*I.J. Image, Graphics and Signal Processing,* **2022, 5, 58-71**
Published Online on October 8, 2022 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2022.05.05

# MLSMBQS: Design of a Machine Learning Based Split & Merge Blockchain Model for QoS-Aware Secure IoT Deployments

**Shital Agrawal**
PhD. Research Scholar, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan, INDIA
Email: shitalagrawal2022@outlook.com

**Shailesh Kumar**
Research Guide, Associate Professor, SVCET, Chittoor, INDIA
Email: shaileshkumar1610@gmail.com

Received: 17 March 2022; Accepted: 29 May 2022; Published: 08 October 2022

**Abstract:** Internet of Things (IoT) Networks are multitier deployments which assist on-field data to be sensed, processed, communicated, and used for taking control decisions. These deployments utilize hardware-based components for data sensing & actuation, while cloud components are used for data-processing & recommending control decisions. This process involves multiple low-security, low-computational capacity & high-performance entities like IoT Devices, short range communication interfaces, edge devices, routers, & cloud virtual machines. Out of these entities, the IoT Device, router, & short-range communication interfaces are highly vulnerable to a wide-variety of attacks including Distributed Denial of Service (DDoS), worm hole, sybil, Man in the Middle (MiTM), Masquerading, spoofing attacks, etc. To counter these attacks, a wide variety of encryption, key-exchange, and data modification models are proposed by researchers. Each of these models have their own levels of complexities, which reduces QoS of underlying IoT deployments. To overcome this limitation, blockchain-based security models were proposed by researchers, and these models allow for high-speed operations for small-scale networks. But as network size is increased, delay needed for blockchain mining increases exponentially, which limits its applicability. To overcome this issue, a machine learning based blockchain model for QoS-aware secure IoT deployments is proposed in this text. The proposed MLSMBQS model initially deploys a Proof-of-Work (PoW) based blockchain model, and then uses bioinspired computing to split the chain into multiple sub-chains. These sub-chains are termed as shards, and assists in reduction of mining delay via periodic chain splitting process. The significance of this research is use of Elephant Herd Optimization (EHO) which assists in managing number of blockchain-shards via splitting or merging them for different deployment conditions. This decision of splitting or merging depends on blockchain's security & quality of service (QoS) performance. Due to integration of EHO for creation & management of sidechains, the findings of this research showcase that the proposed model is capable of improving throughput by 8.5%, reduce communication delay by 15.3%, reduce energy consumption by 4.9%, and enhance security performance by 14.8% when compared with existing blockchain & non-blockchain based security models. This is possible because EHO initiates dummy communication requests, which are arbitrarily segregated into malicious & non-malicious, and usedfor continuous QoS & security performance improvement of the proposed model. Due to this continuous performance improvement, the proposed MLSMBQS model is capable of deployment for a wide variety of high-efficiency IoT network scenarios.

**Index Terms:** IoT, Blockchain, Sidechain, Machine Learning, QoS, PoW, EHO, Delay, Security, Energy, Attacks.

## 1. Introduction

Blockchain based IoT Networks are able to optimize security & provide better QoS performance due to their immutability, transparency, traceability, and distributed computing characteristics. To design such networks, a large number of processing components including miner nodes, verifier nodes, block design managers, consensus enforcement agents, etc. are required. A typical blockchain based IoT Network model is depicted in Fig. 1, wherein data from sensors is collected on a local gateway node, which stores this data onto a blockchain [1, 2, 3] database. The model uses Local Gateways, Adaptaton Layers, Application Layers, Distributed Computing Layers, etc. to improve scalability and performance under different real-time conditions. These layers work in tandem to incorporate high efficiency and low complexity models that have better flexibility when applied to real-time networks.

 

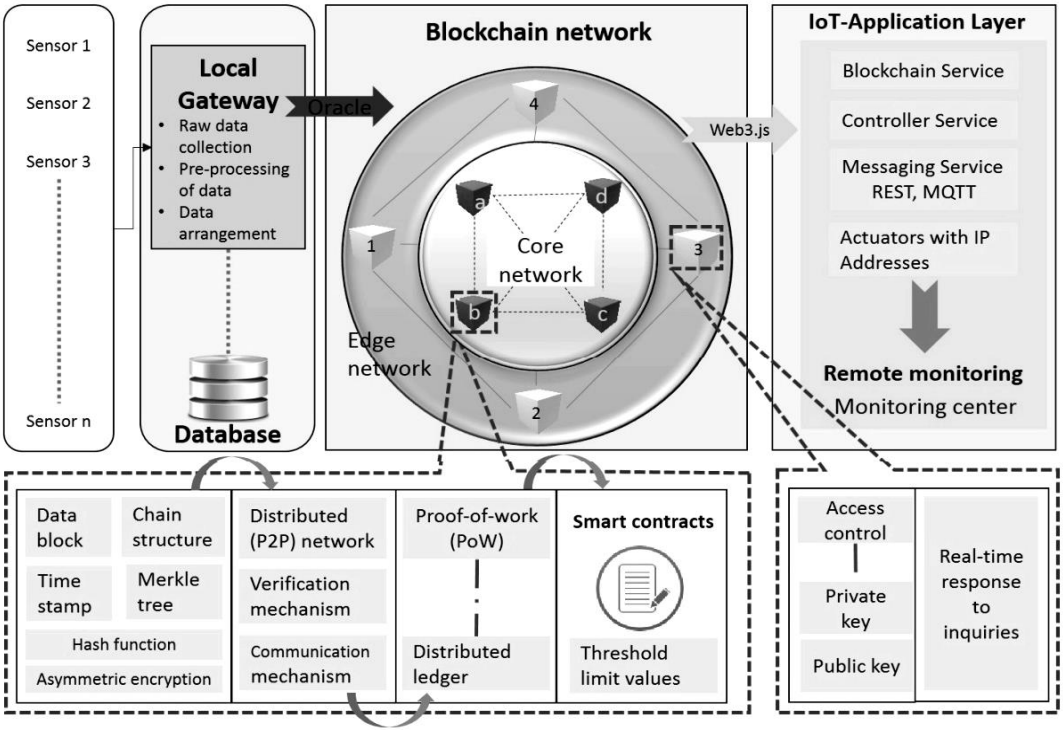


Fig. 1. A typical blockchain-based IoT Network Model

This database consists of different types of block-structures, consensus models, access control models, key-exchange mechanisms, etc. which assist in efficient storage & retrieval of data blocks. To store a block into this blockchain, a number of delay components are needed, which can be observed via equation 1 as follows,

$$D_{store} = N * \left(D_{read} + D_{verify} + D_{hash}\right) + D_{write} \quad (1)$$

Where, $D_{read}, D_{verify}$&$D_{write}$ represents delay needed to read, verify & write the blocks to the chain, while $D_{store}$ represents delay needed to store the block in the blockchain which consists of $N$ existing blocks. It can be observed that, this delay is directly proportional to the chain length, and will increase exponentially with it. To reduce this delay, various sidechain-based models are proposed by researchers, and each of them vary in terms of security, computational complexity, and scalability performance. A review of these models, along with their nuances, advantages, limitations, and future research scopes is discussed in the next section of this text. Based on this discussion, main limitations of these models include, but are not limited to, scalability of these sidechain models depends directly on the underlying consensus method and block structure, due to which their applicability to general purpose deployments is limited. The main objective of this paper is to overcome this limitation via design of machine learning based split & merge blockchain model for QoS-aware secure IoT deployments, which is discussed in section 3 of this text. Performance of this model is evaluated in terms of computational delay, energy consumption, & security level metrics in section 4, and is compared with various state-of-the-art 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 assortment of blockchain frameworks are intended to further develop proficiency and assault versatility of remote organizations. For example, the work done in [4, 5, 6] proposes models for abstaining from sticking organizations, mining assaults, presence of Carrier Sense Multiple Access/Collision Avoidance (CSMA/CD), and asset designation procedures. These procedures take into account execution upgrade of remote organizations under application explicit situations. Essentially, the work in [7] proposes models for secure hub steering, secure power exchanging, secure information correspondence, and secure trust assessment system utilizing blockchains. The proposed models use the benefits of blockchain to gauge and track any undesirable foes, and eliminate them from the organization. Blockchain is known for its permanence, recognizability, and dispersed execution, and the models proposed in [8, 9, 10] use this characteristic to plan side chain (SC) blockchain arrangements, media based blockchain correspondences, and security conservation with task offloading for high productivity applications. These models have

demonstrated to have great QoS and high security execution under various sorts of organization conditions. Essentially, the work proposed in [11, 12, 13, 14, 15] additionally use blockchain for secure range access, plan of lightweight web of things (IoT) organizations, private Body AreaNetwork (BAN) plan, and secure asset portion under different organization conditions. These conventions are seen to have elite execution, alongside high overheads because of expansion in blockchain length.

Offloading information to different organizations [16], edge figuring for further developed mining productivity [19], decentralizing radio access [18, 19], elite execution examination of ongoing blockchain models [20, 21], and decentralized trust the board [22, 23] additionally use blockchains, however advance its exhibition utilizing equal handling and circulated registering models. Utilizations of these conventions can be seen from [24, 25, 26, 27,28], wherein quantum mindful eVoting, boosted blockchain models (BBM), joint asset designation, pontoon-based agreement, and plan of shrewd systems administration frameworks is depicted. These applications help with understanding the profundity with which blockchain and its partners are being utilized in remote organizations for improving their exhibition, and lessening assault likelihood in the organization. Particular blockchain model plans can be seen from [29, 30, 31, 32, 33] wherein unattended wellbeing observing, range sharing exchanges, property and attribute-based encryption (ABE) for secure telemedicine, secure energy move in vehicular energy organizations, and superior execution gadget to-gadget (D2D) transcoding utilizing support learning is depicted. This multitude [34, 35] of uses show that blockchain models can be joined with various AI and profound learning models for working on their inner execution.

### *2.2 Design of machine learning based split & merge blockchain model for QoS-aware secure IoT deployments*

From the literature survey, it was observed that a wide variety of sidechaining models were proposed by researchers, and each of them varies in terms of security level, QoS level, and other quantitative & qualitative metrics. But these models have limited scalability, because they work via splitting the chain into multiple parts, and do not perform chain merging operations. Due to which, number of sidechains are always increasing, which limits its computational performance when used for large-scale networks. To overcome this limitation, a EHO based sidechaining model is proposed in this text. Overall flow of the proposed model is visualized from fig. 2, wherein it can be observed that input blockchain is initially checked in terms of QoS & security metrics, to take merging & split decisions.

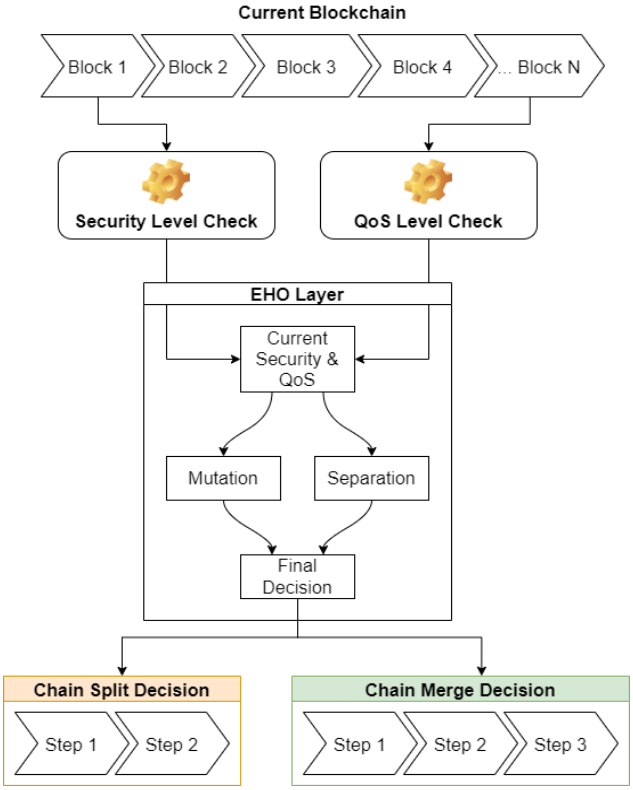


Fig. 2. Overall flow of the proposed model

From the flow it can be observed that decisions for splitting & merging the main blockchain are taken by the EHO model, which evaluates current security & QoS metrics. For simplicity, design of the proposed model is divided into different sub-parts, and each of these parts are discussed in separate sub-sections of this text. Researchers can implement the model in part(s) or as a whole depending upon their application's requirements.

*2.3. Design of the Security & QoS level checking layer*

The model initially considers original blockchain, which requires splitting or merging, and evaluates various security & QoS parameters. These parameters are evaluated via the following process,

- A set of $N$ dummy communication requests are initiated by the model
- These requests are stochastically divided into normal ($N_r$) & malicious requests ($M_r$).
- The malicious requests are further divided into the following attacks,
  - Man in the Middle (MiTM)
  - Distributed Denial of Service (DDoS)
  - Worm hole
  - Sybil
  - Masquerading
  - Spoofing attacks
- The blockchain is exposed to these attacks, and its parametric evaluation is done in terms of end-to-end delay, energy requirement, throughput, packet delivery ratio (PDR), and security levels

The end-to-end delay is evaluated for malicious & non-malicious requests via equation 2 & 3 respectively as follows,

$$D(M) = \frac{\sum_{i=1}^{M_r} t_{end_i} - t_{start_i}}{M_r} \tag{2}$$

$$D(N) = \frac{\sum_{i=1}^{N_r} t_{end_i} - t_{start_i}}{N_r} \tag{3}$$

Similarly, energy required for communication is evaluated via equations 4 & 5 as follows,

$$E(M) = \frac{\sum_{i=1}^{M_r} E_{start_i} - E_{end_i}}{M_r} \tag{4}$$

$$E(N) = \frac{\sum_{i=1}^{N_r} E_{start_i} - E_{end_i}}{N_r} \tag{5}$$

While, throughput, and PDR are evaluated via equations 6, 7, 8 & 9 as follows,

$$T(M) = \sum_{i=1}^{M_r} \frac{Rx(P)_i}{M_r * D(M)}) \tag{6}$$

$$T(N) = \sum_{i=1}^{N_r} \frac{Rx(P)_i}{N_r * D(N)} \tag{7}$$

$$PDR(M) = \sum_{i=1}^{M_r} \frac{Rx(P)_i}{Tx(P)_i * M_r} \tag{8}$$

$$PDR(N) = \sum_{i=1}^{N_r} \frac{Rx(P)_i}{N_r * Tx(P)_i} \tag{9}$$

Where, $t_{start}, t_{end}$ represents start & end time of communication, $E_{start}, E_{end}$ represents energy level of nodes before starting and after finishing the communication, $RX(P) \& TX(P)$ represents number of received & transmitted packets during the communication. Based on these metrics, security level for these requests is evaluated via equation 10 as follows,

$$SL = \frac{\frac{D(N)}{D(M)} + \frac{E(N)}{E(M)} + \frac{T(M)}{T(N)} + \frac{PDR(M)}{PDR(N)}}{4} \tag{10}$$

If the security level is more or less than 1, then it indicates that network's performance is highly variant between normal & malicious requests, if it is near to 1, then the network is currently performing fine, and there is no need of chain splitting or merging operations. In the prior case, an EHO model layer is activated, which assists in deciding whether to split the chain or merge it, depending upon its temporal performance metrics. Design of this layer is discussed in the next section of this text.

*2.4. Design of the EHO modelling layer*

Once the decision to split & merge is taken, then an EHO model is activated, which assists finalizing whether to split or merge the chains. This model uses temporal blockchain performance, and estimates whether it requires chain merging, or splitting, for better security & QoS performance. To perform this task, the following process is used,

- Initialize EHO parameters,
  - Number of iterations ($N_i$)
  - Number of herds ($N_h$)
  - Learning rate ($L_r$)
  - Current Number of sidechains ($N_{sc}$)
  - Length of each sidechain ($L_{sc}$)
- Initially mark all herds as 'to be modified'
- For each iteration in 1 to $N_i$
  - For each herd in 1 to $N_h$
    - If this herd is marked as 'not to be modified', then go to the next herd
    - Else, Modify this herd via the following process,
- Select a stochastic sidechain from the current list of sidechains, and generate a stochastic number of requests($N_{stoch}$) for block addition to this chain.
- Segregate these requests into normal & malicious, and evaluate QoS & security metrics for each request via equations 2 to 10
- Based on these metrics, evaluate herd fitness via equation 11,

$$f_h = \frac{\left[\sum_{i=1}^{N_{stoch}} SL_i - \sum_{j=1}^{N_{stoch}} \frac{SL_j}{N_{stoch}}\right]}{N_{stoch}} * \left[\frac{D(N)-D(M)}{D(M)} + \frac{E(N)-E(M)}{E(M)} + \frac{T(M)-T(N)}{T(N)} + \frac{PDR(M)-PDR(N)}{PDR(N)}\right] \quad (11)$$

  - This evaluation is done for each herd, and then a fitness threshold is evaluated via equation 12 as follows,

$$f_{th} = \frac{\sum_{i=1}^{N_h} f_{h_i} * L_r}{N_h} \quad (12)$$

  - Herds with fitness value more than $f_{th}$ are marked as 'to be modified', while others are marked as 'not to be modified'
  - The herd with minimum fitness is marked as 'Matriarch' herd, and based on this herd's fitness, learning rate is modified as per equation 13,

$$New(L_r) = Old(L_r) * \frac{Min\left(\cup_{i=1}^{N_h} f_{h_i}\right)}{\sum_{i=1}^{N_h} f_{h_i}} \quad (13)$$

- At the end of $N_i$ iterations, select the herd with minimum fitness at the output.

The selected herd is analyzed for security performance and QoS performance levels. These levels are compared with currently used blockchain, and decision rules are applied. These rules can be observed from table 1 as follows, where $C$ & $M$ represents current & Matriarch levels,

Table 1. Decision rules for merging or splitting current blockchain

| QoS | Security (S) | Decision |
|---|---|---|
| $C(QoS) > M(QoS)$ | $C(S) = M(S)$ | Merge this chain with current blockchain |
| $C(QoS) = M(QoS)$ | $C(S) = M(S)$ | Use the current blockchain without any changes |
| $C(QoS) < M(QoS)$ | $C(S) = M(S)$ | Split this chain into 2 equal parts |
| $C(QoS) > M(QoS)$ | $C(S) > M(S)$ | Merge this chain with current blockchain |
| $C(QoS) = M(QoS)$ | $C(S) > M(S)$ | Merge this chain with current blockchain |
| $C(QoS) < M(QoS)$ | $C(S) > M(S)$ | Split this chain into 2 equal parts |

| | | |
|---|---|---|
| $C(QoS) > M(QoS)$ | $C(S) < M(S)$ | Split this chain into 2 equal parts |
| $C(QoS) = M(QoS)$ | $C(S) < M(S)$ | Split this chain into 2 equal parts |
| $C(QoS) < M(QoS)$ | $C(S) < M(S)$ | Split this chain into 2 equal parts |

Based on these rules, current blockchain is either split into 2 equal parts, or merged with existing chain for better QoS & security performance levels.

*2.5 Management of splitting & merging decisions*

Once the decision about merging or splitting the main blockchain is given by the EHO model, then different processesare evaluated to execute these decisions. To execute split decision, the following process is used,

- If decision to split the chain is recommended, then, currently used chain is divided into 2 equal parts, and $SL$ is evaluated for each chain via equation 10, which assists in estimation of security & QoS levels for these chains.
- Based on these levels, selection threshold is evaluated via equation 14,

$$Sel_{th} = \frac{SL_1}{SL_2} \tag{14}$$

Where, $SL_1$& $SL_2$ represents security level of chain 1 & chain 2 respectively.

- If $Sel_{th} > 1$, then chain 2 is used, else chain 1 is used for addition of future blocks into the blockchain. Similarly, to execute merge decision, the following process is used,
- Select the sidechain with $SL$ value closest to value 1, which assists in identification of chain with better QoS & security levels.
- Use this sidechain for merging the current sidechain.

Based on these decisions, the blockchains are merged, or split, for ensuring optimum security & QoS performance for current network deployment. This performance was evaluated in terms of different qualitative & quantitative metrics, and discussed in the next section of this text.

## 3. Experimental Result and Analysis

The proposed model uses a combination of EHO with recommendation engine to improve QoS & security of existing blockchain deployments. In order to evaluate its performance, simulation on standard networking scenarios is needed. To perform this task, the following network parameters were considered,

Channel Type: Wireless Channel
Propagation Model: Two Ray Ground
Network interface: Physical & Wireless
MAC Protocol: MAC 802.16a
Interface Queue type: Priority queued drop tail
Antenna Type: Omnidirectional Antenna
Number of nodes: 50 to 500
Routing protocol: AOMDV
Network X Size: 500
Network Y Size: 500
Packet Size: 2000 bytes per packet
Packet Interval: 0.001 seconds per packet

Based on these standard IoTNetwork standard parameters, evaluation was done for end-to-end communication delay, energy consumption during each communication, packet delivery ratio (PDR) andthroughput obtained for all communications. This performance was compared with SC [8], BAN [14], and BBM [25] under the same network conditions. These methods use similar internal models, due to which they were used for comparison. Each of these comparisons were done for 100 different communications, for varying number of nodes. Based on these conditions, table 2 represents delay performance for each of the models.

Table 2. Delay performance for different nodes over 100 communications

| Num. Nodes | Delay (ms) SC [8] | Delay (ms) BAN [14] | Delay (ms) BBM [25] | Delay (ms) MLSM BQS |
|---|---|---|---|---|
| 50 | 0.25 | 0.29 | 0.24 | 0.15 |
| 75 | 0.30 | 0.34 | 0.28 | 0.18 |
| 100 | 0.40 | 0.46 | 0.38 | 0.24 |
| 150 | 0.51 | 0.59 | 0.48 | 0.30 |
| 200 | 0.59 | 0.68 | 0.56 | 0.36 |
| 250 | 0.69 | 0.79 | 0.65 | 0.41 |
| 300 | 0.80 | 0.91 | 0.75 | 0.48 |
| 400 | 0.86 | 0.99 | 0.81 | 0.51 |
| 500 | 0.93 | 1.07 | 0.88 | 0.56 |

From these evaluations and fig. 3, it can be observed that end-to-end delay has been reduced by 15.6% when compared with SC [8], 24.8% with compared with BAN [14] and 14.9% when compared withBBM [25]models. This is due to use of end-to-end delay metrics while selection& management of sidechains.

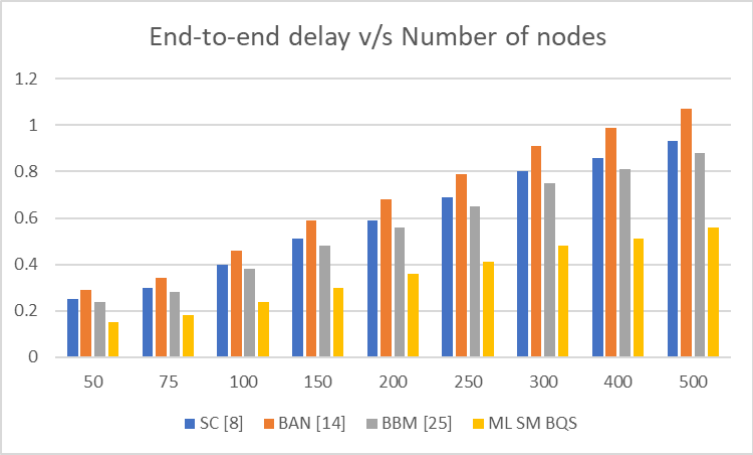


Fig. 3. End-to-end delay v/s Number of nodes

Similar observations can be seen for energy, consumption from table 3 as follows,

Table 3. Energy performancefor different nodes over 100 communications

| Num. Nodes | E (mJ) SC [8] | E (mJ) BAN [14] | E (mJ) BBM [25] | E (mJ) ML SM BQS |
|---|---|---|---|---|
| 50 | 5.33 | 6.14 | 5.05 | 3.19 |
| 75 | 5.76 | 6.63 | 5.46 | 3.44 |
| 100 | 6.05 | 6.96 | 5.73 | 3.61 |
| 150 | 6.29 | 7.23 | 5.96 | 3.75 |
| 200 | 6.48 | 7.45 | 6.14 | 3.87 |
| 250 | 6.86 | 7.89 | 6.50 | 4.10 |
| 300 | 7.33 | 8.44 | 6.95 | 4.38 |
| 400 | 7.67 | 8.82 | 7.26 | 4.58 |
| 500 | 7.96 | 9.15 | 7.54 | 4.75 |

From these evaluations and fig. 4, it can be observed that energy consumption has been reduced by 16.8% when compared with SC [8], 26.5% with compared with BAN [14] and 15.2% when compared with BBM [25] models. This is due to use of residual energy metric while selection & management of sidechains.

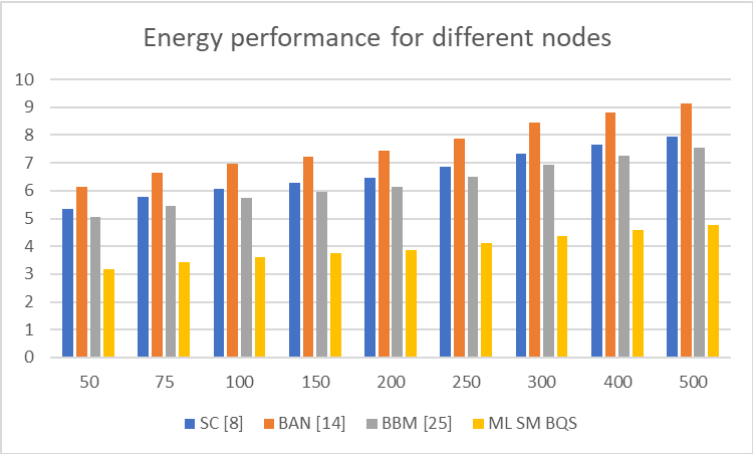


Fig. 4. Energy v/s Number of nodes

This improvement allows the system to be applied for real-time use cases like low-powered body sensor networks. Performance evaluation in terms of throughput can be observed from table 4 as follows,

Table 4. Throughput performancefor different nodes over 100 communications

| Num. Nodes | Thr. (kbps) SC [8] | Thr. (kbps) BAN [14] | Thr. (kbps) BBM [25] | Thr. (kbps) ML SM BQS |
|---|---|---|---|---|
| 50 | 312.38 | 271.63 | 369.21 | 486.68 |
| 75 | 320.00 | 278.26 | 378.21 | 498.55 |
| 100 | 321.90 | 279.91 | 380.46 | 501.52 |
| 150 | 324.29 | 281.99 | 383.28 | 505.23 |
| 200 | 327.14 | 284.47 | 386.65 | 509.68 |
| 250 | 329.52 | 286.54 | 389.47 | 513.39 |
| 300 | 332.86 | 289.44 | 393.41 | 518.59 |
| 400 | 336.67 | 292.76 | 397.91 | 524.52 |
| 500 | 340.09 | 295.74 | 401.96 | 529.86 |

From these evaluations and fig. 5, it can be observed that throughput has increased by 26.3% when compared with SC [8], 23.5% with compared with BAN [14] and 10.8% when compared with BBM [25] models. This is due to use of throughput metric while selection & management of sidechains.

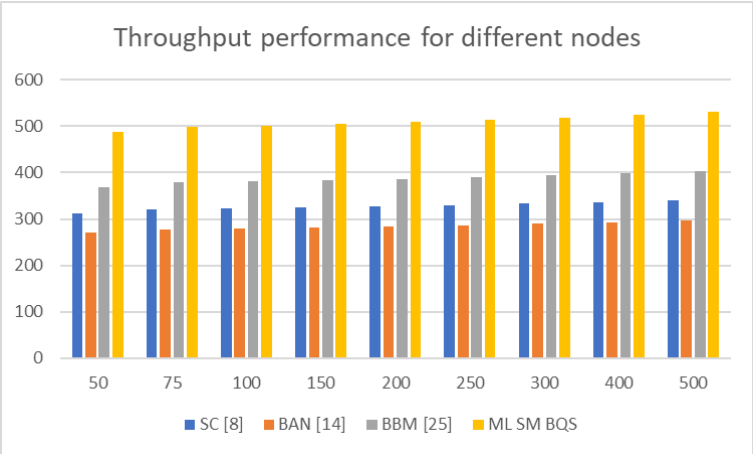


Fig. 5. Throughput (kbps) v/s Number of nodes

Similarly, packet delivery ratio of these models was compared, and can be observed from table 5 as follows,

Table 5. PDR performancefor different nodes over 100 communications

| Num. Nodes | PDR (%) SC [8] | PDR (%) BAN [14] | PDR (%) BBM [25] | PDR (%) ML SM BQS |
|---|---|---|---|---|
| 50 | 93.90 | 94.00 | 90.92 | 98.65 |
| 75 | 94.10 | 94.19 | 91.11 | 98.85 |
| 100 | 94.29 | 94.38 | 91.29 | 99.05 |
| 150 | 94.38 | 94.48 | 91.38 | 99.15 |
| 200 | 94.43 | 94.52 | 91.43 | 99.20 |
| 250 | 94.52 | 94.62 | 91.52 | 99.30 |
| 300 | 94.62 | 94.71 | 91.61 | 99.40 |
| 400 | 94.71 | 94.81 | 91.71 | 99.50 |
| 500 | 94.84 | 94.93 | 91.83 | 99.63 |

From these evaluations and fig. 6, it can be observed that throughput has increased by 4.3% when compared with SC [8], 4.5% with compared with BAN [14] and 6.8% when compared with BBM [25] models. This is due to use of PDR metric while selection & management of sidechains

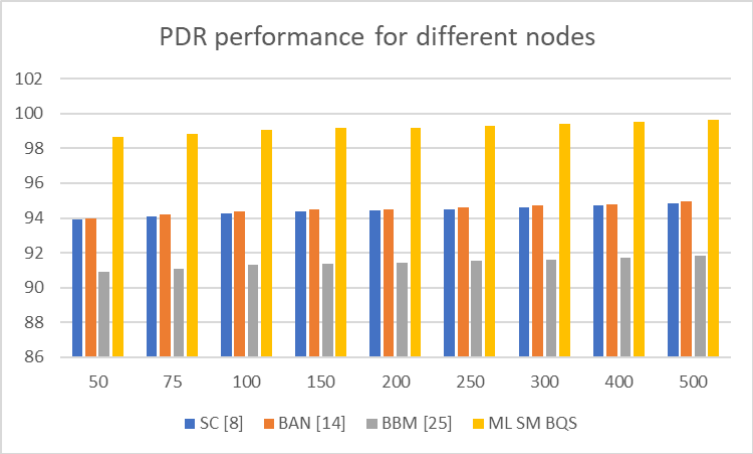


Fig. 6. PDR v/s Number of nodes

Due to this improvement in performance, the proposed model is capable of high QoS IoT Network deployments. Similar evaluated was done for the model under different types of attacks. This performance evaluation can be observed from the next section of this text.

## 4. Evaluation of Security Performance

The sidechain model is capable of removing wide variety of network attacks. To test it capabilities, QoS performance was observed under attack, and compared with QoS performance without attacks. To observe this, QoS evaluations were done for energy and delay performance, with-attack and without-attack. These metrics were tabulated in tables 6 through 13, by varying number of nodes and the following scenarios,

- MT – Masquerading attack with proposed model
- FT – Flooding attack with proposed model
- ST – Sybil attack with proposed model
- NT – Normal network with proposed model
- MA – Masquerading attack without proposed model
- FA – Flooding attackwithout proposed model
- SA – Sybil attackwithout proposed model
- NA – Normal network without attacks

Table 6. QoS Performance for 50 nodes

| Parameter | Delay (ms) | Energy (mJ) |
|---|---|---|
| MT | 0.18 | 64.48 |
| FT | 0.32 | 37.21 |
| ST | 0.24 | 28.44 |
| NT | 0.64 | 18.01 |
| MA | 0.27 | 593.21 |
| FA | 0.67 | 167.51 |
| SA | 0.91 | 629.35 |
| NA | 3.43 | 83.00 |

Reduction of end-to-end delay, and energy consumption can be observed, due to which network performance is improved, and overall QoS is enhanced. The same performance is observed for 100 nodes as follows,

Table 7. QoS Performance for 100 nodes

| Parameter | Delay | Energy |
|---|---|---|
| MT | 0.27 | 233.64 |
| FT | 0.48 | 930.70 |
| ST | 0.41 | 125.73 |
| NT | 0.70 | 157.41 |
| MA | 0.69 | 715.10 |
| FA | 0.35 | 3918.91 |
| SA | 0.50 | 1725.82 |
| NA | 0.18 | 70.59 |

From this performance evaluation, it can be observed that the proposed model requires lower energy, and lower energy when compared with similar attack scenarios. The performance of proposed model is almost similar to the performance of network without any attack, due to which it can be deployed for various attack detection and mitigation scenarios. Similar observations were done for 200 nodes, and were tabulated in table 8 as follows,

Table 8. QoS Performance for 200 nodes

| Parameter | Delay | Energy |
|---|---|---|
| MT | 0.38 | 953.67 |
| FT | 0.14 | 1265.81 |
| ST | 0.37 | 187.70 |
| NT | 0.55 | 852.89 |
| MA | 0.44 | 3233.41 |
| FA | 4.36 | 2261.42 |
| SA | 4.15 | 17.05 |
| NA | 0.43 | 82.47 |

From this performance evaluation, it can be observed that the proposed model requires lower energy, and lower energy when compared with similar attack scenarios. This is due to use of merging and splitting operations, which assist in better blockchain deployments. The performance of proposed model is almost similar to the performance of network without any attack, due to which it can be deployed for various attack detection and mitigation scenarios. Similar observations were done for 250 nodes, and were tabulated in table 9 as follows,

Table 9. QoS Performance for 250 nodes

| Parameter | Delay | Energy |
|---|---|---|
| MT | 2.37 | 29.36 |
| FT | 1.60 | 53.56 |
| ST | 0.54 | 711.42 |

| | | |
|---|---|---|
| NT | 2.65 | 45.70 |
| MA | 0.20 | 1163.41 |
| FA | 3.73 | 18.54 |
| SA | 2.60 | 27.39 |
| NA | 0.42 | 87.71 |

From this performance evaluation, it can be observed that the proposed model requires lower energy, and lower energy when compared with similar attack scenarios. This is due to use of merging and splitting operations, which assist in better blockchain deployments. The performance of proposed model is almost similar to the performance of network without any attack, due to which it can be deployed for various attack detection and mitigation scenarios. Similar observations were done for 300 nodes, and were tabulated in table 10 as follows,

Table 10. QoS Performance for 300 nodes

| Parameter | Delay | Energy |
|---|---|---|
| MT | 2.46 | 25.52 |
| FT | 3.27 | 927.98 |
| ST | 2.58 | 20.06 |
| NT | 1.40 | 451.35 |
| MA | 3.41 | 14.40 |
| FA | 2.63 | 22.90 |
| SA | 2.42 | 19.94 |
| NA | 2.66 | 96.82 |

From this performance evaluation, it can be observed that the proposed model requires lower energy, and lower energy when compared with similar attack scenarios. This is due to use of merging and splitting operations, which assist in better blockchain deployments. The performance of proposed model is almost similar to the performance of network without any attack, due to which it can be deployed for various attack detection and mitigation scenarios. Similar observations were done for 350 nodes, and were tabulated in table 11 as follows,

Table 11. QoS Performance for 350 nodes

| Parameter | Delay | Energy |
|---|---|---|
| MT | 3.31 | 9.24 |
| FT | 2.27 | 15.14 |
| ST | 3.95 | 8.12 |
| NT | 3.28 | 10.90 |
| MA | 2.42 | 41.93 |
| FA | 2.76 | 13.82 |
| SA | 2.63 | 13.76 |
| NA | 2.85 | 99.69 |

From this performance evaluation, it can be observed that the proposed model requires lower energy, and lower energy when compared with similar attack scenarios. This is due to use of merging and splitting operations, which assist in better blockchain deployments. The performance of proposed model is almost similar to the performance of network without any attack, due to which it can be deployed for various attack detection and mitigation scenarios. Similar observations were done for 500 nodes, and were tabulated in table 12 as follows,

Table 12. QoS Performance for 400 nodes

| Parameter | Delay | Energy |
|---|---|---|
| MT | 1.90 | 13.98 |
| FT | 2.10 | 23.42 |
| ST | 2.60 | 12.40 |
| NT | 3.33 | 14.00 |
| MA | 3.28 | 12.71 |
| FA | 2.39 | 13.37 |
| SA | 0.55 | 929.65 |
| NA | 2.30 | 108.50 |

From this performance evaluation, it can be observed that the proposed model requires lower energy, and lower energy when compared with similar attack scenarios. This is due to use of merging and splitting operations, which assist in better blockchain deployments. The performance of proposed model is almost similar to the performance of network without any attack, due to which it can be deployed for various attack detection and mitigation scenarios. Similar observations were done for 500 nodes, and were tabulated in table 13 as follows,

Table 13. QoS Performance for 500 nodes

| Parameter | Delay | Energy |
|---|---|---|
| MT | 2.89 | 8.73 |
| FT | 3.15 | 1.88 |
| ST | 2.91 | 7.21 |
| NT | 3.56 | 1267.47 |
| MA | 0.53 | 813.04 |
| FA | 2.39 | 13.37 |
| SA | 3.05 | 12.04 |
| NA | 28.41 | 12.01 |

Network performance for normal operating conditions (without attack, and without blockchain) match closely with conditions for attacks with proposed model. While network performance under attack without proposed blockchain model reduces exponentially, thereby showcasing the fact that the proposed model is able to improve network performance even under different attacks. This further indicates that the proposed network model is capable of countering different types of attacks with high efficiency for different network scenarios.

## 5. Discussion and Conclusion

The proposed model uses a combination of EHO with decision making process in order to improve QoS while enhancing network security performance. Due to which, the model is capable of application under different attack scenarios, while maintaining high QoS performance. The model showcases better performance when compared with various state-of-the art methods due to incorporation of end-to-end delay, energy requirement, throughput, packet delivery ratio (PDR), and security levels during node selection process. Such novelty in design is not yet proposed by other researchers, which assists in improving underlying model's performance. This performance was compared with various state-of-the-art models, and it was observed that, end-to-end delay has been reduced by 15.6% when compared with SC [8], 24.8% with compared with BAN [14] and 14.9% when compared with BBM [25] models, while, energy consumption has been reduced by 16.8% when compared with SC [8], 26.5% with compared with BAN [14] and 15.2% when compared with BBM [25] models. Similar improvements were observed for PDR, & throughput performance under different network scenarios. Due to which the model is suited for high QoS deployments. The model was also evaluated in terms of delay & energy under different attack scenarios, and it was observed that performance of the model did not change even under attacks. Due to which the model is capable of mitigating various attacks, for moderate to dense networks. In future, researchers can integrate deep learning for model sidechain selection, which will assist in better chain splitting, and thus further improve QoS & security performance. Moreover, researchers can validate this performance under a greater number of attacks, which will allow them to validate model performance under real-time scenarios.

## References

[1] Liu, Guangyi, enDajie Jiang. "5G: Vision and Requirements for Mobile Communication System towards Year 2020". Chinese Journal of Engineering 2016 (2016): 1–8. Web.N.p., n.d. Web. 2 Mrt 2022.
[2] Jesus, Emanuel Ferreira et al. "A survey of how to use Blockchain to secure Internet of Things and the stalker attack". Security and communication networks 2018 (2018): 1–27. Web.
[3] Singh, Rajeev, Sudeep Tanwar, enTeekParval Sharma. "Utilization of Blockchain for Mitigating the Distributed Denial of Service Attacks". Security and privacy 3.3 (2020): n. pag. Web.
[4] Li, Min et al. "A sidechain-based decentralized authentication scheme via optimized two-way peg protocol for smart community". IEEE Open Journal of the Communications Society 1 (2020): 282–292. Web.
[5] Xu, Hao et al. "RAFT based wireless blockchain networks in the presence of malicious jamming". IEEE wireless communications letters 9.6 (2020): 817–821. Web.
[6] Lee, Gilsoo et al. "Performance analysis of blockchain systems with wireless mobile miners". IEEE Networking Letters 2.3 (2020): 111–115. Web.
[7] Cao, Bin et al. "How does CSMA/CA affect the performance and security in wireless blockchain networks". IEEE transactions on industrial informatics 16.6 (2020): 4270–4280. Web.
[8] Guo, Fengxian et al. "Adaptive resource allocation in future wireless networks with blockchain and mobile edge computing". IEEE transactions on wireless communications 19.3 (2020): 1689–1703. Web.

[9] Tangsen, Huang, Xiaowu Li, enXiangdong Ying. “A blockchain-based node selection algorithm in cognitive wireless networks”. IEEE access: practical innovations, open solutions 8 (2020): 207156–207166. Web.
[10] Liu, Ziming et al. “A blockchain-enabled secure power trading mechanism for smart grid employing wireless networks”. IEEE access: practical innovations, open solutions 8 (2020): 177745–177756. Web.
[11] She, Wei et al. “Blockchain trust model for malicious node detection in wireless sensor networks”. IEEE access: practical innovations, open solutions 7 (2019): 38947–38956. Web.
[12] W. She, Q. Liu, Z. Tian, J. -S. Chen, B. Wang and W. Liu, “Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks,” in *IEEE Access*, vol. 7, pp. 38947-38956, 2019.
[13] Cui, Zhihua et al. “A hybrid BlockChain-based identity authentication scheme for multi-WSN”. IEEE transactions on services computing (2020): 1–1. Web.
[14] Y. Liu, F. R. Yu, X. Li, H. Ji and V. C. M. Leung, “Decentralized Resource Allocation for Video Transcoding and Delivery in Blockchain-Based System With Mobile Edge Computing,” in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11169-11185, Nov. 2019.
[15] Nguyen, Dinh C. et al. “Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning”. IEEE transactions on network and service management 17.4 (2020): 2536–2549. Web.
[16] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung and M. Song, “Computation Offloading and Content Caching in Wireless Blockchain Networks With Mobile Edge Computing,” in *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11008-11021, Nov. 2018.
[17] Fan, Xin, en Yan Huo. “Blockchain based dynamic spectrum access of non-real-time data in cyber-physical-social systems”. IEEE access: practical innovations, open solutions 8 (2020): 64486–64498. Web.
[18] Danzi, Pietro et al. “Delay and communication tradeoffs for blockchain systems with lightweight IoT clients”. IEEE internet of things journal 6.2 (2019): 2354–2365. Web.
[19] Xiao, Lijun et al. “A secure framework for data sharing in private blockchain-based WBANs”. IEEE access: practical innovations, open solutions 8 (2020): 153956–153968. Web.
[20] Zhao, Ning, Hao Wu, enYali Chen. “Coalition game-based computation resource allocation for wireless blockchain networks”. IEEE internet of things journal 6.5 (2019): 8507–8518. Web.
[21] Chen, Tianrui et al. “Blockchain secured auction-based user offloading in heterogeneous wireless networks”. IEEE wireless communications letters 9.8 (2020): 1141–1145. Web.
[22] Kumar, Tanesh et al. “BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks”. IEEE access: practical innovations, open solutions 8 (2020): 154166–154185. Web.
[23] Ling, Xintong et al. “Blockchain radio access network (B-RAN): Towards decentralized secure radio access paradigm”. IEEE access: practical innovations, open solutions 7 (2019): 9714–9723. Web.
[24] Alrubei, Subhi M. et al. “Latency and performance analyses of real-world wireless IoT-blockchain application”. IEEE sensors journal 20.13 (2020): 7372–7383. Web.
[25] Yang, Zhe et al. “Blockchain-based decentralized trust management in vehicular networks”. IEEE internet of things journal 6.2 (2019): 1495–1505. Web.
[26] Gao, Shiyao et al. “An anti-quantum E-voting protocol in blockchain with audit function”. IEEE access: practical innovations, open solutions 7 (2019): 115304–115316. Web.
[27] Kang, Jiawen et al. “Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks”. IEEE wireless communications letters 8.1 (2019): 157–160. Web.
[28] Sun, Wen et al. “Joint resource allocation and incentive design for blockchain-based mobile edge computing”. IEEE transactions on wireless communications 19.9 (2020): 6050–6064. Web.
[29] Huang, Dongyan, Xiaoli Ma, enShengli Zhang. “Performance analysis of the raft consensus algorithm for private blockchains”. IEEE transactions on systems, man, and cybernetics. Systems 50.1 (2020): 172–181. Web.
[30] Liu, Yiming et al. “Blockchain and machine learning for communications and networking systems”. IEEE Communications Surveys & Tutorials 22.2 (2020): 1392–1431. Web.
[31] Sidorov, Michail et al. “A public blockchain-enabled wireless LoRa sensor node for easy continuous unattended health monitoring of bolted joints: Implementation and evaluation”. IEEE sensors journal 20.21 (2020): 13057–13065. Web.
[32] Zheng, Shuang et al. “Smart contract-based spectrum sharing transactions for multi-operators wireless communication networks”. IEEE access: practical innovations, open solutions 8 (2020): 88547–88557. Web.
[33] Wang, Yuntao, Zhou Su, en Ning Zhang. “BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network”. IEEE transactions on industrial informatics 15.6 (2019): 3620–3631. Web.
[34] Liu, Mengting et al. “A deep reinforcement learning-based transcoder selection framework for blockchain-enabled wireless D2D transcoding”. IEEE transactions on communications 68.6 (2020): 3426–3439. Web.
[35] Mousumi Mitra, Aviroop Chowdhury, " A Modernized Voting System Using Fuzzy Logic and Blockchain Technology", International Journal of Modern Education and Computer Science(IJMECS), Vol.12, No.3, pp. 17-25, 2020.DOI: 10.5815/ijmecs.2020.03.03.
[36] Dipti Pawade, Avani Sakhapara, Raj shah, Siby Thampi, Vignesh Vaidya. " Blockchain Based Secure Traffic Police Assistant System ", International Journal of Education and Management Engineering (IJEME), Vol.10, No.6, pp.34-41, 2020. DOI: 10.5815/ijeme.2020.06.05.
[37] Siddhartha Sen, Sripati Mukhopadhyay, Sunil Karforma, " A Blockchain based Framework for Property Registration System in E-Governance", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.13, No.4, pp. 30-46, 2021. DOI: 10.5815/ijieeb.2021.04.03

## Authors' Profiles

**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 AI-ML.

**How to cite this paper:** Shital Agrawal, Shailesh Kumar, " MLSMBQS: Design of a Machine Learning Based Split & Merge Blockchain Model for QoS-Aware Secure IoT Deployments", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.14, No.5, pp. 58-71, 2022. DOI:10.5815/ijigsp.2022.05.05