International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2022/215921 Volume 9, Issue 5, September – October (2022)

RESEARCH ARTICLE

QSIH: Design of a Novel QoS-Aware Sidechain-Based IoT Network Design for Secure Healthcare Deployments

Pooja Mishra
Department of Computer Science and Engineering, Oriental University, Indore, Madhya Pradesh, India.
pooja26.mishra@gmail.com

Sandeep Malik
Department of Computer Science and Engineering, Oriental University, Indore, Madhya Pradesh, India.
sandeepmalik@orientaluniversity.in

Received: 17 August 2022 / Revised: 11October 2022 / Accepted: 15 October 2022 / Published: 30 October 2022

Abstract – Internet of Medical Things (IoMT) are networks which are targeted towards design of healthcare communication interfaces with low latency and high security. In order to design such interfaces, efficient models for data encryption, hashing, privacy, and quality of service (QoS) awareness are needed. A wide variety of standard medical interfaces are proposed by researchers, which assist in reducing network redundancies for high-throughput and low latency communications. These interfaces also implement security models that ensure data encryption & privacy. But due to incorporation of encryption methods, QoS performance of the IoMT devices reduces, which limits their real-time usability for in-patient monitoring & treatment. In order to improve IoMT QoS while maintaining high security, this text proposes design of QSIH, which is a QoS-aware sidechain model that can be used for securing IoMT networks. The proposed model describes design of a blockchain-based data storage & communication interface, which is capable of removing a wide variety of network attacks. The delay needed for communication in any blockchain-based interface increases exponentially w.r.t. number of blocks added to the system. In order to reduce this delay, a novel machine learning model based on Genetic Algorithm optimization is proposed. The proposed model splits the main blockchain into multiple shards in a QoS-aware manner, thereby ensuring low delay, and high communication throughput. The shards (or sidechains) are managed using an interactive Q-Learning (IQL), which is able to expand or contract these chains depending upon network's QoS performance. Sidechains which are unused for large periods of time are combined together, and archived for future reference. The archived sidechains are formed from main blockchain, and are merged with other sidechains depending upon archival requirements of the network. Due to such a dynamic side chaining model, the proposed QSIH model is capable of reducing network communication delay by 18%, increase throughput by 14%, reduce storage cost by 5%, while maintaining high level of security & privacy in the network. The model was tested under different IoMT scenarios, and it was observed that it showcased consistent performance across different network emulations.

Index Terms – IoMT, Healthcare, Blockchain, Machine Learning, Sidechain, Optimization, QoS.

1. INTRODUCTION

In order to perform high speed, high accuracy, and high performance IoT based health care monitoring, the designed devices must follow certain principles. These principles include high precision monitoring, effective analysis, and efficient control. A large number of algorithms have been proposed for performing these tasks, and each of the algorithms have their own nuances, advantages, and limitations. But in order to understand the process of data flow in healthcare IoT, it is necessary that IoT components like sensors, storage devices, analytical processing algorithms, cloud deployments, and actuation points must be carefully studied. The flow of a typical healthcare IoT model [1], that includes sensors, storage devices, analytical processing units, cloud interface and actuating entities (Doctors) can be observed from figure 1, wherein flow of data from devices to storage, and back to reporting can be observed. Any healthcare IoT system works in the following steps,

- Data capturing from wearable and non-wearable devices, wherein data from ECG sensors, blood pressure sensors, oxygen monitors, and temperature monitors, etc. is captured and stored into a unified format. This data is then given to the cloud for further processing. There are 2 main responsibilities of every data capture IoT healthcare device.
    - Reduce any reading errors during data capturing, which is done via pre-processing algorithms like adaptive median filtering, averaging, etc.

- Store the data in a format which is transmittable, understandable, and secure, which is done via the use of data storage standard like extensible markup language (XML), Java simple object notation (JSON), etc. Models like encryption, hashing, data framing, secret sharing, etc. are used for the purpose of securing the data from both internal and external threats.

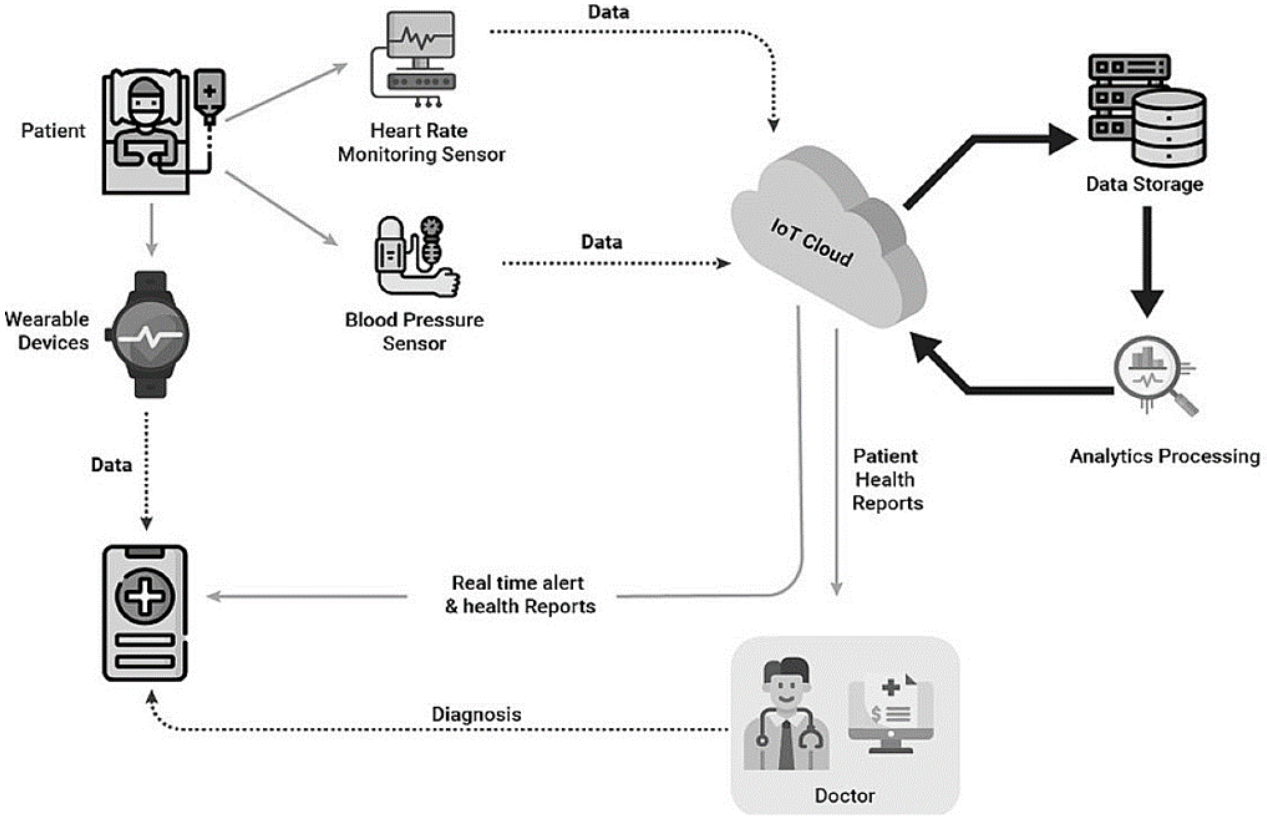

Figure 1 A Typical Healthcare IoT Data Flow

- Data from the capture devices is given to an IoT cloud layer, wherein it is segregated for storage. The storage unit requires this data to be either in the form of rows & columns, or in the form of structured files. Some IoT cloud deployments like Azure and Google cloud accept data in unstructured form, but then convert the data into their internal proprietary format, which helps them to effectively retrieve this data via indexing whenever required. Databases like MySQL (Structured Query Language), Firebase, Microsoft SQL, etc. are used for this purpose.
- Data from these databases given to an analytical processing unit, wherein online analytical processing algorithms (OLAP) [1] like aggregation, partitioning, data cube processing, etc. are used. These algorithms allow healthcare IoT data to be inferred via temporal analysis, which assists in analysis of patient's previous and current conditions and predicts in case of any future complications. This is one of the most important blocks in the system, as the accuracy of this block decides action plans which will be taken up by doctors for improving patient's health. Deep learning algorithms like convolutional neural networks (CNNs), Q-Learning, Support Vector Machine (SVM), etc. are used for this purpose.
- The processed data is given back to the cloud, from here Doctor's device & healthcare centre's devices are informed about patient conditions. Based on this inference, reports are generated, and action plans are chalked out. In order to provide high quality reports, algorithms [2] like labelling, categorization, clustering, etc. are used. These algorithms provide effective ways in which data can be represented in the system, such that overall experience & efficiency of data visualization can be improved.
- Based on these reports further processing is done, such that the patient's health condition can be improved. This process runs in a loop, and the system efficiency is evaluated after each report. Based on this efficiency, corrective actions are taken such that there are visual improvements in the patient's health.

1.1. Motivation

In order to design an effective healthcare IoT system, it is necessary that each of the described individual blocks be designed with highest efficiency. An architecture to design these blocks with high efficiency and to improve the effectiveness of the existing deployed healthcare IoT blocks is mentioned in this text. Based on this review, it was observed that Internet of Medical Things (IoMT) are networks which are targeted towards design of healthcare communication interfaces with low latency and high security. In order to design such interfaces, efficient models for data encryption, hashing, privacy, and quality of service (QoS) awareness are needed. A wide variety of standard medical interfaces are proposed by researchers, which assist in reducing network redundancies for high-throughput and low latency communications. These interfaces also implement security models that ensure data encryption & privacy. But due to incorporation of encryption methods, QoS performance of the IoMT devices reduces, which limits their real-time usability for in-patient monitoring & treatment. Thus, the motivation of this text is to improve IoMT QoS while maintaining high security, this text proposes design of QSIH, which is a QoS-aware sidechain model that can be used for securing IoMT networks.

1.2. Contributions

The following are probable contributions of this text,

1. Design of a side chain model for securing healthcare deployments
2. Incorporation of QoS-awareness in the sidechain-based IoT network design
3. Improved security due to integration of blockchains for secure healthcare deployments

1.3. Paper Structure

In order to design the proposed system, it is necessary to review and analyze already existing healthcare IoT systems [2, 3, 4] w.r.t. their nuances, advantages, and drawbacks. The next section does this task by reviewing some of the recent IoT deployment models, and evaluates their effectiveness in terms of accuracy of decision making, response time, application area, etc. This is followed by design of the proposed architecture, and its result evaluation. Finally, this chapter concludes with some interesting observations about the proposed architecture and recommends methods to improve it.

2. LITERATURE REVIEW

Researchers have presented a diverse assortment of models for blockchains, and each of these models has its own features in terms of the performance and operational measurements they use. For instance, the research presented in [5, 6] suggests using a variety of different consensus models for blockchain, in addition to Software Defined Network (SDN) for low delay, reliable, and secure model with powerful emergency handling capabilities (LSRDM-EH), which can be used for real-time deployments. Because these models use approaches of a high complexity when creating healthcare applications, they are not capable of being scaled up for usage in large-scale deployments. Automation in Procurement Contracts (APC) is proposed as a solution to this constraint in the research published in [7], which suggests its usage for improved blockchain performance in large-scale application situations. The model makes use of smart contracts and automates the procedures for updating them by making use of low-complexity decision making methods. Researchers have suggested similar models in [8, 9, and 10], where they explore the usage of Consortium Blockchains, Edge Computing with Blockchains (ECB), and Attribute-Based Searchable Encryption for Blockchain-based Search Applications (ABSE2). These models contribute to the enhancement of storage capacities for a variety of healthcare applications via the use of data augmentation and redundancy control. Extensions to these models are discussed that make use of Blockchain Logging Contracts (BLCs) [11], permissioned blockchains with security risk management (SRM) [12], Lattices-based Cryptography with Deep Learning (LCDL) [13], and use of Machine Learning (ML) blockchains [14], all of which assist in improving quality of service and security performance under a variety of attack types. These models increase QoS performance in response to a variety of attack types by using high density feature extraction and classification approaches.

Methods that help improve resistance to various types of network assaults are also studied by researchers. These methods are considered in conjunction with methods that aid in the increase of security levels while retaining context-aware performance. These models are explored in [15, 16, and 17], whereby the usage of Software-Defined Infrastructure for blockchains, Patient-Centric Blockchains, and confidential group transactions, which aid in boosting performance under a variety of various use cases, are mentioned. Researchers have come up with similar models that make use of Autonomous Encryption-Decryption (AED) [18], Blockchain based Edge Computing (BEC) [19], and Hybrid Cryptography by making use of Elliptic Curve Cryptography (ECC) and Edwards-Curve Digital Signature Algorithm (EdDSA) [20]. However, these models use very complicated encryption and processing techniques, which restricts their scalability performance when applied for a variety of hospitals. Work in [21], [22], and [23] propose the use of Ring Signature and Stealth Address (RSSA), Decoupled Processing, and multilayer models for the incorporation of scalability-aware methods that can be optimized with regard to the number of block requests. These are some of the ways that this performance could be improved. These models are further expanded by the usage of scalable blockchains [24] and fortified blockchains (FBs) [25], both of which help in combining privacy preservation in addition to fine-tuned access control for various applications.

2.1. Need of the Proposed Model

Based on the review, it can be observed that these models involve highly complex encryption algorithms, which lower the quality of service that may be achieved by IoMT devices. Moreover, these models also showcase lower QoS under attacks, due to which the next section presents design of the proposed model which is a novel QoS-aware sidechain-based Internet of Things network architecture as a potential solution to this problem. This design is intended for use in secure healthcare installations. The model was evaluated using a variety of use cases, and its quality of service and security levels were analyzed, then compared to a variety of methodologies that are considered to be state-of-the-art techniques.

3. DESIGN OF THE PROPOSED NOVEL QOS-AWARE SIDECHAIN-BASED IOT NETWORK DESIGN FOR SECURE HEALTHCARE DEPLOYMENTS

From the literature review, it can be observed that existing security models for IoT based healthcare deployments incorporate complex encryption methods, which reduce QoS performance of IoMT devices. Due to which their real-time usability is reduced for in-patient monitoring & treatment applications. In order to overcome this limitation, this section proposes design of a QoS-aware sidechaining model which can be used for highly scalable healthcare deployments. To perform this task, a Novel Machine Learning Model (MLM) that uses Genetic Algorithm for splitting the main blockchain into multiple shards. These shards incorporate QoS-awareness into the model and thereby ensure low delay, and high communication throughput. Overall flow of the model is described in figure 2, wherein it can be observed that the shards (or sidechains) are managed via an interactive Q-Learning (IQL) method, which enables splitting & combining operations on the chains. Combination or archiving operations are performed on the sidechains depending upon their temporal utility. While splitting operations are performed depending upon current QoS performance of the network deployment. Thus, the GA Model aims at integrating better security and higher QoS levels for healthcare deployments, while IQL Model assists in incrementally improving QoS-awareness while reducing attack probability for different request types. Both the models Design of the full model is segregated into different sub modules, and each of these modules are described in different sub-sections of this text. Researchers can refer these sections to design the model is part(s) or as a whole, depending upon their network requirements.

3.1. Design of the GA Model for QoS & Security Aware Healthcare Deployments

All requests for data storage are processed by a GA based Model, which evaluates current blockchain configurations, and selects a sidechain for storage purposes. The block structure used for this purpose can be observed from figure 3 as follows,

Previous Hash	Sensor Details	Sensor Values	Patient Details	Timestamp
Doctor Details	Sidechain Number	Sidechain Meta Data	Nonce	Current Hash

Figure 3 Block Structure Used for Storing Patient Information

From this figure, it can be observed that each block stores the following information,

- Hash of previous block, which is used to incorporate traceability and transparency characteristics
- Sensor details & Sensor value, which assists in identification of sensor type, sensed value, and other sensor-specific parameters.
- Patient details, which consists of Name, Address, Contact Details, etc., that can be used to uniquely identify the patients
- Timestamp stores current time information for temporal analysis
- Doctor Detail, consists of Name, Address, Specialization, Contact Details, etc., that can be used to uniquely identify the doctors
- Sidechain Number, which consists of sidechain ID, that is used to recognize current sidechain from a series of other chains
- Sidechain Meta Data stores information about the sidechain that includes, number of blocks, aggregation criteria, etc.
- Nonce is a stochastic number which is used to uniquely identify blockchain hashes
- Current Hash stores hash of the current block, and is used to incorporate immutability in deployed blockchains.

Every block addition request is processed using Proof of Work (PoW) based consensus, which assists in simplifying the mining process. The PoW Model requires evaluation of unique hashes that follow a certain set of rules. The proposed GA Model aims minimizing delay needed during mining operations, and is evaluated for each batch of N_{batch} block addition requests. The model works via the following process,

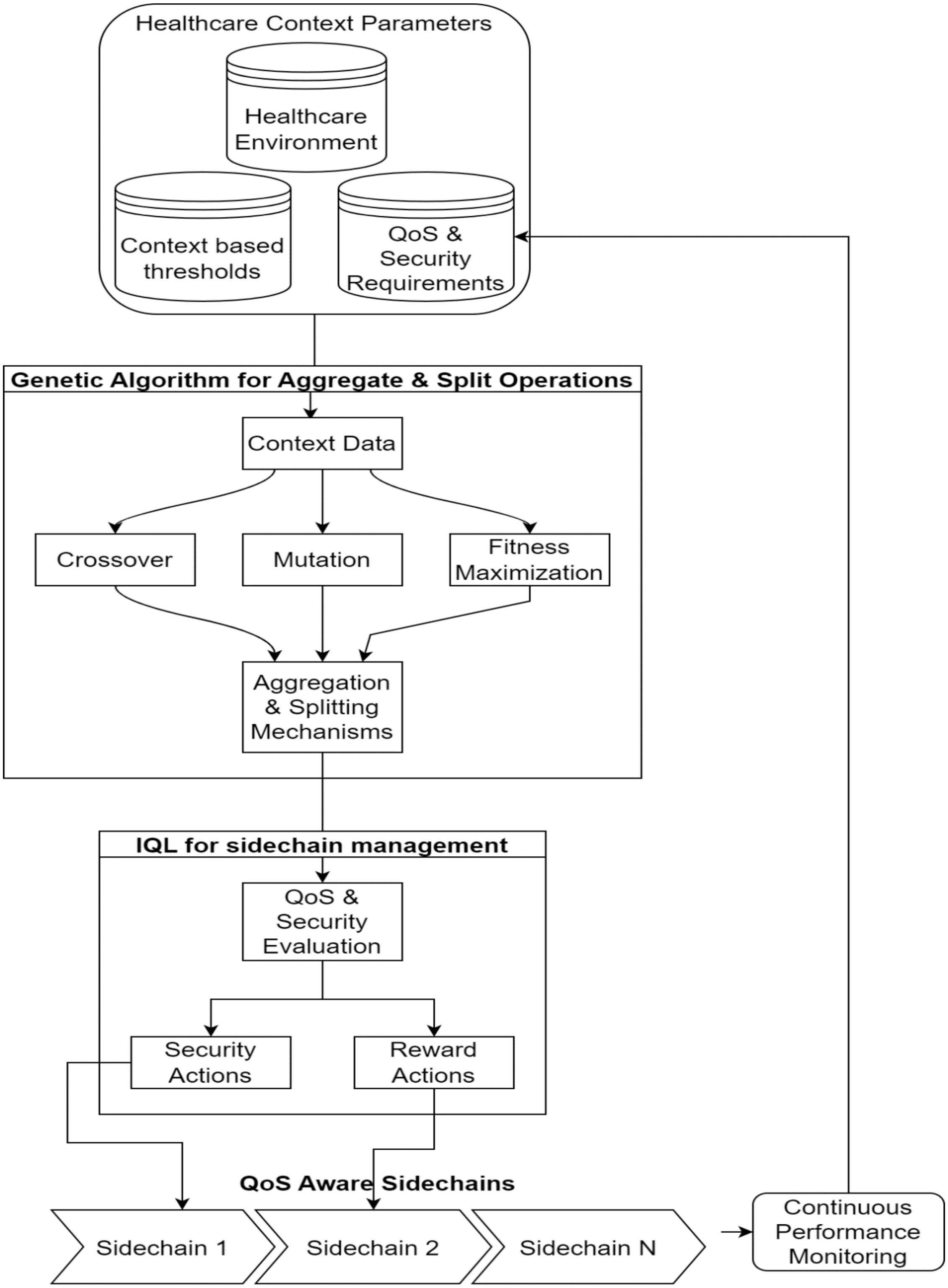
Healthcare Context Parameters
Healthcare Environment
Context based thresholds
QoS & Security Requirements
Genetic Algorithm for Aggregate & Split Operations
Context Data
Crossover
Mutation
Fitness Maximization
Aggregation & Splitting Mechanisms
IQL for sidechain management
QoS & Security Evaluation
Security Actions
Reward Actions
QoS Aware Sidechains
Sidechain 1
Sidechain 2
Sidechain N
Continuous Performance Monitoring

Figure 2 Overall Flow of the Proposed Model

- Initialize the following GA Parameters,
    - Total iterations to be used for validation (N_i)
    - Total solutions to be generated for optimization (N_s)
    - Learning rate for deciding crossover & mutation operations (L_r)
    - Current number of sidechains (N_{sc})
    - Length of each sidechain (L_{sc})
- Initially mark all solutions as 'to be mutated'
- For each iteration between 1 to N_i, perform the following tasks,
    - For each solution between 1 to N_s, evaluate sidechains via the following process,
        - If current solution is marked as 'not to be mutated', then skip it and move to the next solution in sequence
        - Else, generate a new solution via the following process,
- Stochastically select a sidechain via equation 1,

$$Sel_{sc} = STOCH(1, N_{sc}) \dots (1)$$

Where, Sel_{sc} represents selected sidechain, while STOCH generates a stochastic number between the given ranges.

- Add the current blocks to this sidechain, and evaluate its fitness via equation 2 as follows,

$$f_i = \frac{L_{sc}}{Max(\cup L_{sc}) * N_{batch}} \sum_{j=1}^{N_{batch}} \frac{D_j}{Max(D)} + \frac{E_j}{Max(E)} + \frac{Max(T)}{T_j} + \frac{100}{PDR_i} \dots (2)$$

Where, D, E, PDR, T represents end-to-end delay, energy consumption, packet delivery ratio, and throughput, which is calculated via equations 3, 4, 5 and 6 as follows,

$$D = t_{end} - t_{start} \dots (3)$$

$$E = RE_{start} - RE_{end} \dots (4)$$

$$T = \frac{P_{rx}}{D} \dots (5)$$

$$PDR = \frac{P_{rx}}{P_{tx}} \dots (6)$$

Where, $t_{end} t_{start}$ represent finishing & starting timestamps for block addition requests, while, RE, P_{rx}, P_{tx} represents residual energy, reception energy, and transmission energy levels for different bock addition requests.

- Based on this evaluation, fitness levels are calculated for different solutions.
    - Repeat this process for all solutions, and evaluate an iteration fitness threshold via equation 7 as follows,

$$f_{th} = \sum_{i=1}^{N_s} f_i * \frac{L_r}{N_s} \dots (7)$$

-
    - Mark solution as 'to be mutated', if $f_i \geq f_{th}$, else mark it as 'not to be mutated'
- Repeat this process for all iterations

At the end of final iteration, identify solution with minimum fitness, and select it as a probable candidate for adding blocks. Now perform Man in the Middle (MITM), Sybil, and Distributed Denial of Service (DDoS) attacks on selected chain, and estimate its fitness levels. Based on the obtained fitness levels, evaluate the following process,

- If $f_{attack} \leq \frac{f_{normal}}{L_r}$, then, the blockchain's security performance is fine, and it can be used without split or aggregation operations.
- Else, blockchain either needs to be split or aggregated with other chains, which is done via the following process,
    - If $f_{attack} \geq \frac{f_{normal}}{2 * L_r}$, then split the blockchain into 2 equal parts, and store blocks into the chain with lower length
    - Else, aggregate current sidechain with another sidechain with lower length, and use this long length chain for addition of blocks

Using this process, blocks are added either to an existing sidechain, a new smaller length sidechain, or an aggregated larger length sidechain, which assists in improving both QoS & security performance under different real-time network deployments. This performance is further improved via use of an IQL Model that continuously monitors existing QoS & security levels, and decides whether to split or aggregate the chains. Design of this model is discussed in the next section of this text.

3.2. Design of the IQL Model for Incrementally Improving QoS-Awareness While Maintaining Better Security Performance

After adding block to a selected sidechain, an IQL Model is used for continuous performance & QoS monitoring, which assists in improving its real-time deployment capabilities. The model evaluates a reward function via equation 8, which is calculated for consecutive block addition requests. It uses fitness values from the GA Model for continuous performance optimizations,

$$r = \frac{f(New) - f(Old)}{\partial} - \emptyset * Max[\cup f] + f(Old) \ldots (8)$$

Where, $f(New) f(Old)$ represents new & old fitness values, while $\partial\emptyset$ represents learning rate of the model, and a discount factor, which assists in continuous optimization of QoS performance. If the value of $r > 1$, then QoS levels for current sidechain configuration is reducing, thus current sidechain is split into 2 parts, and the smaller sidechain is used for addition of blocks. Otherwise, current configuration is optimum, and doesn't need any split operations. Due to which, the model is capable of high-speed, low energy, high throughput, high PDR and better security performance. This performance is evaluated in the next section, and compared with various state-of-the-art models, which assists in validating its real-time deployment capabilities.

4. RESULT ANALYSIS AND COMPARISON

It has been determined, based on the work that has been provided, that the QSIH model combines quality of service awareness with security awareness for a variety of distinct real-time use cases. The model was trained for Sybil, DDoS, and MITM assaults; hence, it is capable of decreasing the impact of these attacks under various hospital management situations since it was trained for these attacks. In order to assess the validity of these assertions, the QSIH model that was developed was contrasted with the mainstream blockchain-based healthcare deployments described in LSR DM EH [6], LCDL [13], and BEC [19].

In order to get an accurate assessment of how well these healthcare deployments work, they are tested in a variety of environments and under a variety of threats. The number of patient-to-doctor interactions was changed linearly between 500 and 5000, and the same nodes were utilized for communication throughout each run. This was done on the basis of typical network settings.

The likelihood of attacker nodes was changed between 5% and 25% for the purpose of validating the performance of the security system under Sybil, Distributed Denial of Service (DDoS), and Man in the Middle (MITM) attack types. In the course of these assaults, the typical levels of quality of service were measured and analyzed in terms of energy consumption (E), packet delivery ratio (PDR), end-to-end communication delay (D), and throughput (T).

This performance is considered in relation to the following: In part 4.1, we cover QoS performance without any kind of assault. In section 4.2, we cover QoS performance when under attack, which helps with calculating QoS levels for a variety of network topologies.

4.1. QoS Performance for Different Healthcare Deployments

The performance of the proposed QSIH model is better when compared with the performance of the LSR DM EH [6], LCDL [13], and BEC [19] models. This is because QoS-awareness is included during trust-based routing. This performance is assessed by changing the number of patients from 100 to 500, and also by measuring the QoS values for a variety of patient-to-doctor communication volumes (NPTDC). The following table 1 showcases the simulation environment for validation of the proposed model under real-time scenarios,

Table 1 Simulation Parameters Used for Validation of the Proposed Model Sets

Network Parameter	Parameter Value
Propagation Model	Two Ray Ground
MAC	802.16
Interface queue type	Priority Queue
Number of nodes	40 – 100
Routing Protocol	AOMDV
Network Size	200 m x 200 m
Idle Power	0.5 mW
Reception Power	1 mW
Transmission Power	2 mW
Sleep Power	0.0001 mW
Transition Power	0.3 mW
Transition Time	0.008 s
Initial Node Energy	200 mW

Table 2 Average End-to-End Delay for Different Blockchain Communications

No. of Patients				100, 250, 500
NPTDC	D (ms) LSR DM EH [6]	D (ms) LCDL [13]	D (ms) BEC [19]	D (ms) Proposed
500	0.90	1.01	1.10	0.79
600	0.97	1.08	1.18	0.84
700	1.03	1.14	1.24	0.89
800	1.07	1.20	1.30	0.93

900	1.13	1.26	1.39	1.00
1000	1.20	1.40	1.58	1.16
1250	1.36	1.72	1.96	1.45
1500	1.78	2.19	2.46	1.80
2000	2.23	2.64	2.90	2.10
2250	2.60	2.95	3.24	2.34
2500	2.81	3.26	3.59	2.60

After simulating the network parameters for each transmission, the results are then averaged to arrive at an approximation of the final quality of service values. This procedure of averaging provides for accurate assessment of the performance of the underlying model, and it facilitates in comparing the performance of this model to that of typical models used in secure hospitals. The values for end-to-end delay (D), when combined for 100, 250, and 500 patients, are reported in table 2.

It can be seen from this evaluation and figure 4 that the proposed model has a delay that is 10.4 percentage points lower than LSR DM EH [6], 15.5 percentage points lower than LCDL [13], and 18.5 percentage points lower than BEC [19]. This is because delay-aware mining operations were utilized to create the model. These activities help improve the quality-of-service levels of the proposed model, which ultimately results in an improvement in the model's overall performance across a variety of deployment circumstances. Similar observations are made for the patients' energy performance, and the combined results for 100, 250, and 500 patients are summarized in table 3.

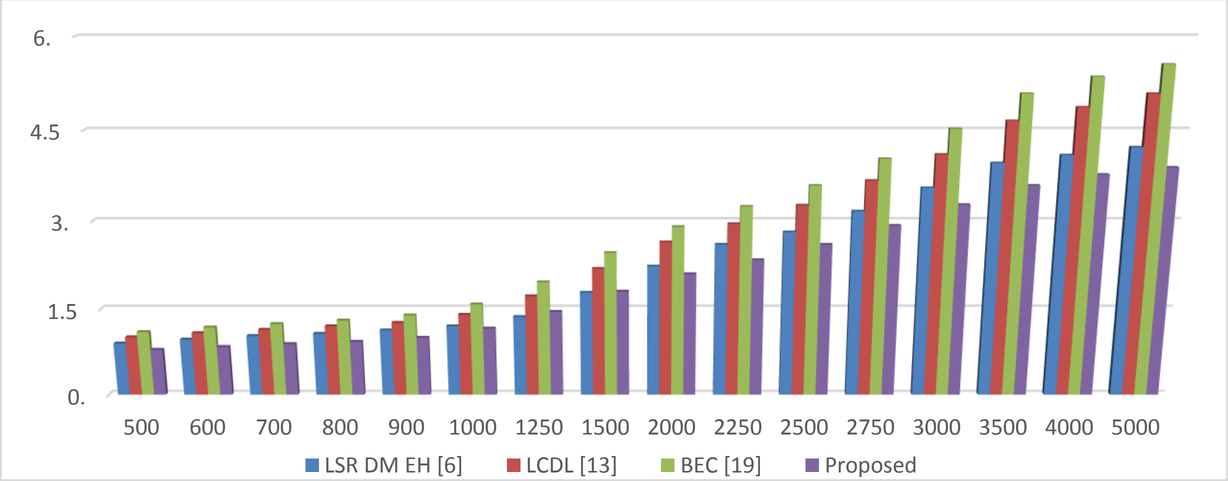

Figure 4 Average End-to-End Delay for Different Blockchain Communications

Table 3 Average Energy Consumption for Different Blockchain Communications

No.	of	Patients		100, 250, 500
NPTDC	E (mJ) LSR DM EH [6]	E (mJ) LCDL [13]	E (mJ) BEC [19]	E (mJ) Proposed
500	2.10	3.30	2.95	2.18
600	2.45	3.63	3.20	2.35
700	2.54	3.82	3.38	2.49
800	2.72	4.05	3.58	2.63

Because of the use of energy-aware mining and sidechain selection operations, the proposed model has 4.9% less energy consumption than the LSR DM EH [6], 10.5% less energy consumption than the LCDL [13], and 8.3% less energy consumption than the BEC [19]. This can be seen based on this evaluation, as well as figure 5, where it can be seen that the proposed model has these numbers under different scenarios. This helps to improve the quality-of-service levels of the proposed model, which ultimately boosts the model's overall performance across a variety of deployment circumstances. Similar findings are made about the throughput performance, which, when combined for 100, 250, and 500 patients, may be viewed as follows from table 4.

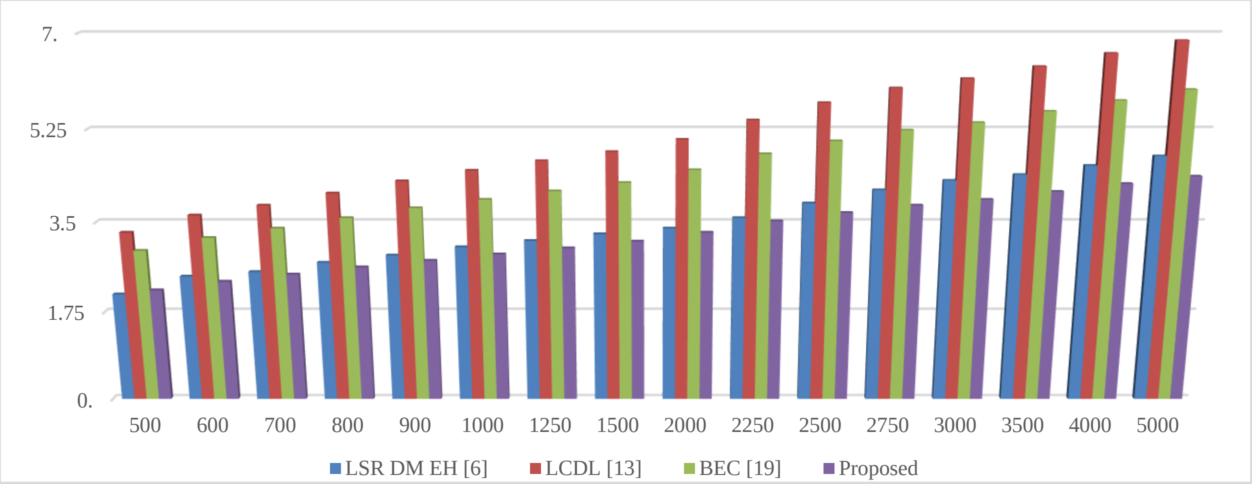

Figure 5 Average Energy Consumption for Different Blockchain Communications

Table 4 Average Throughput for Different Blockchain Communications

No.	of	Patients		100, 250, 500
NPTDC	T (kbps) LSR DM EH [6]	T (kbps) LCDL [13]	T (kbps) BEC [19]	T (kbps) Proposed
500	287.36	299.95	346.90	349.73
600	290.05	302.35	349.60	352.46
700	291.94	304.61	352.30	355.30
800	294.36	307.30	355.40	358.46
900	297.13	310.03	358.55	361.58
1000	299.64	312.62	361.60	364.61
1250	302.15	315.22	364.66	367.63
1500	304.66	317.81	367.66	370.66

2000	307.16	320.40	370.66	373.68
2250	309.67	322.99	373.66	376.70
2500	312.18	325.63	376.66	379.73
2750	314.69	328.27	379.66	382.75
3000	317.20	330.91	382.66	385.78
3500	319.70	333.46	385.63	388.77
4000	322.21	336.01	388.60	391.76
5000	324.72	338.56	391.57	394.74

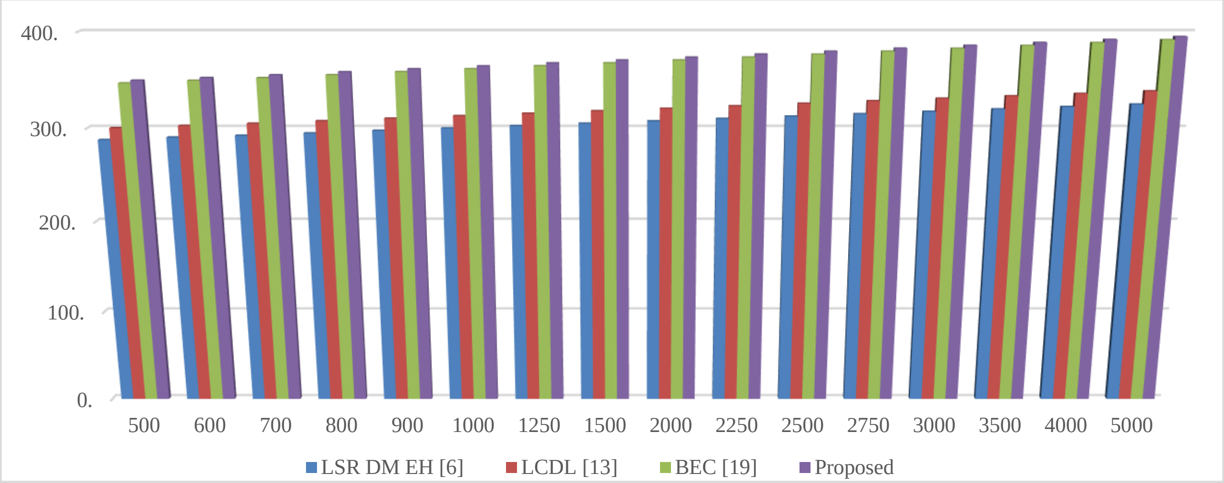

Figure 6 Average Throughput for Different Blockchain Communications

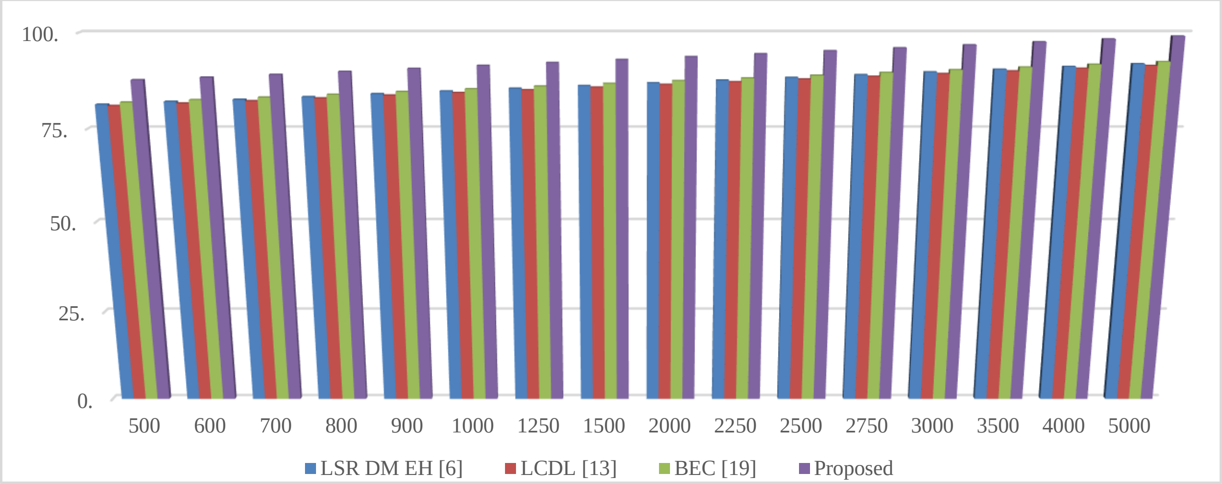

Figure 7 Average PDR for Different Blockchain Communications

Table 5 Average PDR for Different Blockchain Communications

No. of Patients 100, 250, 500				
NPTDC	PDR (%) LSR DM EH [6]	PDR (%) LCDL [13]	PDR (%) BEC [19]	PDR (%) Proposed
500	81.34	81.00	81.92	87.76
600	82.10	81.65	82.56	88.44
700	82.64	82.25	83.20	89.15
800	83.33	82.99	83.94	89.94
900	84.11	83.73	84.68	90.72
1000	84.82	84.42	85.38	91.48
1250	85.53	85.13	86.09	92.24
1500	86.24	85.83	86.80	93.00
2000	86.95	86.54	87.52	93.76
2250	87.66	87.24	88.22	94.52
2500	88.36	87.95	88.94	95.28
2750	89.08	88.65	89.65	96.04
3000	89.79	89.35	90.35	96.80
3500	90.50	90.06	91.06	97.57
4000	91.21	90.75	91.77	98.32
5000	91.92	91.45	92.47	99.07

As a result of the incorporation of throughput (Figure 6) for mining and sidechain selection operations, the proposed model has a throughput that is 25.5% higher than LSR DM EH [6], 23.8% higher than LCDL [13], and 19.5% higher than BEC [19]. This is observable based on this evaluation and figure 6, and it can be seen that the proposed model has a higher throughput than LSR DM EH [6]. This helps to improve the quality-of-service levels of the proposed model, which ultimately boosts the model's overall performance across a variety of deployment circumstances. Comparable observations have been made on the packet delivery ratio (PDR) performance. The results of these observations, which have been aggregated for 100, 250, and 500 patients and are shown in table 5.

Due to the incorporation of PDR for mining and sidechain selection operations, the proposed model has 6.5% higher PDR than LSR DM EH [6, 5.9% higher PDR than LCDL [13], and 4.5% higher PDR than BEC [19]. This can be seen based on this evaluation and figure 7, which shows that the PDR for the proposed model is significantly higher under different scenarios.

This helps to improve the quality-of-service levels of the proposed model, which ultimately boosts the model's overall performance across a variety of deployment circumstances. These assessments are expanded to account for a variety of various numbers of assaults inside the network, and they are covered in the next section of this text.

4.2. Security Performance for Different Healthcare Models in Presence of Attacks in the Networks

As a result of the incorporation of IQL with GA based blockchain model for data communications, the QoS performance of the proposed model is superior when compared with LSR DM EH [6], LCDL [13], and BEC [19] models under various attacks. This is due to the fact that the proposed model incorporates IQL with GA based blockchain model for data communications. The performance of this network is measured by changing the number of attacker (NA) nodes from 5% to 25% while simultaneously evaluating the quality of service parameters. Estimates have been made on the typical values of QoS for Sybil, MITM, and DDoS assaults. In accordance with this assessment technique, the values for end-to-end delay (D) for various protocols under these assaults are tabulated as follows in table 6.

On the basis of this evaluation and figure 8, it is possible to see that the proposed model has a delay that is 15.5% lower than LSR DM EH [6], 18.3% lower delay than LCDL [13], and 16.5% lower delay than BEC [19]. This is because the proposed model incorporates the delay that is caused by mining and sidechain selection operations. This improvement in delay performance demonstrates that the suggested model is capable of obtaining improved QoS even when subjected to various sorts of assaults, which confers on it the quality of being robust to many types of network attacks. Similar findings are made about the performance of energy. One may see this for Sybil, MITM, and DDoS assaults by looking at table 7.

Table 6 Average End-to-End Delay for Different Attacks

Type	of	Attack		Sybil, MITM, DDoS
NA (%)	D (ms) LSR DM EH [6]	D (ms) LCDL [13]	D (ms) BEC [19]	D (ms) Proposed
5.00	0.97	1.06	1.03	0.82
5.50	1.03	1.13	1.09	0.87
6.00	1.09	1.19	1.14	0.92
6.25	1.14	1.25	1.22	0.98

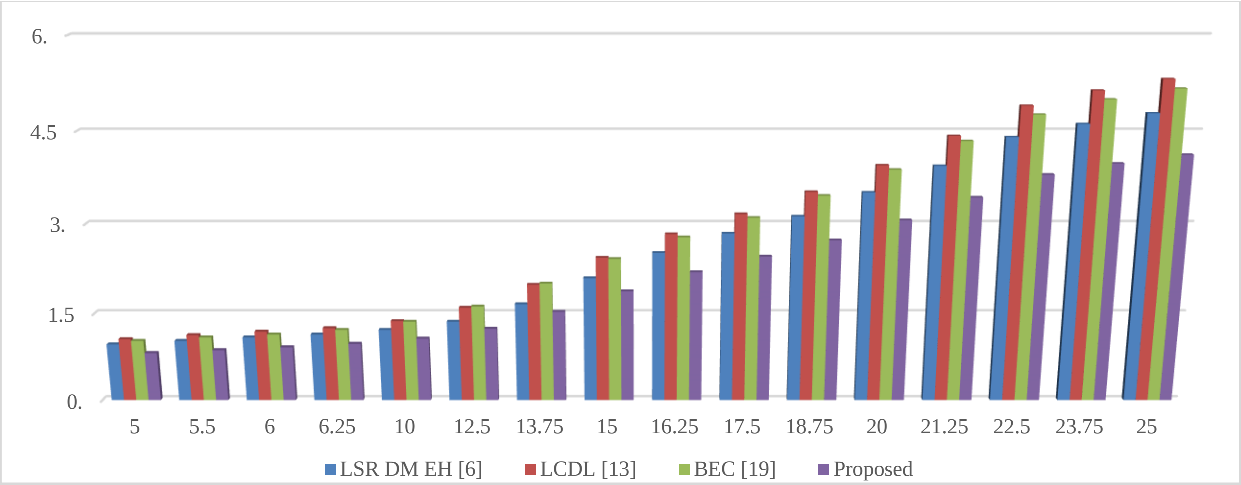

Figure 8 Average End-to-End Delay for Different Attacks

Table 7 Average Energy Consumption for Different Attacks

Type	of	Attack		Sybil, MITM, DDoS
NA (%)	E (mJ) LSR DM EH [6]	E (mJ) LCDL [13]	E (mJ) BEC [19]	E (mJ) Proposed
5.00	2.67	2.98	2.90	2.09
5.50	2.95	3.21	3.11	2.27
6.00	3.11	3.40	3.28	2.39
6.25	3.30	3.59	3.46	2.53
10.00	3.48	3.77	3.63	2.66
12.50	3.64	3.93	3.78	2.78
13.75	3.78	4.09	3.94	2.89
15.00	3.93	4.27	4.13	3.02
16.25	4.12	4.52	4.38	3.18
17.50	4.40	4.80	4.63	3.38
18.75	4.75	5.10	4.86	3.60
20.00	5.05	5.39	5.10	3.81
21.25	5.37	5.68	5.34	4.02
22.50	5.68	5.97	5.58	4.23
23.75	6.00	6.26	5.82	4.44
25.00	6.31	6.55	6.06	4.65

Due to the incorporation of energy during mining and sidechain selection operations, the proposed model has 16.5% lower energy consumption than the LSR DM EH [6], 18.5% lower energy consumption than the LCDL [13], and 18.3% lower energy consumption than the BEC [19]. Based on this evaluation and figure 9, it can be seen that the proposed model has 18.5% lower energy consumption than the BEC [19].

This improvement in energy consumption performance demonstrates that the suggested model is capable of obtaining superior QoS even when subjected to a variety of attack types, which confers on it the characteristic of being robust to a variety of network assaults. Similar findings are made about throughput performance, and this can be seen for Sybil, MITM, and DDoS assaults by looking at table 8.

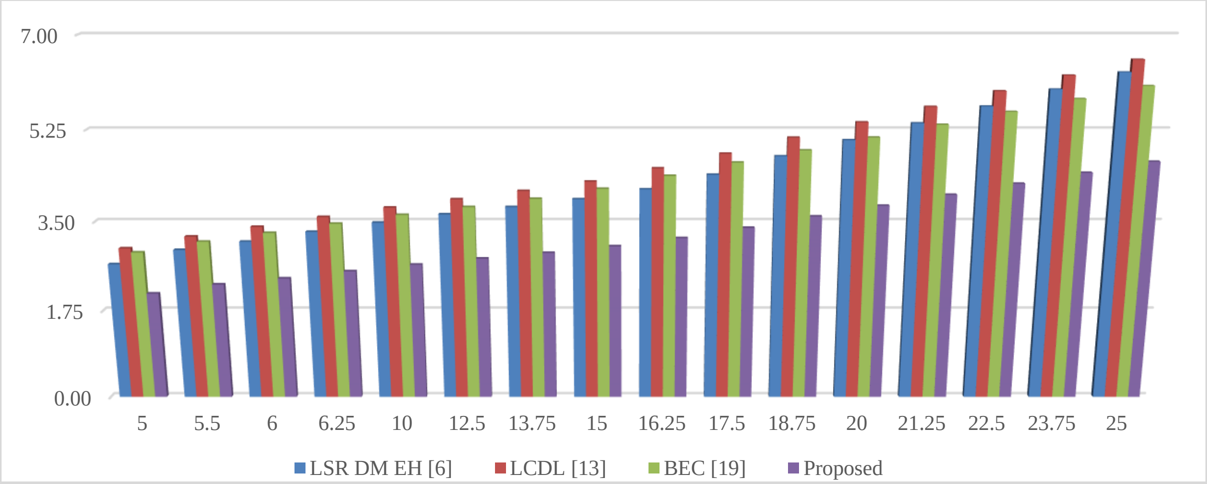

Figure 9 Average Energy Consumption for Different Attacks

Table 8 Average Throughput Performance for Different Attacks

Type	of	Attack		Sybil, MITM, DDoS
NA (%)	T (kbps) LSR DM EH [6]	T (kbps) LCDL [13]	T (kbps) BEC [19]	T (kbps) Proposed
5.00	312.69	332.99	318.10	433.13
5.50	315.25	335.60	320.61	436.58
6.00	317.60	338.31	323.26	440.04
6.25	320.36	341.30	326.10	443.92
10.00	323.23	344.26	328.91	447.80
12.50	325.95	347.14	331.66	451.55
13.75	328.67	350.02	334.40	455.29
15.00	331.38	352.90	337.15	459.04
16.25	334.10	355.78	339.89	462.79
17.50	336.81	358.66	342.64	466.54
18.75	339.53	361.54	345.38	470.28
20.00	342.24	364.43	347.39	473.70
21.25	344.93	367.27	349.90	477.32

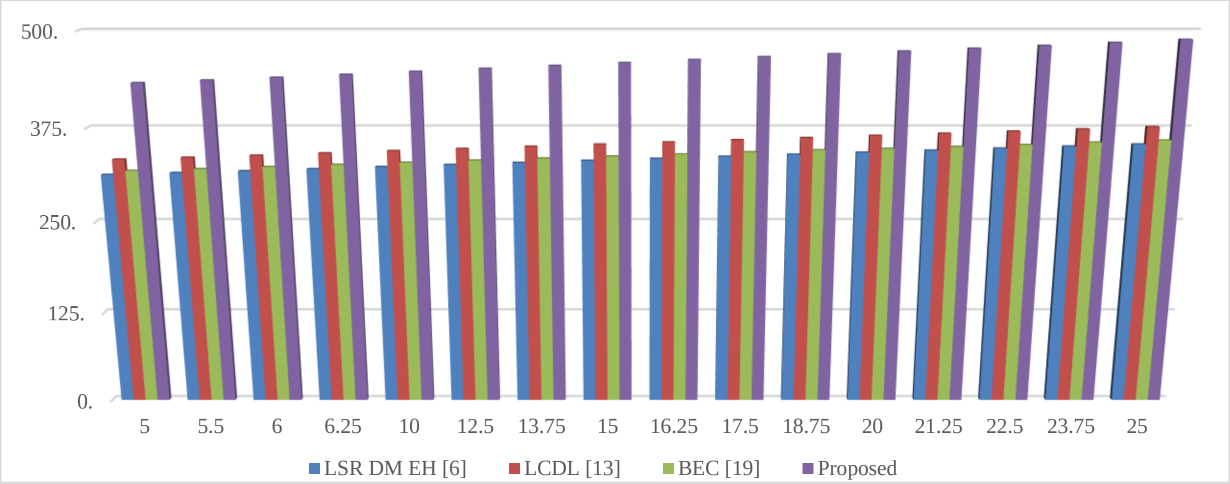

Figure 10 Average Throughput Performance for Different Attacks

Table 9 Average Packet Delivery Ratio Performance for Different Attacks

Type	of	Attack		Sybil, MITM, DDoS
NA (%)	PDR (%) LSR DM EH [6]	PDR (%) LCDL [13]	PDR (%) BEC [19]	PDR (%) Proposed
5.00	61.83	59.29	65.09	89.84
5.50	62.41	59.76	65.60	90.54
6.00	62.82	60.20	66.11	91.26
6.25	63.34	60.74	66.69	92.07
10.00	63.94	61.28	67.28	92.88
12.50	64.48	61.79	67.85	93.65

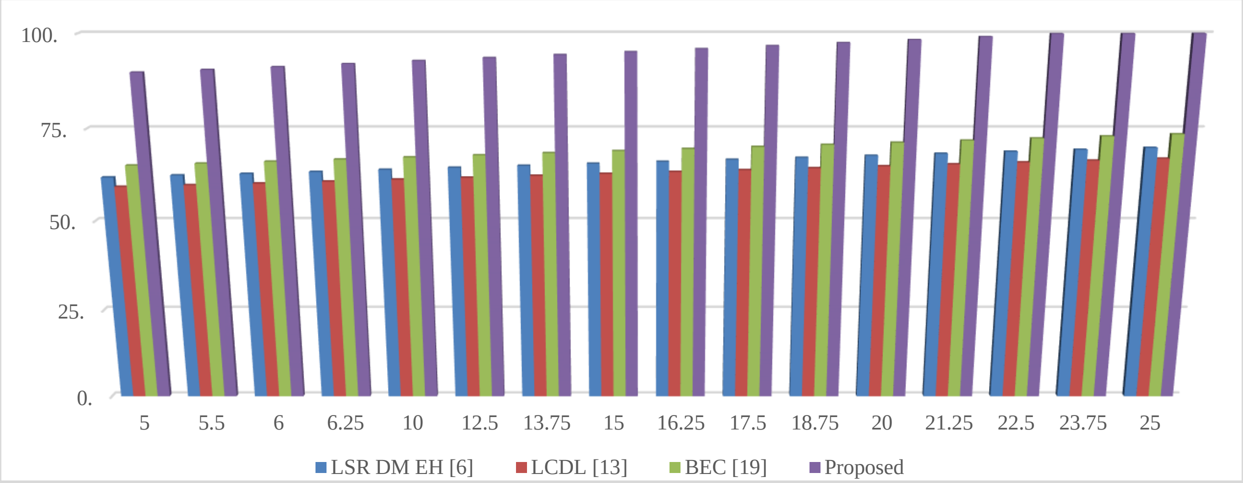

Figure 11 Average Packet Delivery Ratio Performance for Different Attacks

This evaluation and figure 10 show that the proposed model has a throughput that is 16.5% higher than BEC [19], which is due to the incorporation of throughput during mining and sidechain selection operations. The proposed model also has a throughput that is 18.3% higher than LCDL [13], which is higher than LSR DM EH [6], and has a throughput that is 20.4% higher than LCDL [6]. This improvement in throughput performance demonstrates that the suggested model is capable of obtaining superior QoS even when subjected to a variety of attack types, which confers on it the characteristic of being robust to a variety of network assaults. Similar findings are made about PDR performance; this can be seen for Sybil, MITM, and DDoS assaults by looking at table 9.

Due to the incorporation of PDR during mining and sidechain selection operations, the proposed model has a 25.5% higher PDR than LSR DM EH [6, 28.3% higher PDR than LCDL [13], and 23.5% higher PDR than BEC [19]. This is observable based on this evaluation and figure 11, and it can be seen that the proposed model has a higher PDR than LSR DM EH [6]. This improvement in PDR performance demonstrates that the suggested model is capable of attaining superior QoS even when subjected to a variety of attack types, which confers on it the characteristic of being robust to a variety of network assaults. As a result, the suggested model is extremely successful in terms of its QoS performance, which helps facilitate its implementation for a broad range of different secure healthcare applications.

5. CONCLUSION AND FUTURE SCOPE

The suggested model interactively combines the Genetic Algorithm (GA) with the IQL in order to integrate security and QoS awareness. This helps the model improve its latency, energy consumption, throughput, and PDR performance while it is subjected to network threats. Combining the GA Model, which provides an estimate of the various sidechain configurations, with the IQL Method, which provides assistance in dynamically scaling the underlying blockchains, is what the model employs. The IQL Method develops reward functions after doing temporal quality of service analysis on a variety of block batches. The incremental values of these functions are examined, and judgments about the chain growth, aggregation, and splitting procedures are made.

Due to these integrations, the proposed model has a lower delay, lower energy consumption higher throughput, and higher PDR when compared with LSR DM EH [6], LCDL [13], and BEC [19] models. This is because the model incorporates these parameters for mining and sidechain selection operations. This helps to improve the quality-of-service levels of the proposed model, which ultimately boosts the model's overall performance across a variety of deployment circumstances. This performance was observed to be consistent across different attack types this improvement in QioS performance demonstrates that the suggested model is capable of maintaining better efficiency even when subjected to a variety of attack types, which confers on it the characteristic of being robust to a variety of network assaults. These findings were also constant for throughput and PDR levels, which makes the model very valuable for real-time healthcare deployments under a variety of attack types In the future, researchers will be able to improve the performance of the model by using deep learning techniques such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and other similar methods. These models need to be verified on real-time datasets in order to provide an accurate assessment of their scalability performance under a variety of conditions. In addition, researchers have the ability to combine many bioinspired models into one another via a cascading process in order to constantly improve sidechaining performance while accounting for a variety of deployment-specific use cases.

REFERENCES

[1] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover and E. Hossain, "A Novel Smart Healthcare Design, Simulation, and Implementation Using Healthcare 4.0 Processes," in IEEE Access, vol. 8, pp. 118433-118471, 2020, doi: 10.1109/ACCESS.2020.3004790.

[2] P. P. Ray, D. Dash, K. Salah and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," in IEEE Systems Journal, vol. 15, no. 1, pp. 85-94, March 2021, doi: 10.1109/JSYST.2020.2963840.

[3] S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar and R. A. Khan, "A Systematic Analysis on Blockchain Integration With Healthcare Domain: Scope and Challenges," in IEEE Access, vol. 9, pp. 84666-84687, 2021, doi: 10.1109/ACCESS.2021.3087608.

[4] M. Zarour et al., "Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records," in IEEE Access, vol. 8, pp. 157959-157973, 2020, doi: 10.1109/ACCESS.2020.3019829.

[5] A. A. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S. Z. Abdul Rasid and M. F. Yusof, "Scalability Challenges in Healthcare Blockchain System—A Systematic Review," in IEEE Access, vol. 8, pp. 23663-23673, 2020, doi: 10.1109/ACCESS.2020.2969230.

[6] 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.

[7] I. A. Omar, R. Jayaraman, M. S. Debe, K. Salah, I. Yaqoob and M. Omar, "Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts," in IEEE Access, vol. 9, pp. 37397-37409, 2021, doi: 10.1109/ACCESS.2021.3062471.

[8] G. Subramanian and A. Sreekantan Thampy, "Implementation of Blockchain Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations," in IEEE Access, vol. 9, pp. 162459-162475, 2021, doi: 10.1109/ACCESS.2021.3132302.

[9] A. Awad Abdellatif et al., "MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange," in IEEE Internet of Things Journal, vol. 8, no. 21, pp. 15762-15775, 1 Nov.1, 2021, doi: 10.1109/JIOT.2021.3052910.

[10] Mamta, B. B. Gupta, K. -C. Li, V. C. M. Leung, K. E. Psannis and S. Yamaguchi, "Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System," in IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1877-1890, December 2021, doi: 10.1109/JAS.2021.1004003.

[11] M. H. Chinaei, H. Habibi Gharakheili and V. Sivaraman, "Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract," in IEEE Internet of Things Journal, vol. 8, no. 12, pp. 10117-10130, 15 June15, 2021, doi: 10.1109/JIOT.2021.3051433.

[12] M. Iqbal and R. Matulevičius, "Exploring Sybil and Double-Spending Risks in Blockchain Systems," in IEEE Access, vol. 9, pp. 76153-76177, 2021, doi: 10.1109/ACCESS.2021.3081998.

[13] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi and N. Kumar, "BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1242-1255, 1 April-June 2021, doi: 10.1109/TNSE.2019.2961932.

[14] M. Kassab, J. DeFranco, T. Malas, P. Laplante, G. Destefanis and V. V. G. Neto, "Exploring Research in Blockchain for Healthcare and a Roadmap for the Future," in IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 4, pp. 1835-1852, 1 Oct.-Dec. 2021, doi: 10.1109/TETC.2019.2936881.

[15] P. Li et al., "ChainSDI: A Software-Defined Infrastructure for Regulation-Compliant Home-Based Healthcare Services Secured by Blockchains," in IEEE Systems Journal, vol. 14, no. 2, pp. 2042-2053, June 2020, doi: 10.1109/JSYST.2019.2937930.

[16] A. P. Singh et al., "A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications," in IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5779-5789, Aug. 2021, doi: 10.1109/TII.2020.3037889.

[17] L. Ismail, H. Materwala and S. Zeadally, "Lightweight Blockchain for Healthcare," in IEEE Access, vol. 7, pp. 149935-149951, 2019, doi: 10.1109/ACCESS.2019.2947613.

[18] P. P. Ray, B. Chowhan, N. Kumar and A. Almogren, "BIoTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10857-10872, 1 July1, 2021, doi: 10.1109/JIOT.2021.3050703.

[19] D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "BEdgeHealth: A Decentralized Architecture for Edge-Based IoMT Networks Using Blockchain," in IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11743-11757, 15 July15, 2021, doi: 10.1109/JIOT.2021.3058953.

[20] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao and Y. Zhang, "A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System," in IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5914-5925, 1 April1, 2021, doi: 10.1109/JIOT.2020.3032997.

[21] D. Lee and M. Song, "MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address," in IEEE Access, vol. 9, pp. 158122-158139, 2021, doi: 10.1109/ACCESS.2021.3130552.

[22] G. S. Aujla and A. Jindal, "A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 491-499, Feb. 2021, doi: 10.1109/JSAC.2020.3020655.

[23] Z. Bao, Q. Wang, W. Shi, L. Wang, H. Lei and B. Chen, "When Blockchain Meets SGX: An Overview, Challenges, and Open Issues," in IEEE Access, vol. 8, pp. 170404-170420, 2020, doi: 10.1109/ACCESS.2020.3024254.

[24] A. Adavoudi Jolfaei, S. F. Aghili and D. Singelee, "A Survey on Blockchain-Based IoMT Systems: Towards Scalability," in IEEE Access, vol. 9, pp. 148948-148975, 2021, doi: 10.1109/ACCESS.2021.3117662.

[25] B. S. Egala, A. K. Pradhan, V. Badarla and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control," in IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11717-11731, 15 July15, 2021, doi: 10.1109/JIOT.2021.3058946.

Authors

Mrs. Pooja Mishra is pursuing her Ph.D. Degree from the Department of Computer Science and Engineering at Oriental University, Indore, Madhya Pradesh, India. She did her M.E from SPPU University,Pune in 2015 and Graduation in 2007 from Nagpur University. She has total 14 years of teaching experience. She has won the award for Innovative Implementable Idea under the Department of Ministry Electronics & IT. Her research interest includes Knowledge in Internet of Things, Machine learning and Deep learning.

Dr Sandeep Malik is currently working as Professor at Department of Computer Science and Engineering, Oriental University, Indore MP (INDIA). He received his Ph.D. degree in Computer Science and Engineering from Singhania University Rajasthan in 2015. He has also obtained M.Phil degree in CS from CDLU Sirsa in 2007. He did his M.Tech. degree from Kuruksherta University in 2004 and Graduation degree from CCS University Meerut in 2001.He has Teaching Experience of more than 20 years and Research Experience of more than 7 years. 3 Ph.D. CSE Degree has been already awarded under his Supervision as Guide and currently guiding 7 Ph.D. CSE Scholars. He has published and presented more than 60 Research Papers in International Journals and International and National Conferences of repute. His area of Research include ANN, Data Mining and Databases, Block chain and Decentralized Systems, IOT, AI and Cyber Physical Systems, Cyber Security etc.

How to cite this article:

Pooja Mishra, Sandeep Malik, “QSIH: Design of a Novel QoS-Aware Sidechain-Based IoT Network Design for Secure Healthcare Deployments”, International Journal of Computer Networks and Applications (IJCNA), 9(5), PP: 624-640, 2022, DOI: 10.22247/ijcna/2022/215921.