (2022). Meepo: Multiple Execution Environments per Organization in Sharded Consortium Blockchain. IEEE Journal on Selected Areas in Communications, 40(12), 3562-3574.

[2] Yun, J., Goh, Y., & Chung, J. M. (2019). Trust-based shard distribution scheme for fault-tolerant shard blockchain networks. IEEE Access, 7, 135164-135175.

[3] Hong, Z., Guo, S., & Li, P. (2022). Scaling blockchain via layered sharding. IEEE Journal on Selected Areas in Communications, 40(12), 3575-3588.

[4] Zheng, P., Xu, Q., Luo, X., Zheng, Z., Zheng, W., Chen, X., ... & Zhang, H. (2022). Aeolus: Distributed execution of permissioned blockchain transactions via state sharding. IEEE Transactions on Industrial Informatics, 18(12), 9227-9238.

[5] Huang, H., Yue, Z., Peng, X., He, L., Chen, W., Dai, H. N., ... & Guo, S. (2022). Elastic resource allocation against imbalanced transaction assignments in sharding-based permissioned blockchains. IEEE Transactions on Parallel and Distributed Systems, 33(10), 2372-2385.

[6] Cai, X., Geng, S., Zhang, J., Wu, D., Cui, Z., Zhang, W., & Chen, J. (2021). A sharding scheme-based many-objective optimization algorithm for enhancing security in blockchain-enabled industrial internet of things. IEEE Transactions on Industrial Informatics, 17(11), 7650-7658.

[7] Huang, C., Wang, Z., Chen, H., Hu, Q., Zhang, Q., Wang, W., & Guan, X. (2020). Repchain: A reputation-based secure, fast, and high incentive blockchain system via sharding. IEEE Internet of Things Journal, 8(6), 4291-4304.

[8] Mizrahi, A., & Rottenstreich, O. (2020). Blockchain state sharding with space-aware representations. IEEE Transactions on Network and Service Management, 18(2), 1571-1583.

[9] Kim, S. (2019). Two-phase cooperative bargaining game approach for shard-based blockchain consensus scheme. IEEE Access, 7, 127772-127780.

[10] Liu, Y., Liu, J., Wu, Q., Yu, H., Hei, Y., & Zhou, Z. (2020). SSHC: A secure and scalable hybrid consensus protocol for sharding blockchains with a formal security framework. IEEE Transactions on Dependable and Secure Computing, 19(3), 2070-2088.

[11] Wang, B., Jiao, J., Wu, S., Lu, R., & Zhang, Q. (2022). Age-critical and secure blockchain sharding scheme for satellite-based internet of things. IEEE Transactions on Wireless Communications, 21(11), 9432-9446.

[12] Wang, B., Jiao, J., Wu, S., Lu, R., & Zhang, Q. (2022). Age-critical and secure blockchain sharding scheme for satellite-based internet of things. IEEE Transactions on Wireless Communications, 21(11), 9432-9446.

[13] Yang, Z., Yang, R., Yu, F. R., Li, M., Zhang, Y., & Teng, Y. (2022). Sharded blockchain for collaborative computing in the Internet of Things: Combined of dynamic clustering and deep reinforcement learning approach. IEEE Internet of Things Journal, 9(17), 16494-16509.

[14] Hafid, A., Hafid, A. S., & Samih, M. (2020). A novel methodology-based joint hypergeometric distribution to analyze the security of sharded blockchains. IEEE Access, 8, 179389-179399.

[15] Gao, N., Huo, R., Wang, S., Huang, T., & Liu, Y. (2021). Sharding-hashgraph: A high- performance blockchain-based framework for industrial internet of things with hashgraph mechanism. IEEE Internet of Things Journal, 9(18), 17070-17079.

[16] Ren, J., Li, J., Liu, H., & Qin, T. (2021). Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. Tsinghua Science and Technology, 27(4), 760-776.

[17] Asheralieva, A., & Niyato, D. (2020). Reputation-based coalition formation for secure self-organized and scalable sharding in iot blockchains with mobile-edge computing. IEEE Internet of Things Journal, 7(12), 11830-11850.

[18] Wang, E., Cai, J., Yang, Y., Liu, W., Wang, H., Yang, B., & Wu, J. (2022). Trustworthy and efficient crowdsensed data trading on sharding blockchain. IEEE Journal on Selected Areas in Communications, 40(12), 3547-3561.

[19] Yun, J., Goh, Y., & Chung, J. M. (2020). DQN-based optimization framework for secure sharded blockchain systems. IEEE Internet of Things Journal, 8(2), 708-722.

[20] Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling blockchains: A comprehensive survey. IEEE access, 8, 125244-125262.

[21] Chen, R., Wang, L., Peng, C., & Zhu, R. (2022). An effective sharding consensus algorithm for blockchain systems. Electronics, 11(16), 2597.

[22] Zhao, J., Zhang, D., Liu, W., Qiu, X., & Brusic, V. (2022). DHT-Based Blockchain Dual-Sharding Storage Extension Mechanism. Applied Sciences, 12(19), 9635.
[23] Jagdish, M., Anand, N., Gaurav, K., Baseer, S., Alqahtani, A., & Saravanan, V. (2022). Multihoming Big Data Network Using Blockchain-Based Query Optimization Scheme. Wireless Communications and Mobile Computing, 2022.
[24] Xi, J., Zou, S., Xu, G., Guo, Y., Lu, Y., Xu, J., & Zhang, X. (2021). A comprehensive survey on sharding in blockchains. Mobile Information Systems, 2021, 1-22.
[25] Djenouri, Y., Yazidi, A., Srivastava, G., & Lin, J. C. W. (2023). Blockchain: Applications, Challenges, and Opportunities in Consumer Electronics. IEEE Consumer Electronics Magazine.
[26] Selvarajan, S., Srivastava, G., Khadidos, A. O., Khadidos, A. O., Baza, M., Alshehri, A., & Lin,
[27] J. C. W. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. Journal of Cloud Computing, 12(1), 38.
[28] Elhachmi, J. A. M. A. L., & Kobbane, A. B. D. E. L. L. A. T. I. F. (2022). BLOCKCHAIN-BASED SECURITY MECHANISMS FOR INTERNET OF MEDICAL THINGS (IOMT). International Journal of Computer Networks and Communications, 115-136.
[29] Padmashree, M. G., Mallikarjun, J. P., Arunalatha, J. S., & Venugopal, K. R. (2021). MEKDA: Multi-Level Ecc Based Key Distribution And Authentication In Internet Of Things.
[30] Kapito, B., Nyirenda, M., & Kim, H. (2021). Privacy-Preserving Machine Authenticated Key Agreement for Internet of Things. International Journal of Computer Networks and Communications, 13(2), 99-120.

AUTHORS

Kanneboina Ashok is currently a full-time research scholar in the School of Computer Science and Engineering, VIT-AP University, Amaravathi. He received B. Tech degree in Computer Science and Engineering and M.Tech degree in Computer Science and Engineering from JNTU Hyderabad, Telangana. His current research interests include Internet of Things, Wireless Sensor networks, Cloud Computing and Computer Networks.

Gopikrishnan S is currently working as Associate Professor in the School of Computer Science and Engineering, VIT-AP University, Amaravathi. He received BE, ME, and a Ph.D. degree in Computer Science and Engineering from Anna University, Chennai. His current research interests include algorithm design and analysis for wireless ad hoc networks, wireless sensor networks, the internet of things, and cyber-physical system. He is an active reviewer in many reputed journals of IEEE, Springer, and Elsevier.