LCMQSINABM: Design of a Low-Power Hybrid Consensus Method for QoS-aware Sidechain-Based IoT Networks via Augmented Bioinspired Computing Models

***Shital Agrawal*[1] *and Shailesh Kumar*[2]**

[1]PhD. Research Scholar, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan, INDIA, Email: shitalagrawal2022@outlook.com

[2]Research Guide, Associate Professor, SVCET, Chittoor, INDIA

Received 24 March, 2022; Revised 7 July, 2022; Accepted 7 July, 2022

Available online 7 July, 2022 at www.atlas-tjes.org, doi: 10.22545/2022/00189

Security is one of the primary issues in any wireless network deployment, because, wireless nodes are susceptible to a wide-variety of internal and external attacks. These include improper authentication and access control, distributed denial of service (DDoS), sybil, spoofing, spying, masquerading, etc. Securing networks against these attacks requires an immutable, transparent, traceable, and distributed computing security model, that has minimum overheads. Most of these characteristics are fulfilled via the use of blockchains, which assist in the low-complexity deployment of security and hashing models. But the delay needed to scale these blockchains increases exponentially w.r.t. chain length, due to which researchers split the main blockchain into multiple sidechains. A wide variety of models are proposed by researchers for sidechain formation, and most of them are consensus dependent, which limits the scalability. Moreover, the energy needed to mine blocks for these sidechains depends directly on the consensus model, encryption model, hash rules, and length of the blockchain. Thus, models proposed for sidechain formation are context-specific and have limited scalability performance when used for multiple blockchain types. To overcome these limitations, and maintain high security performance, this text proposes the design of a Low-power hybrid Consensus Method for QoS-aware Sidechain-based IoT Networks via Augmented Bioinspired computing Models. This method uses a combination of Proof-of-Work (PoW), Proof-of-Stake (PoS) and Proof-of-Authority (PoA) based consensus models, which assist in reducing its mining delay. The PoW model allows the selection of nodes with higher performance, PoS allows the selection of nodes with a higher stake, and PoA ensures better control of IoT devices. Selection of these consensus models is done via the use of an Improved Genetic Algorithm (IGA) model, that evaluates the power needed for mining, and minimizes it using a rule-based method. This is combined with a sidechain creation model, that assists in improving QoS performance via dynamically splitting the main blockchain into performance-specific sidechains. These sidechains are categorized into low-power, low-delay, and high-throughput sidechains, which are formed via Elephant Herding Optimization (EHO) model. Due to the combination of IGA for

consensus selection, and EHO for sidechain creation, the proposed model is able to reduce the energy needed for mining by 15.4% when compared with various state-of-the-art models. It is also able to improve mining speed by 5.3%, while maintaining high security performance under different IoT Network attacks. Due to this performance enhancement, the proposed model is capable of being deployed for a wide variety of low-delay healthcare IoT, high-throughput industrial IoT, and low energy home IoT application deployments.

Keywords: IoT, security, QoS, IGA, EHO, mining, sidechain, PoS, PoW, PoA, attacks, delay, energy, consensus.

1 Introduction

Modeling low power, and high security IoT deployments is a multidomain task that involves consensus selection, miner resource optimization, selection of mining strategy, selection of block structure, etc. A typical PoWbased consensus model for blockchain mining is depicted in Figure 1, wherein PoW puzzles are defined and solved via different high-capacity miner nodes [1].

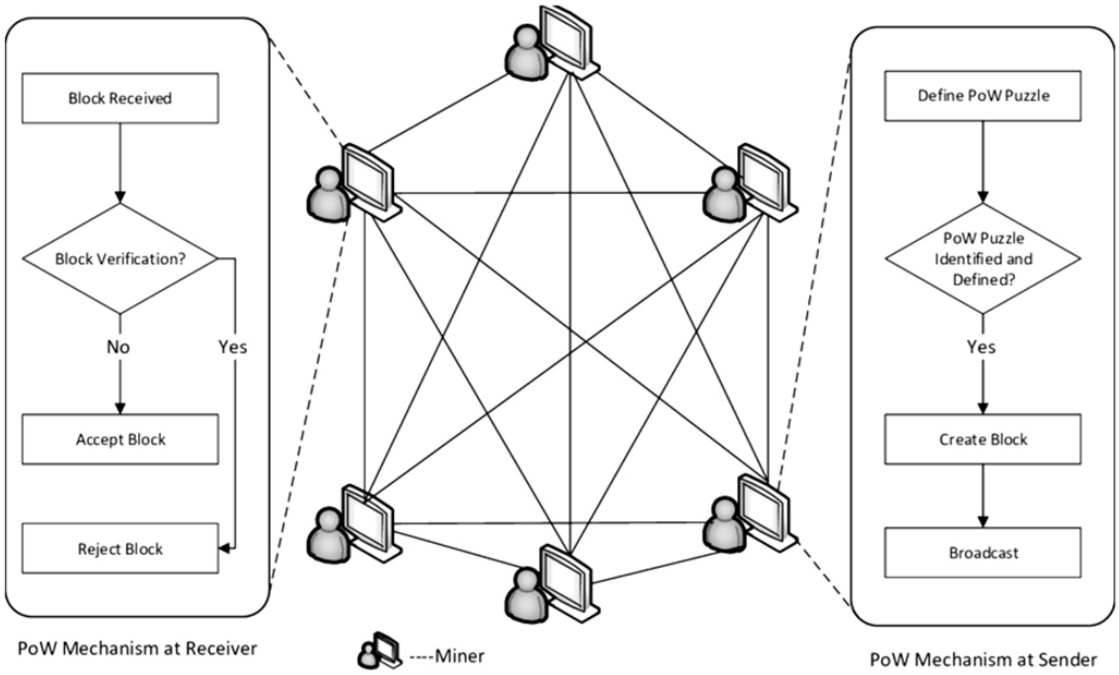

Figure 1: *A typical PoW consensus model for blockchain mining.*

These solutions are broadcasted onto the network, and are selected based on length of resulting blockchains. This process allows the model to improve verification capability for blocks, by accepting the block only when more than 51% of nodes agree upon the broadcasted solutions. The delay needed to add a block (a.k.a. mine a block) to PoW powered blockchain is calculated via equation 1 as follows,

$$D(M) = L_B * D(R) + L_B * D(V) + (L_B - 1) * D(H) + D(W)... \quad (1)$$

Where, D(M), D(R), D(V), D(H), and D(W) represents delays needed for mining, reading, verification, hashing and writing a block to the blockchain, while L_B represents length of the blockchain. Based on this

equation, it can be observed that the delay needed for mining exponentially increases w.r.t. length of the chain, thus making PoW impractical for large-length blockchains that are needed for real-time IoT network deployments. To overcome this issue, and design a highly useful IoT deployable model, a wide variety of consensus and sidechaining models are proposed by researchers [2, 3, 4]. These models are discussed in the next section of this text, wherein their nuances, advantages, limitations, and future research scopes are reviewed and compared. Based on this discussion, it can be observed that very few of these models have low-power capabilities, while even fewer of them propose the development of dynamic context-aware sidechains. To overcome these limitations, section 3 proposes the design of LCMQSINABM, which is a Low-power hybrid Consensus Method for QoS-aware Sidechain-based IoT Networks via Augmented Bioinspired Computing Models. The performance of this model is compared in section 3, wherein end-to-end delay, energy consumption, and throughput are evaluated for different state-of-the-art consensus and sidechaining methods. Finally, this text concludes with some interesting observations about the proposed model and recommends various methods to further improve its performance.

2 Material and Methods

2.1 Literature Review

A wide variety of blockchain based IoT models are proposed by researchers. For instance, work in [5, 6] proposes Blockchain Based Hierarchical Tree Layered Fog-IoT (BFIM), and fuzzy hashes for enhancing blockchain security. But these models are highly context-sensitive and cannot be scaled. Thus, work in [7] proposes a Dynamic Device Management framework for Application-Oriented Block Generation under Consortium Blockchain-Based IoT Systems. This model is highly scalable and has better performance for a wide variety of IoT network deployments. Similar models are proposed in [8, 9, 10], wherein researchers have used Blockchain-Based Access Control for IoT (BorderChain), Optimized Blockchain based Software Defined Network Framework (Smart Block SDN), and blockchain based Market for IoT Network models. These models define application specific frameworks for blockchain deployments, and thus are highly effective under specialized network conditions. Extended models that use Lagrange Coded Private Blockchain (LCPB) [11], Q-Learning for blockchain optimization (QL) [12], resource allocation via Reinforcement Learning model (RL) [13], blockchain Gateways for resource constrained applications [14], and mobile edge computing-based blockchains [15], which allow the blockchain models to extend their general-purpose performance under different scenarios.

Privacy models for better applicability of IoT devices are proposed in [16, 17, 18], wherein Privacy-Preserving and Secure Framework (PPSF), Ethereum based blockchain, and double layered blockchain for access control (DLBAC) are discussed by researchers. These models assist in improving mining efficiency via use of augmented blockchain structures. Extensions to these models are presented in [19, 20, 21], wherein security, privacy, access control, IoT fault detection via Machine Learning, and Trusted Data Sharing with Privacy Protection are proposed by researchers. These models must be extended via the work in [22, 23, 24, 25], wherein use of Artificial Intelligence (AI), trust-based models, transaction prediction, and smart grid-based access control management models are discussed. MIMO based antenna models are discussed in [26, 27, 28] and [29, 30, 31], wherein researchers have proposed the use of Microstrip Antenna Arrays, Substrate Integrated Waveguides, Low-Noise Stable Broadband Microwave Amplifiers, Magnetically Scannable Slotted Waveguide Antennas, Leaky Wave Antennas, and Anisotropic and di electric antennas which can be used for improving communication performance for real-time radios under different network conditions. These models assist in improving miner performance via integrating multiple optimization techniques while maintaining low complexity of processing and consensus. But very few of these models assist in the design of QoS-aware methods that can be used with high security, which limits their performance. To overcome this limitation, the next section proposes the design of a Low-power hybrid Consensus Method for QoS-aware Sidechain-based IoT Networks via Augmented Bioinspired Computing Models. The performance of this model is evaluated in terms of various QoS metrics, and compared with various state-of-the-art models under different communication scenarios.

2.2 Design of the proposed Low-power hybrid Consensus Method for QoS-aware Sidechain-based IoT Networks via Augmented Bioinspired computing Models

From the literature review, it was observed that a very few models were available for low-energy, and high-security QoS-aware IoT Network deployments. Thus, to overcome this issue, a novel Low-power hybrid Consensus Method for QoS-aware Sidechain-based IoT Networks via Augmented Bioinspired computing Models is proposed in this section. The proposed model initially uses a consensus selection method via the Improved Genetic Algorithm (IGA), which assists in selecting between PoW, PoS and PoA consensus models. This selection is done based on user requests, and considering the delay needed for mining blocks for the current blockchain configuration. The IGA model is extended via EHO, which is used for the creation of sidechains for application-specific requirements. The overall flow of this model is depicted in Figure 2, wherein both IGA and EHO can be observed to be working in tandem to continuously optimize the security and QoS performance of the IoT blockchain network.

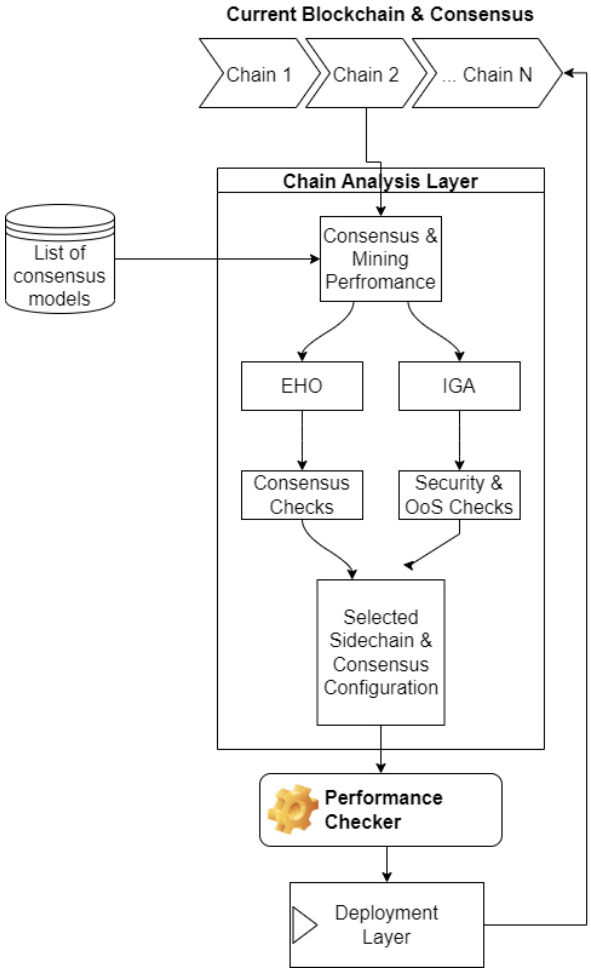

Figure 2: *Overall flow of the proposed model.*

From the flow, it can be observed that the model initially analyzes current blockchain, and its consensus parameters. These parameters are evaluated via EHO and IGA models, which assist in the selection of consensus models, QoS metrics, and security performance via efficiently creating sidechains. The selected consensus method along with sidechain configuration is given to a performance checker model, which assists in the final deployment of blockchains in the IoT network.

To simplify the design process, the model is segregated into different subparts, and each of these parts is discussed in different sub-sections of this text.

2.3 Design of the IGA Model for selection of QoS-aware consensus method

Consensus models allow blockchain networks to decide whether a block should be added to the blockchain or not. To perform this decision, a wide variety of consensus mechanisms are proposed by researchers, and it was observed that PoS, PoW and PoA models have better performance than others. The proposed model is able to reduce the delay needed for consensus by selecting most suitable consensus parameters. These parameters include a nonce range for PoW, stake needed for consensus in PoS, and access levels in PoA, in order to achieve faster consensus. To perform this task, the following IGA process model is used,

- Initialize IGA parameters,
  - Number of iterations (N_i)
  - Number of solutions (N_s)
  - Learning rate (L_r)
  - Estimated number of blocks to be added in this chain (B_{added})
- Initially mark all chains as 'to be modified'
- For each iteration in 1 to N_i
  - For each solution in 1 to N_s
    - If this solution is marked as 'not to be modified', then go to the next solution.
    - Else, generate a new solution via the following process,
      - Evaluate a minimum and maximum value of nonce range via equation 2

$$Min(nonce)=STOCH(1,Max(Int)),$$
$$Max(nonce)=STOCH(Min(nonce),Max(Int))\ldots(2)$$

Where, *STOCH,Max(Int)* represents a stochastic Markovian process, and maximum value of Integer range respectively.

- Evaluate maximum stake levels needed to add these blocks via equation 3,

$$Max(Stake)=60 * L\_r\ldots(3)$$

- Evaluate maximum authority levels which must be granted to these blocks via equation 4,

$$Max(Auth)=L\_r*L(Auth)\ldots(4)$$

Where, *L(Auth)* represents total authority levels available in the IoT deployment. These levels include read authority, write authority, modify authority, etc.

- Identify L_r*B_{added} number of nodes from the list of nodes, and start addition of blocks to the blockchain
- Use the nonce range, stake level, and authorization levels from equations 2, 3, and 4; and mine B_{added} blocks.

- Calculate the delay needed to mine these blocks via equation 1, and evaluate solution fitness via equation 5 as follows,

$$f_i = \sum_{j=1}^{Badded} \frac{D(M)_j}{B_{added}} \dots \tag{5}$$

- Evaluate fitness for each solution, and then calculate fitness threshold via equation 6 as follows,

$$f_{th} = \sum_{i=1}^{N_s} f_i * \frac{L_r}{N_s} \dots \tag{6}$$

- Solutions that have fitness more than f_{th} are marked as 'to be modified', because their mining delay is higher than others, while remaining solutions are marked as 'not to be modified'
- Based on the fitness values of solutions which are marked as 'to be modified', evaluate new learning rate via equation 7,

$$New(L_r) = L_r * \left[1 + \frac{(M(S) - NM(S)}{Max(M(S), NM(S))}\right] \tag{7}$$

  Where, $M(S)$ and $NM(S)$ represents the number of solutions which are marked as 'to be modified', and the number of solutions which are marked as 'not to be modified'

Based on this new value of L_r, values of stake, authority, and a number of nodes are modified in each iteration. At the end of the last iteration, identify the solution with minimum fitness, and use its parameters for consensus.

Based on this process, ranges for the nonce, maximum stake, and maximum authority levels are decided. These ranges are used for mining newer blocks, which assists in the continuous optimization of consensus delays. For any new requests, these ranges are used, and blocks are added to the blockchain. While adding new blocks, an EHO model is activated, which assists in the creation of security and QoS-aware sidechains for underlying IoT network deployment. The design of this model is discussed in the next sub-section of this text.

2.4 Design of the EHO Model for Creation of Security and QoS-aware Sidechains

The EHO model assists in dividing the current blockchain into sidechains, which are used for QoS and security-aware operations. This model works on a split and merge process, which assists in either dividing the current blockchain into different parts or merging the current sidechain with central blockchain. This model is activated as soon as a pre-set number of blocks are added to the blockchain. This pre-set number is evaluated via equation 8 as follows,

$$N(Blocks)^{EHO} = \sum_{i=1}^{N_{sc}} \frac{L_i}{N_{sc}} \dots \tag{8}$$

Where, N_{sc}, and L_i represent a current number of sidechains, and the length of each sidechain respectively. The EHO model works via the following process,

- Initialize parameters of EHO model,
  - Total EHO iterations (N_i^{EHO})
  - Total EHO herds (N_h^{EHO})

  - Learning rate of the EHO model (L_r^{EHO})

- To start with, mark all herds as 'to be changed'
- For every EHO iteration in 1 to N_i^{EHO}
  - For every EHO herd in 1 to N_h^{EHO}
    - Check if this herd needs to be changed, if not, then go to the next herd.
    - Else, Change this herd's internal parameters via the following process,
      + Stochastically select a chain from current list of sidechains, and initiate stochastic requests for adding blocks to this chain.
      + Divide these requests into malicious and normal requests, and evaluate delay needed to add a block to the chain under normal and malicious requests via equations 9 and 10 as follows,

$$D(Malicious) = \frac{\sum_{j=1}^{M_{requests}} t_{end_j} - t_{strat_j}}{M_{requests}} \tag{9}$$

$$D(Normal) = \frac{\sum_{j=1}^{N_{requests}} t_{end_j} - t_{strat_j}}{N_{requests}} \tag{10}$$

$$E(Malicious) = \frac{\sum_{i=1}^{M_{requests}} E_{start_i} - E_{end_i}}{M_{requests}} \tag{11}$$

$$E(Normal) = \frac{\sum_{i=1}^{N_{requests}} E_{start_i} - E_{end_i}}{N_{requests}} \tag{12}$$

Where E_{start} and E_{end} represent mining start and completion energy levels in the mining nodes. Similarly, evaluate throughput and packet delivery ratio (PDR) during mining via equations 13 to 16 as follows,

$$T(Malicious) = \sum_{j=1}^{M_{requests}} \frac{R_x(P)_i}{D(M) * M_{requests}} \tag{13}$$

$$T(Normal) = \sum_{i=1}^{N_{requests}} \frac{R_x(P)_i}{D(N) * N_{requests}} \tag{14}$$

$$PDR(Malicious) = \sum_{i=1}^{M_{requests}} \frac{R_x(P)_i}{M_{requests} * Tx(P)_i} \tag{15}$$

$$PDR(Normal) = \sum_{i=1}^{N_{requests}} \frac{R_x(P)_i}{Tx(P)_i * N_{requests}} \tag{16}$$

Where, $Tx(P)$ and $Rx(P)$ represents total number of packets transmitted and received during the mining process. These metrics are combined to form an approximate security level for the current herd via equation 17 as follows,

$$SL_i = \frac{\frac{D(Normal)}{D(Malicious)} + \frac{E(Normal)}{E(Malicious)} + \frac{T(Malicious)}{T(Normal)} + \frac{PDR(Malicious)}{PDR(Normal)}}{4} \tag{17}$$

Using these metrics, a herd fitness value is evaluated via equation 18 as follows,

$$\begin{aligned} f_h^{EHO} &= \frac{\left[\sum_{i=1}^{N_S} SL_i - \sum_{j=1}^{N_S} \frac{SL_i}{N_{stoch}}\right]}{N_S} * \\ &[\frac{D(Normal) - D(Malicious)}{D(M)} + \frac{E(Normal) - E(Malicious)}{E(M)} \\ &+ \frac{T(Malicious) - T(Normal))}{T(Normal)} + \frac{PDR(Malicious) - PDR(Normal)}{PDR(Normal)}] \end{aligned} \tag{18}$$

Based on this evaluation for each herd, a herd-level fitness threshold is evaluated via equation 19 as follows,

$$f_{th} = \frac{1}{N_h} * \sum_{i=1}^{N_h} f_{h_i} * L_r \tag{19}$$

Each herd fitness is checked, and compared with f_{th}, and herds with fitness more than threshold are marked as 'to be changed', while others are marked as 'not to be changed'.

The 'Matriarch' herd is identified as the herd with minimum fitness, which assists in continuously updating EHO learning rate via equation 20 as follows,

$$New(L_r^{EHO}) = Min\left(\bigcup_{i=1}^{N_h^{EHO}} f_{h_i}^{EHO}\right) * \frac{old(L_r^{EHO})}{\sum_{i=1}^{N_h^{EHO}} f_{h_i}^{EHO}} \tag{20}$$

After completion ofN_i^{EHO} iterations, the herd with minimum fitness is selected as the 'Matriarch' herd, and its QoS and security levels are compared with the current blockchain's performance metrics. This comparison can be observed from Table 1, where C_B and M^{EHO} represents current blockchain's levels and EHO Matriarch levels respectively.

Table 1: Rules to create new sidechains or merge with existing central blockchain.

QoS Levels	SL Value	Merge and Split decision
$C_B(QoS) > M^{EHO}(QoS)$	$C_B(SL) = M^{EHO}(SL)$	Perform blockchain merge operations
$C_B(QoS) = M^{EHO}(QoS)$	$C_B(SL) = M^{EHO}(SL)$	No change in blockchain
$C_B(QoS) < M^{EHO}(QoS)$	$C_B(SL) = M^{EHO}(SL)$	Perform blockchain split operation
$C_B(QoS) > M^{EHO}(QoS)$	$C_B(SL) > M^{EHO}(SL)$	Perform blockchain merge operations
$C_B(QoS) = M^{EHO}(QoS)$	$C_B(SL) > M^{EHO}(SL)$	Perform blockchain merge operations
$C_B(QoS) < M^{EHO}(QoS)$	$C_B(SL) > M^{EHO}(SL)$	Perform blockchain split operation
$C_B(QoS) > M^{EHO}(QoS)$	$C_B(SL) < M^{EHO}(SL)$	Perform blockchain split operation
$C_B(QoS) = M^{EHO}(QoS)$	$C_B(SL) < M^{EHO}(SL)$	Perform blockchain split operation
$C_B(QoS) < M^{EHO}(QoS)$	$C_B(SL) < M^{EHO}(SL)$	Perform blockchain split operation

To perform blockchain splits, the following process is used,

- Divide the current blockchain into 2 equal parts and evaluate SL for both of these parts.
- Based on this evaluation, evaluate the selection ratio via equation 21,

$$S(Ratio) = \frac{SL_{part_2}}{SL_{part_1}} \tag{21}$$

  Where, SL_{part_1} and SL_{part_2} represents levels of security for part 1 and part 2 of the blockchain respectively.
- If S(Ratio)>1, then chain 1 is selected as the main blockchain, else chain 2 is used as main blockchain, and new blocks are added to the selected chains.

To perform blockchain merging identify sidechain with $SL \approx 1$, and use it to merge the current blockchain. Using these decisions, blockchains are either split or merged with other chains. The performance of this model is evaluated in terms of delay, energy consumption, throughput and PDR; and is compared with various state-of-the-art methods. This performance is discussed in the next section of this text.

3 Result Analysis and Comparison

The proposed LCMQSINABM model uses a combination of QoS and security-aware models in order to improve consensus performance under various scenarios. Apart from this, the model is capable of improving security performance via the use of sidechain-based IoT Network deployments. To evaluate the performance of the proposed model, its QoS metrics are compared with QL [12], RL [13], and DL BAC [18]. These IoT networks use blockchain and other related technologies to improve the security and QoS performance of the underlying network. All these models were tested via the following standard IoT Network parameters (see Table 2).

Based on IoT and nodes configuration, a number of nodes varied between 500 to 5000, and their average QoS performance was evaluated for a different number of communications. This assists in evaluating its QoS performance. To identify its security performance, attacking nodes were varied between50 to 500 for worm hole (WH), man in the middle (MITM) and distributed denial of service (DDoS)attacks. During attacks, average of QoS metrics including end-to-end communication delay (D), energy consumption (E), delay jitter (JD), packet delivery ratio (PDR) and throughput (T) were evaluated.

Initially, the network's QoS performance was evaluated without any attacks, and compared with QL [12], RL [13], and DL BAC [18] models. This performance was estimated by varying number of nodes between 500 to 5000; and evaluating QoS metrics for different number of communications (NC). As per this evaluation strategy, values for end-to-end delay (D) for different models is tabulated in Table 3.

Based on the average end to end delay performance, it can be observed that the proposed model is 9.5% faster than QL [12], 15.4% faster than RL [13], and 18.3% faster than DL BAC [18] for different number of blockchain communication requests. This is due to the inclusion of delay while selection of miner nodes and selection of consensus models. Similar observations are done for energy requirements, and can be observed in Table 4.

Based on the average energy consumption performance, it can be observed that the proposed model needs8.3% lower energy than QL [12], 25.6% lower energy than RL [13], and 10.5% lower energy than DL BAC [18] for the different number of blockchain communication requests. This is due to the inclusion of energy levels while selecting of miner nodes and the selection of consensus models. Similar observations are done for throughput achieved during the mining process and can be observed in Table 5.

Based on the average throughput performance, it can be observed that the proposed model is able to achieve16.8% higher throughput than QL [12], 15.4% higher throughput than RL [13], and 0.5% higher throughput than DL BAC [18] for different number of blockchain communication requests. This is due

to inclusion of throughput while selection of miner nodes and selection of consensus models. Similar observations are done for packet delivery ratio during mining process, and can be observed in Table 6.

Based on the average packet delivery ratio performance, it can be observed that the proposed model is able to achieve 6.5% better PDR than QL [12], 6.75% better PDR than RL [13], and 5.4% better PDR than DL BAC [18] for a different number of blockchain communication requests. This is due to the inclusion of PDR while selecting of miner nodes and the selection of consensus models. These evaluations are extended for a different number of attacks in the network, and are estimated by a varying number of attacker (NA) nodes between 50 to 500; and estimating the QoS values. As per this evaluation strategy, values for end-to-end delay (D) for different protocols under WH, DDoS, and MiTM is tabulated in Table 7.

Based on the average end-to-end delay performance, it can be observed that the proposed model is able to achieve 10.5% faster performance than QL [12], 15.4% faster performance than RL [13], and 14.1% faster performance than DL BAC [18] for a different number of blockchain attack requests. This is because the underlying model uses security levels during the selection of blockchain split and merge processes. Similar observations are done for energy performance, this can be observed for WH, DDoS and MiTM attacks in Table 8.

Based on the average energy consumption performance, it can be observed that the proposed model is able to achieve 9.4% lower energy consumption than QL [12], 18.2% lower energy consumption than RL [13], and 18.1% lower energy consumption than DL BAC [18] for the different number of blockchain attack requests. This is because the underlying model uses security levels during the selection of blockchain split and merge processes. Similar observations are done for throughput performance, this performance is averaged for DDoS, MITM and WH attacks; and can be observed in Table 9.

Based on the average throughput performance, it can be observed that the proposed model is able to achieve 20.5% better throughput than QL [12], 20.8% better throughput than RL [13], and 25.4% better throughput than DL BAC [18] for the different number of blockchain attack requests. This is because the underlying model uses security levels during the selection of blockchain split and merge processes. Similar observations are done for packet delivery rate (PDR) performance, this performance is averaged between MITM, DDoS and WH attacks; and can be observed in Table 10.

Based on the average packet delivery ratio performance, it can be observed that the proposed model is able to achieve 29.6% better PDR than QL [12], 32.5% better PDR than RL [13], and 26.1% better PDR than DL BAC [18] for the different number of blockchain attack requests. This is because the underlying model uses security levels during selection of blockchain split and merge processes. Thus, the proposed model is able to improve QoS performance even under different attack types, thus making it useful for a wide variety of IoT deployments.

4 Discussion and Conclusion

The proposed model initially combines different consensus models via IGA process, and also uses an integrated EHO model for improvement of sidechain selection capabilities. Due to this, the proposed model is able to outperform various state-of-the-art methods in terms of QoS metrics when compared under different attack and non-attack scenarios. Upon evaluating the performance of the proposed model, it was observed that it is 9.5% faster than QL [12], 15.4% faster than RL [13], and 18.3% faster than DL BAC [18] for a different number of blockchain communication requests, while, requiring 8.3% lower energy than QL [12], 25.6% lower energy than RL [13], and 10.5% lower energy than DL BAC [18], thus making it highly useful for low-delay and low-energy IoT deployments. Similar performance was observed for PDR and throughput performance under different communication scenarios. The model was also tested under different types of attacks, and it was observed that the proposed model is able to achieve 10.5% faster performance than QL [12], 15.4% faster performance than RL [13], and 14.1% faster performance than DL BAC [18] for a different number of blockchain attack requests, while, it was able to achieve 20.5% better throughput than QL [12], 20.8% better throughput than RL [13], and 25.4% better throughput than DL BAC [18] for similar attack requests. Due to such a high-QoS and high-security performance, the proposed

model is capable of being deployed for a wide variety of IoT networks. In the future, the performance of this model must be validated under larger IoT networks, with a greater number of attacks. Furthermore, bioinspired models must be replaced with deep learning models for further improving selection capabilities under different network scenarios.

Table 2: Configurations for IoT network and nodes.

IoT Network Parameter	**Standard value used for evaluation**
Model of propagation	Two Ray Ground
MAC Protocol	802.16
Interface queue type	Priority queue with drop tail
Antenna Type	Omni directional antenna
Number of IoT Nodes	500 to 5000
Routing protocol used for comparison	AOMDV
Network Size for IoT deployment	2000m x 2000 m
Idle mode power	4mW
Receiving mode power	4mW
Transmission mode power	8mW
Sleep mode power	0.004mW
Transition mode power from Sleep to Wake up	0.8mW
Time needed to perform transitions	0.02 s
Initial energy levels of IoT nodes	4000 mW

Table 3: Average end-to-end delay for different blockchain requests.

NC	D (ms) QL [12]	D (ms) RL [13]	D (ms) DL BAC [18]	D (ms) Proposed
250	0.94	1.07	1.18	0.85
300	1.04	1.17	1.28	0.91
350	1.13	1.24	1.35	0.97
400	1.16	1.29	1.41	1.01
450	1.21	1.36	1.49	1.06
500	1.29	1.45	1.60	1.16
625	1.37	1.63	1.87	1.39
750	1.61	2.12	2.43	1.81
1000	2.27	2.77	3.06	2.21
1125	2.81	3.16	3.43	2.47
1250	2.98	3.39	3.73	2.71
1375	3.23	3.81	4.21	3.05
1500	3.75	4.35	4.76	3.43
1750	4.22	4.79	5.28	3.83
2000	4.55	5.44	5.98	4.18
2500	4.64	5.64	6.15	4.26

Table 4: Average energy consumption for different blockchain requests.

NC	E (mJ) QL [12]	E (mJ) RL [13]	E (mJ) DL BAC [18]	E (mJ) Proposed
250	2.16	3.49	3.15	2.33
300	2.65	3.93	3.47	2.54
350	2.77	4.12	3.64	2.68
400	2.91	4.36	3.86	2.85
450	3.09	4.64	4.09	3.01
500	3.29	4.88	4.29	3.14
625	3.42	5.07	4.45	3.27
750	3.56	5.27	4.63	3.40
1000	3.70	5.46	4.82	3.55
1125	3.82	5.75	5.12	3.77
1250	4.08	6.25	5.52	4.05
1375	4.51	6.60	5.73	4.18
1500	4.57	6.59	5.73	4.15
1750	4.49	6.65	5.39	3.73
2000	4.70	6.88	5.20	3.46
2500	4.91	7.06	5.33	3.52

Table 5: Average throughput performance for different blockchain requests.

NC	T (kbps) QL [12]	T (kbps) RL [13]	T (kbps) DL BAC [18]	T (kbps) Proposed
250	317.90	332.16	384.17	387.28
300	321.57	334.80	387.00	390.08
350	322.89	336.88	389.67	392.96
400	325.53	339.92	393.17	396.56
450	328.75	343.04	396.67	400.08
500	331.54	345.92	400.09	403.44
625	334.33	348.80	403.51	406.80
750	337.11	351.68	406.84	410.16
1000	339.90	354.56	410.17	413.52
1125	342.69	357.44	413.51	416.88
1250	345.47	360.32	416.84	420.24
1375	348.26	363.28	420.17	423.60
1500	351.05	366.24	423.51	426.96
1750	353.83	369.12	426.84	430.32
2000	356.62	371.93	430.13	433.63
2500	359.41	374.74	433.41	436.93

Table 6: Average packet delivery ratio performance for different blockchain requests.

NC	PDR (%) QL [12]	PDR (%) RL [13]	PDR (%) DL BAC [18]	PDR (%) Proposed
250	76.87	76.64	77.50	83.02
300	77.76	77.23	78.07	83.63
350	78.08	77.71	78.60	84.23
400	78.72	78.42	79.32	85.00
450	79.50	79.14	80.04	85.75
500	80.17	79.80	80.71	86.48
625	80.84	80.47	81.38	87.20
750	81.52	81.14	82.06	87.91
1000	82.20	81.81	82.73	88.64
1125	82.87	82.48	83.40	89.36
1250	83.54	83.15	84.08	90.08
1375	84.21	83.81	84.76	90.80
1500	84.89	84.48	85.43	91.52
1750	85.56	85.15	86.10	92.25
2000	86.24	85.82	86.78	92.98
2500	86.91	86.47	87.44	93.69

Table 7: Average end-to-end delay for different attack types.

NA	D (ms) QL [12]	D (ms) RL [13]	D (ms) DL BAC [18]	D (ms) Proposed
25	1.28	1.43	1.38	1.10
50	1.39	1.53	1.48	1.18
75	1.48	1.61	1.55	1.24
125	1.54	1.68	1.63	1.31
200	1.63	1.79	1.75	1.40
250	1.75	1.98	2.00	1.55
275	1.99	2.41	2.46	1.86
300	2.54	3.09	3.10	2.36
325	3.29	3.74	3.68	2.89
350	3.78	4.16	4.08	3.25
375	4.08	4.58	4.51	3.56
400	4.56	5.17	5.08	4.00
425	5.19	5.82	5.71	4.51
450	5.78	6.47	6.33	5.02
475	6.42	7.13	6.92	5.53
500	6.58	7.30	7.08	5.66

Table 8: Average energy consumption for different attack types.

NA	E (mJ) QL [12]	E (mJ) RL [13]	E (mJ) DL BAC [18]	E (mJ) Proposed
25	3.53	3.99	3.89	2.79
50	3.99	4.34	4.20	3.07
75	4.19	4.58	4.43	3.23
125	4.44	4.85	4.68	3.42
200	4.72	5.13	4.93	3.62
250	4.96	5.36	5.15	3.79
275	5.15	5.57	5.36	3.94
300	5.35	5.78	5.58	4.09
325	5.57	6.07	5.88	4.28
350	5.87	6.47	6.28	4.54
375	6.33	6.89	6.63	4.85
400	6.68	7.08	6.72	5.01
425	6.68	6.94	6.39	4.89
450	6.42	6.03	5.63	4.42
475	4.97	5.54	5.59	3.93
500	5.11	6.43	6.41	4.39

Table 9: Average throughput performance for different attack types.

NA	T (kbps) QL [12]	T (kbps) RL [13]	T (kbps) DL BAC [18]	T (kbps) Proposed
25	432.73	460.89	440.22	599.44
50	436.40	464.26	443.46	604.04
75	439.08	467.74	446.97	608.40
125	442.96	471.98	450.98	613.85
200	447.05	476.14	454.91	619.33
250	450.82	480.14	458.73	624.55
275	454.59	484.15	462.54	629.75
300	458.38	488.14	466.36	634.95
325	462.14	492.14	470.17	640.16
350	465.91	496.14	473.98	645.37
375	469.68	500.14	477.79	650.57
400	473.45	504.15	481.61	655.78
425	477.22	508.15	483.88	660.29
450	480.99	506.00	449.22	645.44
475	484.77	505.08	423.02	634.95
500	485.58	480.04	416.01	659.23

Table 10: Average packet delivery ratio performance for different attack types.

NA	PDR (%) QL [12]	PDR (%) RL [13]	PDR (%) DL BAC [18]	PDR (%) Proposed
25	62.09	59.61	65.43	90.30
50	62.81	60.07	65.92	90.96
75	63.07	60.43	66.37	91.62
125	63.58	60.98	66.97	92.46
200	64.21	61.54	67.57	93.28
250	64.75	62.06	68.14	94.06
275	65.30	62.58	68.72	94.84
300	65.85	63.10	69.29	95.63
325	66.39	63.62	69.85	94.48
350	66.93	64.14	70.42	95.25
375	67.47	64.66	70.98	96.01
400	68.02	65.18	71.56	96.78
425	68.57	65.70	72.13	97.55
450	69.11	66.22	72.70	98.32
475	69.66	66.74	73.27	99.10
500	70.20	67.25	73.83	99.85

Funding: There is no funding provided to prepare the manuscript.

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

Authors Contribution: Co-authors contributed equally.

References

[1] Ahmed, I., Zhang, Y., Jeon, G., Lin, W., Khosravi, M. R., & Qi, L. (2022). A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city. *International Journal of Intelligent Systems,* int.22852. https://doi.org/10.1002/int.22852

[2] Asheralieva, A., & Niyato, D. (2021). Throughput-Efficient Lagrange Coded Private Blockchain for Secured IoT Systems. *IEEE Internet of Things Journal,* 8(19), 14874–14895. https://doi.org/10.1109/JIOT.2021.3071563

[3] Bera, B., Saha, S., Das, A. K., & Vasilakos, A. V. (2021). Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System. *IEEE Internet of Things Journal,* 8(7), 5744–5761. https://doi.org/10.1109/JIOT.2020.3030308

[4] Debe, M., Salah, K., Jayaraman, R., Yaqoob, I., & Arshad, J. (2021). Trustworthy Blockchain Gateways for Resource-Constrained Clients and IoT Devices. *IEEE Access*, 9, 132875–132887. https://doi.org/10.1109/ACCESS.2021.3115150

[5] He, Y., Wang, Y., Qiu, C., Lin, Q., Li, J., & Ming, Z. (2021). Blockchain-Based Edge Computing Resource Allocation in IoT: A Deep Reinforcement Learning Approach. *IEEE Internet of Things Journal,* 8(4), 2226–2237. https://doi.org/10.1109/JIOT.2020.3035437

[6] Kumar, P., Kumar, R., Srivastava, G., Gupta, G. P., Tripathi, R., Gadekallu, T. R., & Xiong, N. N. (2021). PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities. *IEEE Transactions on Network Science and Engineering*, 8(3), 2326–2341. https://doi.org/10.1109/TNSE.2021.3089435

[7] Li, Z., Hao, J., Liu, J., Wang, H., & Xian, M. (2021). An IoT-Applicable Access Control Model Under Double-Layer Blockchain. *IEEE Transactions on Circuits and Systems II: Express Briefs,* 68(6), 2102–2106. https://doi.org/10.1109/TCSII.2020.3045031

[8] Ma, Z., Wang, L., & Zhao, W. (2021). Blockchain-Driven Trusted Data Sharing With Privacy Protection in IoT Sensor Network. *IEEE Sensors Journal,* 21(22), 25472–25479. https://doi.org/10.1109/JSEN.2020.3046752

[9] Mahrous, W. A., Farouk, M., & Darwish, S. M. (2021). An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash. *IEEE Access,* 9, 151327–151336. https://doi.org/10.1109/ACCESS.2021.3126715

[10] Masoumi, M., Dalili Oskouei, H. R., Mohammadi Shirkolaei, M., & Mirtaheri, A. R. (2022). Substrate integrated waveguide leaky wave antenna with circular polarization and improvement of the scan angle. *Microwave and Optical Technology Letters,* 64(1), 137–141. https://doi.org/10.1002/mop.33047

[11] Moayyed, F., Dalili Oskouei, H. R., & Mohammadi Shirkolaei, M. (2021). High Gain and Wideband Multi-Stack Multilayer Anisotropic Dielectric Antenna. *Progress In Electromagnetics Research Letters,* 99, 103–109. https://doi.org/10.2528/PIERL21062307

[12] Mohammadi Shirkolaei, M. (2020). A New Design Approach of Low-Noise Stable Broadband Microwave Amplifier Using Hybrid Optimization Method. *IETE Journal of Research,* 1–7. https://doi.org/10.1080/03772063.2020.1787879

[13] Mohammadi Shirkolaei, M., Dalili Oskouei, H. R., & Abbasi, M. (2021). Design of 1*4 Microstrip Antenna Array on the Human Thigh with Gain Enhancement. *IETE Journal of Research,* 1–7. https://doi.org/10.1080/03772063.2021.2004459

[14] Mohammadi Shirkolaei, M., & Ghalibafan, J. (2021). Magnetically scannable slotted waveguide antenna based on the ferrite with gain enhancement. *Waves in Random and Complex Media,* 1–11. https://doi.org/10.1080/17455030.2021.1983234

[15] Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Addressing Security and Privacy Issues of IoT Using Blockchain Technology. *IEEE Internet of Things Journal,* 8(2), 881–888. https://doi.org/10.1109/JIOT.2020.3008906

[16] Nguyen, L. D., Leyva-Mayorga, I., Lewis, A. N., & Popovski, P. (2021). Modeling and Analysis of Data Trading on Blockchain-Based Market in IoT Networks. *IEEE Internet of Things Journal,* 8(8), 6487–6497. https://doi.org/10.1109/JIOT.2021.3051923

[17] Oktian, Y. E., & Lee, S.-G. (2021). BorderChain: Blockchain-Based Access Control Framework for the Internet of Things Endpoint. *IEEE Access,* 9, 3592–3615. https://doi.org/10.1109/ACCESS.2020.3047413

[18] Patil, P., Sangeetha, M., & Bhaskar, V. (2021). Blockchain for IoT Access Control, Security and Privacy: A Review. *Wireless Personal Communications,* 117(3), 1815–1834. https://doi.org/10.1007/s11277-020-07947-2

[19] Qiu, C., Wang, X., Yao, H., Du, J., Yu, F. R., & Guo, S. (2021). Networking Integrated Cloud–Edge–End in IoT: A Blockchain-Assisted Collective Q -Learning Approach. *IEEE Internet of Things Journal,* 8(16), 12694–12704. https://doi.org/10.1109/JIOT.2020.3007650

[20] Rahman, A., Islam, Md. J., Montieri, A., Nasir, M. K., Reza, Md. M., Band, S. S., Pescape, A., Hasan, M., Sookhak, M., & Mosavi, A. (2021). SmartBlock-SDN: An Optimized Blockchain-SDN Framework for Resource Management in IoT. *IEEE Access,* 9, 28361–28376. https://doi.org/10.1109/ACCESS.2021.3058244

[21] Ray, P. P., Chowhan, B., Kumar, N., & Almogren, A. (2021). BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem. *IEEE Internet of Things Journal,* 8(13), 10857–10872. https://doi.org/10.1109/JIOT.2021.3050703

[22] Ren, J., Li, J., Liu, H., & Qin, T. (2022). 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. https://doi.org/10.26599/TST.2021.9010046

[23] Shirkolaei, M. M.,& Aslinezhad, M. (2021). Substrate integrated waveguide filter based on the magnetized ferrite with tunable capability. *Microwave and Optical Technology Letters,* 63(4), 1120–1125. https://doi.org/10.1002/mop.32722

[24] Sun, S., Du, R., Chen, S., & Li, W. (2021). Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain. *IEEE Access,* 9, 36868–36878. https://doi.org/10.1109/ACCESS.2021.3059863

[25] Whaiduzzaman, M., Mahi, Md. J. N., Barros, A., Khalil, Md. I., Fidge, C., & Buyya, R. (2021). BFIM: Performance Measurement of a Blockchain Based Hierarchical Tree Layered Fog-IoT Microservice Architecture. *IEEE Access,* 9, 106655–106674. https://doi.org/10.1109/ACCESS.2021.3100072

[26] Wu, D., & Ansari, N. (2021). A Trust-Evaluation-Enhanced Blockchain-Secured Industrial IoT System. *IEEE Internet of Things Journal,* 8(7), 5510–5517. https://doi.org/10.1109/JIOT.2020.3030689

[27] Xiao, W., Liu, C., Wang, H., Zhou, M., Hossain, M. S., Alrashoud, M., & Muhammad, G. (2021). Blockchain for Secure-GaS: Blockchain-Powered Secure Natural Gas IoT System With AI-Enabled Gas Prediction and Transaction in Smart City. *IEEE Internet of Things Journal,* 8(8), 6305–6312. https://doi.org/10.1109/JIOT.2020.3028773

[28] Yang, Q., & Wang, H. (2021). Privacy-Preserving Transactive Energy Management for IoT-Aided Smart Homes via Blockchain. *IEEE Internet of Things Journal,* 8(14), 11463–11475. https://doi.org/10.1109/JIOT.2021.3051323

[29] Zhang, A., Zhang, P., Wang, H., & Lin, X. (2021). Application-Oriented Block Generation for Consortium Blockchain-Based IoT Systems With Dynamic Device Management. *IEEE Internet of Things Journal,* 8(10), 7874–7888. https://doi.org/10.1109/JIOT.2020.3041163

[30] Zhang, W., Wang, J., Han, G., Huang, S., Feng, Y., & Shu, L. (2021). A Data Set Accuracy Weighted Random Forest Algorithm for IoT Fault Detection Based on Edge Computing and Blockchain. *IEEE Internet of Things Journal,*8(4), 2354–2363. https://doi.org/10.1109/JIOT.2020.3044934

[31] Zuo, Y., Jin, S., & Zhang, S. (2021). Computation Offloading in Untrusted MEC-Aided Mobile Blockchain IoT Systems. *IEEE Transactions on Wireless Communications,* 20(12), 8333–8347. https://doi.org/10.1109/TWC.2021.3091861

About the Authors

Shital Agrawal received the BE degree in Computer Science and Engineering from SGB Amravati University India in 2010 and an ME degree in Computer Science and Engg. From S.G.B Amaravati in 2014. Currently, he is a PhD. Research scholar at Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan, INDIA. He started his academic career in 2012 and has been a lecturer at Sharadchandraji Pawar Polytechnic College, Aurangabad. His research interest includes machine learning, IoT and Artificial Intelligence.

Dr. Shailesh Kumar received a BE degree in Computer Science from HMSIT Tumkur, India, in 2009, an MTECH degree in Computer Science From SSIT Tumkur in 2011 and a PhD from JJTU, Rajasthan, in 2018. He started his academic career in 2011 and currently working as Associate Professor in SVCET Chittor. He has published more than eight international research papers and has one Patent. He has taken guest lectures at different prestigious institutes. His research interest includes JAVA programming, C++ and Python