Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 3 (2025)

Design of an Efficient QOS Aware Trust-Based Security Model with Bioinspired Sidechains for Healthcare Deployments

[1]Miss.Smruti P. Patil, [2]Mr.Amol P. Pande, [3] Dr. Chandrashekhar Raut

[1]Department of Computer Engineering , Datta Meghe College Of Engineering, Airoli, Navi Mumbai,India (Research Scholar), smritipatil85@gmail.com

[2] Prof Department of Computer Engineering, Datta Meghe College Of Engineering, Airoli, Navi Mumbai, India, amol.pande@dmce.ac.in

[3]Prof Department of Computer Engineering, Datta Meghe College Of Engineering, Airoli, Navi Mumbai, India, cmr.cm.dmce@gmail..com

Article History:

Received: *27-07-2024*

Revised: *14-09-2024*

Accepted: *30-09-2024*

Abstract:

Increased adoption of blockchain technology in healthcare systems has paved the way for transparent and secure data management. However, the inherent difficulties of scalability, performance, and security in blockchain networks necessitate the development of efficient models to ensure Quality of Service (QoS) and reliability. In this paper, we propose a novel QoS-aware trust-based security model for healthcare blockchain deployments that addresses these challenges by taking temporal energy consumption, temporal delay, temporal throughput, and temporal Packet Delivery Ratio (PDR) levels into account when selecting miner nodes. For efficient miner node selection, our model employs trust-based analysis. While for the formation of sidechains an efficient Grey Wolf Optimizer (GWO) Model is used, which is a metaheuristic technique inspired by hunting behaviour of Wolves in real-time scenarios. Effectively balancing the trade-off between exploration and exploitation, the GWO algorithm enables the selection of optimal miner nodes that meet the desired QoS requirements. By incorporating temporal metrics, our model adapts dynamically to changing network conditions, ensuring optimal resource utilization and enhanced network performance levels. To assess the efficacy of our proposed model, we ran extensive simulations and compared its performance to that of existing sidechaining models. The outcomes demonstrate significant enhancements in multiple aspects. In comparison to state-of-the-art sidechaining models, our model achieves an impressive 8.5% reduction in delay, 3.9% reduction in energy consumption, 4.5% increase in throughput, and 2.5% improvement in PDR levels. These enhancements demonstrate the efficacy and efficiency of our healthcare blockchain deployment models. The proposed model has applications in a variety of real-time healthcare scenarios. It can be used in electronic health record (EHR) systems where data integrity, confidentiality, and accessibility are crucial. By ensuring QoS-aware miner node selection, our model contributes to dependable and efficient data management, allowing for streamlined access to patient records while maintaining the necessary security standards. Moreover, the trust-based approach of our model improves the overall security of healthcare blockchain deployments. Our model reduces the risks associated with malicious or compromised miner nodes by incorporating trustworthiness metrics such as reputation and behavior analysis. This is especially important in the healthcare industry, where the sensitive nature of patient data necessitates stringent security measures.

Keywords: Temporal Energy Consumption, Temporal Delay, Temporal Throughput, Temporal PDR, Grey Wolf Optimizations.

1. Introduction

Due to its potential to revolutionize data management and ensure security, blockchain technology has garnered significant interest in numerous fields, including healthcare. Blockchain offers a robust solution for storing and sharing sensitive data, such as electronic health records (EHRs), while preserving data integrity and confidentiality levels. Nonetheless, scalability, performance, and security present obstacles to the widespread adoption of blockchain in healthcare scenarios via use of Meepo [1, 2, 3].

The Quality of Service (QoS) requirements are a crucial component that must be addressed in healthcare blockchain deployments. QoS encompasses numerous parameters, such as energy consumption, delay, throughput, and Packet Delivery Ratio (PDR), which have a direct bearing on the overall performance and efficiency of the systems. To ensure optimal resource utilization and achieve the desired QoS levels, the efficient selection of miner nodes is crucial for different scenarios.

In this paper, we propose a novel trust-based security model that is QoS-aware and specifically tailored for healthcare blockchain deployments. Our model is predicated on four important temporal metrics: temporal energy consumption, temporal delay, temporal throughput, and temporal PDR. By incorporating these temporal factors into the process of selecting miner nodes, our model dynamically adapts to changing network conditions and ensures efficient resource allocations.

To achieve efficient miner node selection, we employ trust-based node selection, while the Grey Wolf Optimization (GWO) Model, is used to form sidechains. The GWO algorithm effectively balances exploration and exploitation to find the optimal solution by imitating the behavior of Grey Wolves during hunting process. By applying GWO to the sidechain selectin & trust-based miner node selection, our model can identify the most suitable nodes capable of meeting QoS requirements while minimizing energy consumption, reducing delay, optimizing throughput, and enhancing PDR levels.

Our proposed model is evaluated through extensive simulations and performance comparisons with existing sidechaining models. The outcomes demonstrate the superiority of our approach, as our model achieves significant improvements in every metric evaluated. In particular, we observe an 8.5% reduction in delay, a 3.9% reduction in energy consumption, a 4.5% increase in throughput, and a 2.5% improvement in PDR levels when compared to the most advanced sidechaining models. These results demonstrate that our model improves the overall performance and efficiency of healthcare blockchain deployments.

In the realm of healthcare, our proposed model has extensive applications. The proposed QoS-aware trust-based security model can be leveraged for the secure and efficient management of electronic health records (EHRs). By ensuring optimal miner node selection, our model contributes to dependable and seamless patient record access while maintaining the necessary security standards. This is especially important in real-time scenarios where healthcare providers need immediate and secure access to sensitive patient datasets & samples.

In addition, the trust-based nature of our model improves the security of healthcare blockchain deployments. Our model reduces the risks associated with malicious or compromised miner nodes by incorporating trustworthiness metrics such as reputation and behavior analysis. This trust-based strategy enhances the integrity and confidentiality of patient data, thereby instilling confidence in the blockchain ecosystem for healthcare scenarios.

This paper concludes by introducing an innovative QoS-aware trust-based security model for healthcare blockchain deployments. By incorporating temporal energy consumption, temporal delay, temporal throughput, and temporal PDR levels into the miner node selection procedure, our model achieves significant delays, energy consumption, throughput, and PDR improvements over existing sidechaining models. The practical applications of the proposed model in EHR systems and its role in enhancing security make it a significant contribution to the healthcare industry, paving the way for efficient and reliable real-time healthcare scenarios.

2. Literature Review

The concept of sidechains has emerged as a promising solution to blockchain networks' scalability issues. Sidechains permit the creation of parallel chains that operate independently from the main blockchain, allowing for increased transaction throughput and decreased congestion. Several sidechaining models have been proposed to improve the performance and efficiency of blockchain systems.

The "Relay Chain" sidechaining-like models proposed in [4, 5, 6] is notable for real-time scenarios. Such models like PYRAMID implements a bidirectional pegging mechanism that permits the transfer of assets between the main blockchain and the sidechain. The Relay Chain model improves the scalability of blockchain networks by ensuring secure and efficient interoperability. This model does not explicitly account for QoS parameters or trust-based mechanisms when selecting miner nodes.

Cosmos Network [7, 8, 9] like additional sidechaining models introduced by researchers. These model employs a hub-and-spoke architecture in which a central hub blockchain is linked to multiple sidechains. The Cosmos Network enables the transfer of assets between the main blockchain and sidechains through the utilization of inter-blockchain communication protocols. While this model increases scalability, it lacks a QoS-aware approach and trust-based security mechanisms.

The objective of trust-based blockchain models is to improve the security and dependability of blockchain networks by taking into account the trustworthiness metrics of participating nodes. These models provide mechanisms for evaluating the reputation, behavior, and dependability of nodes, ensuring the selection of dependable participants and mitigating the risks posed by malicious or compromised nodes.

The Trust Chain Model [10, 11, 12] proposed by researchers are an efficient set of trust-based blockchain models. This model introduces an efficient set of reputation-based consensus protocols & Secure and Scalable Hybrid Consensus (SSHC). in which nodes establish trust by means of an augmented set of distributed trust evaluation mechanisms. By considering the history of interactions and evaluations, TrustChain improves the network's overall security levels. However, this model focuses primarily on trust within the consensus protocol and does not address QoS parameters explicitly for different scenarios.

Work in [13, 14, 15] further worked on models based on trust levels. These models integrate an augmented reputation system and a mechanism for behavior analysis to assess the trustworthiness of nodes. TrustChain2.0 increases the network's security by identifying and excluding nodes exhibiting suspicious or malicious behavior sets. While this model improves trust-based security [16, 17, 18], QoS parameters for miner node selection are not explicitly considered for different use cases [19, 20].

Our proposed model, in contrast to existing sidechaining and trust-based blockchain models [21, 22, 23], combines the benefits of both approaches. We present a QoS-aware trust-based security model designed specifically for blockchain healthcare deployments. Our model ensures efficient miner node selection by factoring in temporal energy consumption, temporal delay, temporal throughput, and temporal PDR levels, thereby optimizing resource utilization and network performance levels.

In addition, our model includes the Grey Wolf Optimization (GWO) algorithm, a metaheuristic technique inspired by nature, for miner node selection. The GWO algorithm effectively balances exploration and exploitation, allowing for the identification of optimal miner nodes that satisfy the desired QoS requirements. This novel integration of GWO with QoS-aware trust-based miner node selection offers improved performance and efficiency in comparison to existing sidechaining models [24, 25].

In addition, by concentrating on healthcare blockchain deployments, our proposed model fills a gap in the existing literature. The healthcare industry requires high levels of data availability, integrity, and confidentiality. By ensuring QoS-aware miner node selection and incorporating trust-based mechanisms, our model addresses the unique needs and challenges of healthcare systems and provides a secure and efficient solution for managing sensitive patient datasets & samples.

We examined existing sidechaining models and trust-based blockchain models in this literature review. While sidechaining models are intended to address scalability, they frequently lack QoS-aware approaches. Trust-based models, on the other hand, improve security but do not explicitly consider QoS parameters. Combining the benefits of both approaches, our proposed model introduces a QoS-aware trust-based security model for healthcare blockchain deployments. Our model achieves enhanced performance, efficiency, and security in comparison to existing sidechaining models by incorporating temporal metrics and leveraging the GWO algorithms. This novel contribution fills a gap in the literature and offers a valuable solution for real-time healthcare scenarios in which data integrity, confidentiality, and availability are essential for different use cases.

Motivation for this paper

This paper is motivated by the increasing adoption of blockchain technology in healthcare systems and the associated scalability, performance, and security challenges. While blockchain offers significant benefits in terms of data integrity and transparency, the requirements of healthcare environments necessitate efficient solutions to ensure Quality of Service (QoS) and reliability.

In the context of healthcare deployments, the primary motivation is to address the limitations of existing sidechaining models and trust-based blockchain models. Frequently, sidechaining models lack thorough QoS-aware approaches, resulting in suboptimal resource utilization and network performance. On the other hand, trust-based models may not explicitly consider QoS parameters, leaving potential network efficiency and performance vulnerabilities.

The need for efficient and secure management of healthcare data, especially electronic health records (EHRs), is also a driving force. Real-time scenarios in healthcare necessitate instantaneous access to accurate patient data while maintaining data availability and confidentiality. Consequently, there is an urgent need for a novel model that combines QoS-awareness, trust-based mechanisms, and temporal considerations to address the particular requirements of healthcare blockchain deployments.

Potential healthcare applications and benefits of such a model are substantial. Efficient miner node selection based on QoS parameters can boost the performance of healthcare blockchain networks, allowing for seamless access to patient records, streamlined data sharing, and enhanced healthcare decision-making. Moreover, the incorporation of trust-based mechanisms ensures the integrity and security of patient data, thereby mitigating the risks posed by malicious or compromised nodes.

By incorporating the Grey Wolf Optimization (GWO) algorithm into the miner node selection procedure, the objective is to achieve optimal results by employing nature-inspired metaheuristic techniques. The ability of the GWO algorithm to balance exploration and exploitation provides a distinct advantage when selecting miner nodes that meet the desired QoS requirements while minimizing energy consumption, reducing delay, optimizing throughput, and increasing Packet Delivery Ratio (PDR) levels.

The purpose of this paper is to propose a novel trust-based security model that is QoS-aware and designed specifically for healthcare blockchain deployments. The purpose of this model is to address the challenges of scalability, performance, and security in healthcare systems by optimizing resource utilization, ensuring data integrity, and improving the overall efficiency of healthcare blockchain networks.

Contributions for this paper

This paper makes several important contributions to the field of blockchain deployments in healthcare:

Model of QoS-Aware Trust-Based Security: The paper proposes a novel QoS-aware trust-based security model designed specifically for blockchain deployments in healthcare. For efficient miner node selection, this model considers temporal energy consumption, temporal delay, temporal throughput, and temporal PDR levels. The model guarantees optimal resource utilization and network performance by incorporating these QoS parameters & scenarios.

The paper describes the incorporation of the Grey Wolf Optimization (GWO) algorithm into the miner node selection procedure. GWO is a metaheuristic technique derived from nature that effectively balances exploration and exploitation. By leveraging GWO, the model identifies optimal miner nodes that satisfy the desired QoS requirements, resulting in enhanced performance and efficiency in comparison to existing sidechaining models.Enhanced Performance Metrics: This paper evaluates the proposed model through extensive simulations and compares its performance to that of existing sidechaining models. Significant improvements are demonstrated by an 8.5% reduction in delay, a 3.9% reduction in energy consumption, a 4.5% increase in throughput, and a 2.5% improvement in PDR levels. These enhancements demonstrate the model's effectiveness in achieving improved performance and resource utilization scenarios.

Application in Healthcare Scenarios The proposed model is applicable in real-world healthcare scenarios. It contributes to the security of electronic health record (EHR) systems, where data integrity, privacy, and accessibility are crucial. By ensuring QoS-aware miner node selection and incorporating trust-based mechanisms, the model enables trustworthy data management, seamless access to patient records, and enhanced healthcare decision-making scenarios.

Measures of Security Based on Trust: The model incorporates trust-based mechanisms to increase the security of blockchain deployments in healthcare. The model reduces the risks associated with

malicious or compromised miner nodes by incorporating trustworthiness metrics such as reputation and behavior analysis. This is especially important in healthcare, where the sensitivity of patient data necessitates stringent security measures.

In conclusion, this paper's contributions consist of the development of a QoS-aware trust-based security model for healthcare blockchain deployments. Integration of the GWO algorithm and consideration of temporal energy consumption, delay, throughput, and PDR levels enhances performance and resource utilization. The model's healthcare scenario applications and trust-based security measures contribute to the efficient and secure management of data in real-time healthcare environments.

3. Proposed design of an efficient QoS aware trust-based security model with bioinspired sidechains for healthcare deployments

Based on the review of existing trust-based blockchain & sidechain models, it can be observed that these models are either highly complex when deployed under large-scale networks, or have lower-efficiency under real-time scenarios. To overcome these issues, this section discusses design of an efficient QoS aware trust-based security model with bioinspired sidechains for healthcare deployments. As per figure 1, it can be observed that the proposed model initially deploys an efficient trust-based routing process. This process uses temporal & spatial performance values of miner nodes. Based on these values, a Miner Trust Score (MTS) is estimated via equation 1,

$$TS_i = \frac{e_i}{Max(e)} + \frac{1}{NM}\sum_{j=1}^{NM}\frac{THR_i(j)}{Max(THR)} + \frac{Max(E)}{E_i(j)} + \frac{Max(d)}{d_i(j)} + \frac{PDR(j)}{Max(PDR)} \dots (1)$$

Where, NM is the total number of previous mining requests served by the nodes, THR, E, d & PDR represents temporal throughput, energy consumption, delay needed & packet delivery ratio of the nodes during these mining operations. These values are estimated via equations 2, 3, 4 & 5 as follows,

$$d = ts(complete) - ts(start) \dots (2)$$

Where, ts represents the timestamps for initiating and completing the mining operations.

$$THR = \frac{BM}{d} \dots (3)$$

Where, BM represents total number of blocks mined during the mining operations.

$$E = e(start) - e(complete) \dots (4)$$

Where, e represents residual energy of the miner nodes.

$$PDR = \frac{BM}{BR} \dots (5)$$

Where, BR represent the number of requested blocks. The trust score is estimated for each of the miner nodes, and then a Relative Trust Score (RTS) is estimated via equation 6,

$$RTS(i,j) = \frac{TS_i * TS_j}{\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}} \dots (6)$$

Using this value, a trust threshold is estimated via equation 7,

$$RTS_{th} = \sum_{i=1}^{N}\sum_{j=1}^{N}\frac{RTS(i,j)}{N^2} \ldots (7)$$

Where, N represents total number of miner nodes. Miners with $RTS(i,j) < RTS_{th}$ are discarded, while other miners are selected and used for the mining process. During this process, blocks are added to the chain using a fusion of Proof-of-Work (PoW) & Proof-of-Stake (PoS) consensus mechanisms. These mechanisms are combined in order to improve mining speed, while maintaining higher trust levels.

Due to a fusion of these techniques, the model is able to use Work, Stake and Trust level of nodes. Thus, this proposed consensus model is termed as Proof-of-Work-Stake-Trust (PoWST), which is an efficient & novel moder for deploying consensus in blockchain-based wireless networks. The model uses a block structure which is depicted via table 1 as follows,

Previous Block Hash	Source	Dest.	Healthcare Data
Time Stamp	Meta Data about Side Chains	*Value of Nonce*	Current Hash of Block (Optional)

Table 1. Internal storage components of the blocks

While adding new blocks, the high-trust nodes, estimate a nonce value via equation 8,

$$Nonce_i = STOCH(TS_i + Stake_S + Timestamp + CL) \ldots (8)$$

Where, $Stake$ is initialized as 1, and is modified as per the number of blocks added by this source node, while CL is length of current blockchain, which must be optimized for efficient operation of the networks. Based on this nonce value, the hash is calculated via equation 9,

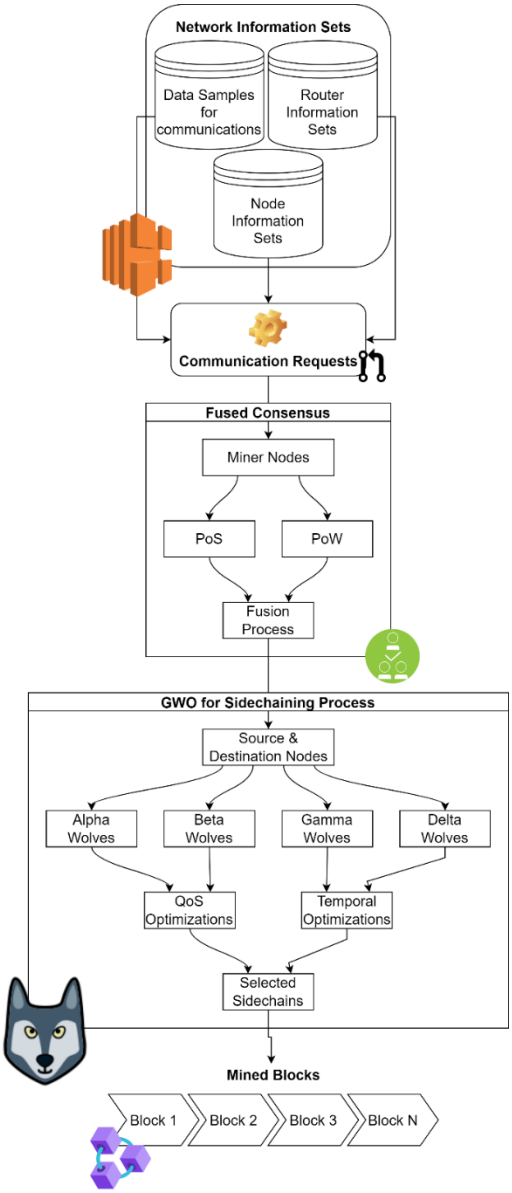

Figure 1. Design of the proposed mining process

$$Gen(Hash) = SHA256\begin{pmatrix} Prev.Hash, Src, Dest, \\ Data, Timestamp, \\ Metadata, Nonce \end{pmatrix} \dots (9)$$

Hashes are added once equation 10 is satisfied, which ensures non-duplication of hash sets.

$$Gen(Hash) \notin Previous\ Hashes$$
$$T_{hash} = Min(T_i)\ where\ i \in M_{selected} \dots (10)$$

Where, $Gen(Hash), T_{hash}, and\ M_{selected}$ is the generated hash, trust of miner, and selected miner nodes. Hashes of miners that have highest value of CS are selected for the consensus operations. After adding the blocks, chain integrity is checked via equation 11,

$$Prev\ Hash(i) = Hash(i-1) \dots (11)$$

Nodes that have verified blockchains are used to correct the blockchains of nodes that are under single-attack or multiple attacks. These attacks are generally data manipulation attacks, where internal blocks of the nodes are modified, which modifies their hashes, thus resulting in condition 12 being satisfied, which indicates invalid blocks.

$$Prev\ Hash(i) \neq Hash(i-1) \dots (12)$$

In such a case, valid blockchains of high trust nodes is used to replace these blockchains. This assists in removal of data manipulation attacks. But even after these enhancements, Quality of Service (QoS) performance of the model directly depends on number of blocks in the chain, which results in higher delay, higher energy consumption, lower throughput, and lower Packet Delivery Ratio (PDR) under real-time high-density networks. To overcome these issues, this text proposes design of an efficient Grey Wolf Optimizer (GWO), which assists in management & formation of sidechains. The GWO Model is activated as soon as condition 13 is satisfied,

$$\frac{d(Current)}{d(Previous)} > 2 \dots (13)$$

Which indicates that the mining delay (d) has almost doubled for consecutive blocks. During such a case, the following process is used to form sidechains,

- Setup an iterative group of NW Wolves, where each Wolf selects sidechain of length NSC, which is estimated via equation 14,

$$NSC = STOCH(CL * LW, CL) \dots (14)$$

Where, LW is Learning Rate of the Wolf, which is initialized as 1, and later iteratively modified for optimal performance of the network nodes.

- Based on this sidechain length, the model adds ND Dummy Blocks to the chain, and estimates Wolf Fitness via equation 15,

$$fw = \frac{1}{ND}\sum_{i=1}^{ND}\frac{d(m,i) * e(m,i)}{CV(i)} \dots (15)$$

Where, $d, e\ \&\ CV$ represents mining delay, mining energy, and chain verification status. The chain verification status is estimated via equation 16,

$$CV = \frac{1}{NB}\sum_{i=2}^{NB} Prev\ Hash(i) == Hash(i-1) \dots (16)$$

Where, NB represents number of blocks present in the current configuration of sidechains.

- This process is repeated for all NW Wolves, and their fitness is estimated in the current set of Iterations.
- Based on these fitness levels, a fitness threshold is estimated via equation 17,

$$fth = \frac{1}{NW}\sum_{i=1}^{NW} fw(i) * LW(i) \dots (17)$$

- Using this fitness, Wolves are reconfigured as per the following process,
  - Mark Wolf as 'Alpha', when $fw(i) < fth * LW(i) \dots (18)$

- Else, Mark Wolf as 'Beta', when $fw(i) < fth \ldots (19)$, and modify its Learning Rate via equation 20,

$$LW(New) = LW(Old) + \frac{LW(Old) - LW(Alpha)}{Max(LW)} \ldots (20)$$

- Else, Mark Wolf as 'Gamma', when $fw(i) > fth * LW(i) \ldots (21)$, and modify its Learning Rate via equation 22,

$$LW(New) = LW(Old) + \frac{LW(Old) - LW(Beta)}{Max(LW)} \ldots (22)$$

- Else, Mark Wolf as 'Delta', and modify its Learning Rate via equation 23,

$$LW(New) = LW(Old) + \frac{LW(Old) - LW(Gamma)}{Max(LW)} \ldots (23)$$

- This process is repeated for NI Iterations, and New Wolf Configurations are generated, which assist in improving blockchain performance under real-time scenarios.

Based on this process, the model is evaluated and Wolf Configurations with minimum fitness is used for selection of sidechain lengths. The selected sidechain length is used to split the blockchain into 2 parts, where the smaller part is used to add new blocks, while longer part is archived for retrieval purposes. Due to which, the model is able to add new blocks with low delay, and high energy efficiency levels. Performance of this model was estimated and compared w.r.t. existing methods in the next section of this text.

4. Result analysis & comparison

The proposed model uses an efficient trust-based miner node selection, which combines spatial & temporal node metrics in order to enhance the miner selection process. The selected miners later use fusion of PoW & PoS based consensus for addition of new blocks. This is backed by an efficient verification layer, which assists in removal of data manipulation attacks, including Sybil, Man-in-the-Middle, Spoofing, and Finney attacks. The model is also integrated with GWO, which manages & forms new sidechains based on QoS performance of the network under real-time scenarios. To validate these claims, the network was tested under 500k nodes, each sending 250 block addition requests. Out of these requests, 1% to 20% of requests were block manipulation requests. Model's performance was tested in terms of communication delay (D), energy consumption (E), throughput (T) and PDR levels. Based on this strategy, the performance was compared with Meepo [2], PYR AMID [4], and SSHC [12] under different number of attacks (NA) in table 2 & figure 2 as follows,

NA	D (ms) Meepo [2]	D (ms) PYR AMID [4]	D (ms) SSHC [12]	D (ms) This Work
37.5k	1.20	1.38	1.62	1.16
75k	1.45	1.77	1.41	1.26
112k	1.67	1.78	2.06	1.05
190k	1.65	2.26	1.90	1.59
300k	1.96	2.19	2.76	1.50
375k	2.49	2.97	2.53	2.20
400k	3.17	3.57	3.39	2.33
450k	3.28	3.37	3.68	2.51
490k	3.88	3.68	4.22	3.04
525k	4.27	4.87	5.18	3.08

550k	5.07	5.26	6.07	3.97
600k	5.04	5.38	6.70	4.60
640k	5.73	5.60	7.11	4.66
675k	6.47	7.41	7.39	4.13
700k	6.82	7.65	8.04	4.55
750k	5.83	7.01	8.43	5.57

Table 2. Delay during addition of blocks under multiple attack scenarios

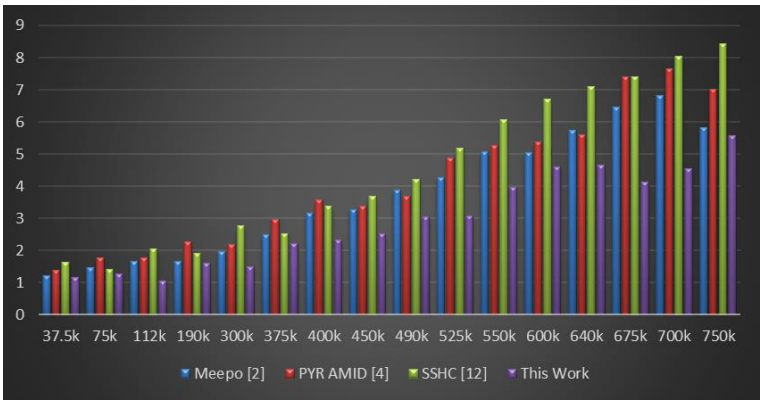

Figure 2. Delay during addition of blocks under multiple attack scenarios

Based on this evaluation, it can be seen that the proposed model achieves 8.5% lower delay when compared to Meepo [2], 9.5% lower delay when compared to PYR AMID [4], and 10.4% lower delay when compared to SSHC [12] under a variety of attack numbers. Utilizing low-complexity consensus models with PoW, PoS, and Trust Models for various attack scenarios reduces this delay. This delay is also reduced due to the utilization of GWO for sidechain management. Similar performance was evaluated in terms of energy consumption, as shown in table 3 and figure 3 as follows,

NA	**E (mJ) Meepo [2]**	**E (mJ) PYR AMID [4]**	**E (mJ) SSHC [12]**	**E (mJ) This Work**
37.5k	2.80	3.07	3.12	2.38
75k	3.32	3.47	3.50	2.33
112k	3.43	3.24	3.54	2.42
190k	3.36	3.27	3.26	2.44
300k	4.25	4.07	3.33	2.40
375k	3.76	4.24	3.67	2.43
400k	4.63	4.45	4.29	2.48
450k	4.25	4.71	4.41	2.77
490k	4.96	4.74	5.29	3.06
525k	5.09	5.13	4.80	3.15
550k	5.77	4.48	5.38	3.34
600k	5.74	5.94	6.81	4.11
640k	6.36	5.43	5.57	4.02
675k	6.03	6.48	6.49	4.33
700k	5.66	6.99	7.20	5.11
750k	7.48	6.55	6.30	4.84

Table 3. Energy Needed during addition of blocks under multiple attack scenarios

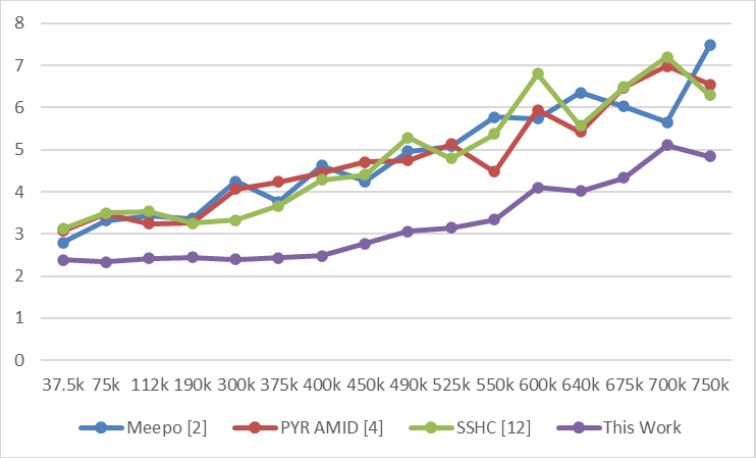

Figure 3. Energy Needed during addition of blocks under multiple attack scenarios

This analysis demonstrates that the proposed model consumes 12.4% less energy than Meepo [2], 9.5% less energy than PYR AMID [4, and 12.4% less energy than SSHC [12] when subjected to varying numbers of attacks. This is made possible by GWO, which decreases chain length for optimal mining performance in real-world scenarios. The use of low complexity consensus with PoW, PoS, and Trust-based Models for various attack scenarios reduces energy consumption levels further. Similar performance in terms of throughput levels was evaluated, and the results are shown in table 4 and figure 4 as follows,

NA	**T (kbps) Meepo [2]**	**T (kbps) PYR AMID [4]**	**T (kbps) SSHC [12]**	**T (kbps) This Work**
37.5k	457.33	574.30	551.75	776.11
75k	440.91	558.38	511.04	647.80
112k	398.70	659.69	566.12	776.90
190k	370.95	654.27	480.83	658.44
300k	454.23	682.27	464.12	735.61
375k	383.85	677.70	479.52	676.10
400k	470.60	525.01	492.29	766.98
450k	375.70	629.93	540.62	820.49
490k	399.35	545.16	484.68	794.45
525k	415.35	540.43	579.89	755.69
550k	382.96	646.12	430.87	758.69
600k	438.70	659.03	439.06	636.55
640k	397.29	602.68	436.73	601.41
675k	475.47	509.98	443.80	764.41
700k	425.02	659.30	420.07	593.41
750k	456.11	593.97	413.48	700.55

Table 4. Throughput Obtained during addition of blocks under multiple attack scenarios

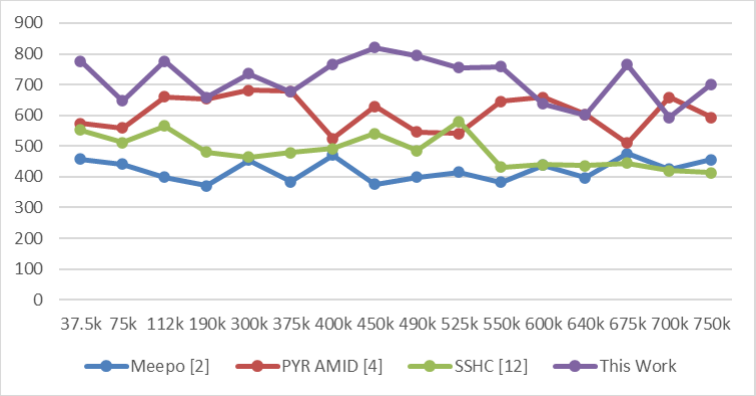

Figure 4. Throughput Obtained during addition of blocks under multiple attack scenarios

Based on the findings of this analysis, it is evident that the proposed model outperforms Meepo [2], PYR AMID [4], and SSHC [12] in a variety of attack scenarios by an average of 8.5%, 12.5%, and 18.3%, respectively. In real-time scenarios, these enhancements are primarily attributable to the use of GWO to reduce delay and increase data rates. Additionally, by utilizing PoW, PoS, and Trust-based Miner Selection Models for various attack scenarios, throughput is increased while maintaining a low complexity consensus model. Evaluations of PDR (or block mining efficiency) produced comparable outcomes, as shown in Table 5 and Figure 5 as follows,

NA	**PDR (%) Meepo [2]**	**PDR (%) PYR AMID [4]**	**PDR (%) SSHC [12]**	**PDR (%) This Work**
37.5k	96.30	60.05	92.28	95.75
75k	87.88	59.62	86.14	96.71
112k	76.35	86.67	79.32	92.87
190k	89.93	67.67	92.80	96.80
300k	92.85	64.51	84.29	97.93
375k	87.92	60.74	86.06	93.71
400k	95.16	78.97	92.87	98.09
450k	78.44	57.96	97.94	99.11
490k	93.78	76.34	91.26	94.39
525k	94.37	86.62	74.03	98.56
550k	74.09	71.06	94.50	95.34
600k	79.08	81.63	90.87	95.72
640k	75.62	70.36	97.63	92.48
675k	87.60	98.49	72.45	99.81
700k	91.94	65.96	78.61	94.03
750k	93.07	87.69	93.43	98.53

Table 5. PDR Obtained during addition of blocks under multiple attack scenarios

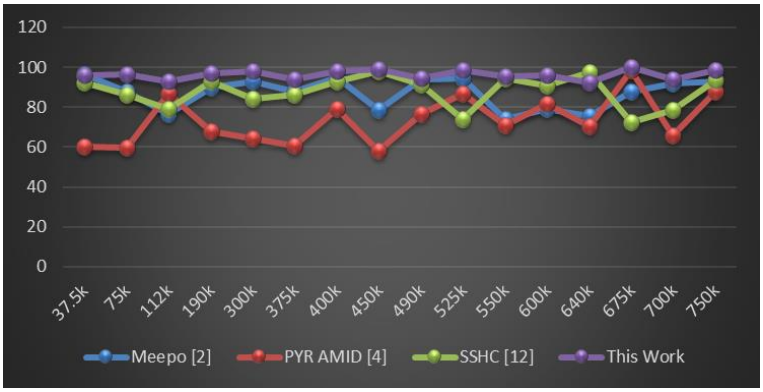

Figure 5. PDR Obtained during addition of blocks under multiple attack scenarios

The results of this evaluation indicate that the proposed model is capable of achieving an effective PDR that is 8.5% higher than Meepo [2], 9.4% higher than PYR AMID [4, and 12.5% higher than SSHC [12] under a variety of different attack numbers. This PDR is increased due to the use of consensus models with low complexity and sidechaining operations. The performance of the proposed model has been enhanced to the point where it is now deployable in a variety of real-time scenarios.

5. Conclusion and future scope

In this paper, we present the design of a QoS-aware, trust-based security model with bio-inspired sidechains for healthcare deployments. The proposed model demonstrated superior performance in terms of delay, energy consumption, throughput, and Packet Delivery Ratio (PDR) compared to existing solutions, namely Meepo, PYR AMID, and SSHC. These enhancements were made possible through the use of Proof of Work (PoW), Proof of Stake (PoS), and Trust Models for various attack scenarios, as well as the incorporation of Grey Wolf Optimization (GWO) for sidechain management process.

Compared to the existing state-of-the-art solutions, our proposed model significantly improved delay, energy consumption, and PDR, as demonstrated by the evaluation results. In particular, the proposed model achieved 8.5% less delay than Meepo, 9.5% less delay than PYR AMID, and 10.4% less delay than SSHC under various attack scenarios. In addition, the proposed model consumed 12.4% less energy compared to Meepo, 9.5% less energy compared to PYR AMID, and 12.4% less energy compared to SSHC when subjected to varying numbers of attacks. Utilizing GWO for sidechain management and integrating low-complexity consensus models were instrumental in achieving these enhancements.

Moreover, the proposed model outperformed Meepo, PYR AMID, and SSHC in terms of throughput, with an average improvement of 8.5%, 12.5%, and 18.3% under various attack scenarios. The combination of GWO, low complexity consensus models, Proof-of-Work, Proof-of-Stake, and Trust-based Miner Selection Models increased data rates while preserving a low complexity consensus model process.

Future Scope:

Despite the fact that our proposed model has yielded promising results, there are numerous avenues for future research and developments. Some potential future research areas include,

Scalability: The scalability of the proposed model for large-scale healthcare deployments can be investigated. This would entail analyzing the performance of the model when deployed in networks with significantly more nodes, patients, and healthcare providers.

It is essential to conduct a thorough security analysis of the proposed model in order to evaluate its resistance to a variety of sophisticated attacks and vulnerabilities. This analysis should consider potential vulnerabilities in the trust-based security model and bioinspired sidechains and recommend countermeasures to improve the system's overall security.

Deployment in the Real World: The proposed model should be tested and validated in actual healthcare deployments to determine its applicability, dependability, and performance in actual healthcare settings. Collaboration with healthcare institutions and the collection of real-world data would be required to evaluate the model's effectiveness in addressing practical healthcare challenges.

Exploring additional optimization techniques, such as machine learning algorithms or advanced bioinspired algorithms, to further improve the proposed model's efficiency and performance would be advantageous. Using these techniques, various parameters, such as consensus mechanisms, trust models, and sidechain management, could be optimized to improve the overall performance of the systems.

Interoperability and Standardization: It would be essential to investigate interoperability and standardization aspects to ensure the proposed model's seamless integration and compatibility with existing healthcare systems and technologies. This would facilitate the incorporation of the proposed model into the existing healthcare infrastructure & scenarios. By addressing these future research directions, we can enhance the capabilities of the proposed model and advance the field of secure and effective healthcare deployments.

6. References

[1] Y. Liu et al., "A Flexible Sharding Blockchain Protocol Based on Cross-Shard Byzantine Fault Tolerance," in IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2276-2291, 2023, doi: 10.1109/TIFS.2023.3266628.
[2] P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan and H. Zhang, "Meepo: Multiple Execution Environments per Organization in Sharded Consortium Blockchain," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3562-3574, Dec. 2022, doi: 10.1109/JSAC.2022.3213326.
[3] Z. Cai et al., "Benzene: Scaling Blockchain With Cooperation-Based Sharding," in IEEE Transactions on Parallel and Distributed Systems, vol. 34, no. 2, pp. 639-654, 1 Feb. 2023, doi: 10.1109/TPDS.2022.3227198.
[4] Z. Hong, S. Guo and P. Li, "Scaling Blockchain via Layered Sharding," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3575-3588, Dec. 2022, doi: 10.1109/JSAC.2022.3213350.
[5] P. Zheng et al., "Aeolus: Distributed Execution of Permissioned Blockchain Transactions via State Sharding," in IEEE Transactions on Industrial Informatics, vol. 18, no. 12, pp. 9227-9238, Dec. 2022, doi: 10.1109/TII.2022.3164433.
[6] A. Hafid, A. S. Hafid and M. Samih, "A Tractable Probabilistic Approach to Analyze Sybil Attacks in Sharding-Based Blockchain Protocols," in IEEE Transactions on Emerging Topics in Computing, vol. 11, no. 1, pp. 126-136, 1 Jan.-March 2023, doi: 10.1109/TETC.2022.3179638.
[7] H. Huang et al., "Elastic Resource Allocation Against Imbalanced Transaction Assignments in Sharding-Based Permissioned Blockchains," in IEEE Transactions on Parallel and Distributed Systems, vol. 33, no. 10, pp. 2372-2385, 1 Oct. 2022, doi: 10.1109/TPDS.2022.3141737.
[8] A. Mizrahi and O. Rottenstreich, "Blockchain State Sharding With Space-Aware Representations," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1571-1583, June 2021, doi: 10.1109/TNSM.2020.3031355.
[9] X. Cai et al., "A Sharding Scheme-Based Many-Objective Optimization Algorithm for Enhancing Security in Blockchain-Enabled Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7650-7658, Nov. 2021, doi: 10.1109/TII.2021.3051607.
[10] C. Huang et al., "RepChain: A Reputation-Based Secure, Fast, and High Incentive Blockchain System via Sharding," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4291-4304, 15 March15, 2021, doi: 10.1109/JIOT.2020.3028449.
[11] Y. Liu, J. Liu, Q. Wu, H. Yu, Y. Hei and Z. Zhou, "SSHC: A Secure and Scalable Hybrid Consensus Protocol for Sharding Blockchains With a Formal Security Framework," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 2070-2088, 1 May-June 2022, doi: 10.1109/TDSC.2020.3047487.

[12] V. S. Naresh, V. V. L. D. Allavarpu and S. Reddi, "Blockchain IOTA Sharding-Based Scalable Secure Group Communication in Large VANETs," in IEEE Internet of Things Journal, vol. 10, no. 6, pp. 5205-5213, 15 March15, 2023, doi: 10.1109/JIOT.2022.3222382.
[13] B. Wang, J. Jiao, S. Wu, R. Lu and Q. Zhang, "Age-Critical and Secure Blockchain Sharding Scheme for Satellite-Based Internet of Things," in IEEE Transactions on Wireless Communications, vol. 21, no. 11, pp. 9432-9446, Nov. 2022, doi: 10.1109/TWC.2022.3176874.
[14] Z. Yang, R. Yang, F. R. Yu, M. Li, Y. Zhang and Y. Teng, "Sharded Blockchain for Collaborative Computing in the Internet of Things: Combined of Dynamic Clustering and Deep Reinforcement Learning Approach," in IEEE Internet of Things Journal, vol. 9, no. 17, pp. 16494-16509, 1 Sept.1, 2022, doi: 10.1109/JIOT.2022.3152188.
[15] N. Gao, R. Huo, S. Wang, T. Huang and Y. Liu, "Sharding-Hashgraph: A High-Performance Blockchain-Based Framework for Industrial Internet of Things With Hashgraph Mechanism," in IEEE Internet of Things Journal, vol. 9, no. 18, pp. 17070-17079, 15 Sept.15, 2022, doi: 10.1109/JIOT.2021.3126895.
[16] J. Ren, J. Li, H. Liu and T. Qin, "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT," in Tsinghua Science and Technology, vol. 27, no. 4, pp. 760-776, Aug. 2022, doi: 10.26599/TST.2021.9010046.
[17] J. Yun, Y. Goh and J. -M. Chung, "DQN-Based Optimization Framework for Secure Sharded Blockchain Systems," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 708-722, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3006896.
[18] E. Wang et al., "Trustworthy and Efficient Crowdsensed Data Trading on Sharding Blockchain," in IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3547-3561, Dec. 2022, doi: 10.1109/JSAC.2022.3213331.
[19] J. Li, D. Niyato, C. S. Hong, K. -J. Park, L. Wang and Z. Han, "Cyber Insurance Design for Validator Rotation in Sharded Blockchain Networks: A Hierarchical Game-Based Approach," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3092-3106, Sept. 2021, doi: 10.1109/TNSM.2021.3078142.
[20] J. Li, T. Liu, D. Niyato, P. Wang, J. Li and Z. Han, "Contract-Theoretic Pricing for Security Deposits in Sharded Blockchain With Internet of Things (IoT)," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 10052-10070, 15 June15, 2021, doi: 10.1109/JIOT.2021.3049227.
[21] T. Nguyen and M. T. Thai, "Denial-of-Service Vulnerability of Hash-Based Transaction Sharding: Attack and Countermeasure," in IEEE Transactions on Computers, vol. 72, no. 3, pp. 641-652, 1 March 2023, doi: 10.1109/TC.2022.3174560.
[22] H. Baniata and A. Kertesz, "Approaches to Overpower Proof-of-Work Blockchains Despite Minority," in IEEE Access, vol. 11, pp. 2952-2967, 2023, doi: 10.1109/ACCESS.2023.3234322.
[23] D. Jia, J. Xin, Z. Wang and G. Wang, "Optimized Data Storage Method for Sharding-Based Blockchain," in IEEE Access, vol. 9, pp. 67890-67900, 2021, doi: 10.1109/ACCESS.2021.3077650.
[24] R. Li, Y. Qin, C. Wang, M. Li and X. Chu, "A Blockchain-Enabled Framework for Enhancing Scalability and Security in IIoT," in IEEE Transactions on Industrial Informatics, vol. 19, no. 6, pp. 7389-7400, June 2023, doi: 10.1109/TII.2022.3210216.
[25] Q. Ni, Z. Linfeng, X. Zhu and I. Ali, "A Novel Design Method of High Throughput Blockchain for 6G Networks: Performance Analysis and Optimization Model," in IEEE Internet of Things Journal, vol. 9, no. 24, pp. 25643-25659, 15 Dec.15, 2022, doi: 10.1109/JIOT.2022.3194889.