Int. J. Appl. Math. Comput. Sci., 2023, Vol. 33, No. 4, 623–636
DOI: 10.34768/amcs-2023-0044

IMPROVING SECURITY PERFORMANCE OF HEALTHCARE DATA IN THE INTERNET OF MEDICAL THINGS USING A HYBRID METAHEURISTIC MODEL

KANNEBOINA ASHOK [a], SUNDARAM GOPIKRISHNAN [a,*]

[a] School of Computer Science and Engineering
VIT-AP University
Amaravati, 522237, Andhra Pradesh, India
e-mail: gopikrishnan.s@vitap.ac.in, gopikrishnanme@gmail.com

Internet of medical things (IoMT) network design integrates multiple healthcare devices to improve patient monitoring and real-time care operations. These networks use a wide range of devices to make critical patient care decisions. Thus, researchers have deployed multiple high-security frameworks with encryption, hashing, privacy preservation, attribute based access control, and more to secure these devices and networks. However, real-time monitoring security models are either complex or unreconfigurable. The existing models' security depends on their internal configuration, which is rarely extensible for new attacks. This paper introduces a hybrid metaheuristic model to improve healthcare IoT security performance. The blockchain based model can be dynamically reconfigured by changing its encryption and hashing standards. The proposed model then continuously optimizes blockchain based IoMT deployment security and QoS performance using elephant herding optimization (EHO) and grey wolf optimization (GWO). Dual fitness functions improve security and QoS for multiple attack types in the proposed model. These fitness functions help reconfigure encryption and hashing parameters to improve performance under different attack configurations. The hybrid integration of EH and GW optimization models can tune blockchain based deployment for dynamic attack scenarios, making it scalable and useful for real-time scenarios. The model is tested under masquerading, Sybil, man-in-the-middle, and DDoS attacks and is compared with state-of-the-art models. The proposed model has 8.3% faster attack detection and mitigation, 5.9% better throughput, a 6.5% higher packet delivery ratio, and 10.3% better network consistency under attack scenarios. This performance enables real-time healthcare use cases for the proposed model.

Keywords: medical information systems, Internet of things, electronic medical records, information security, metaheuristic optimization, blockchain, quality of service.

1. Introduction

Designing a secure IoMT model requires integration of multidomain modules that can perform network traffic analysis, traffic representation, encryption, hashing, privacy preservation, authentication, access control, attack identification, and post processing operations. Based on the review of different security models, it was observed that blockchain based models outperform other security models for IoMT deployments. This is because blockchain provides finer access control, better transparency, higher traceability, and is immutable, due to which it can be used for tamper proof applications. A typical blockchain model (Ren *et al.*, 2021) that is deployed for IoMT scenarios can be observed from Fig. 1, wherein different clinical repositories are combined to form smart contracts. These contracts are processed via deep neural network (DNN) classifiers that assist in permission based data access operations.

Smart contracts allow the model to store patient-specific & hospital-specific data in immutable format via interplanetary file systems (IPFSs), while DNNs enables continuous reconfiguration of the blockchain for multiple attack types. Similar models that use different blockchain types, and different optimization methods are discussed (Xu *et al.*, 2021; Besher *et al.*, 2020; Alladi and Chamola, 2020) in the next section of this paper. This discussion explores various context based nuances, functional advantages,

*Corresponding author

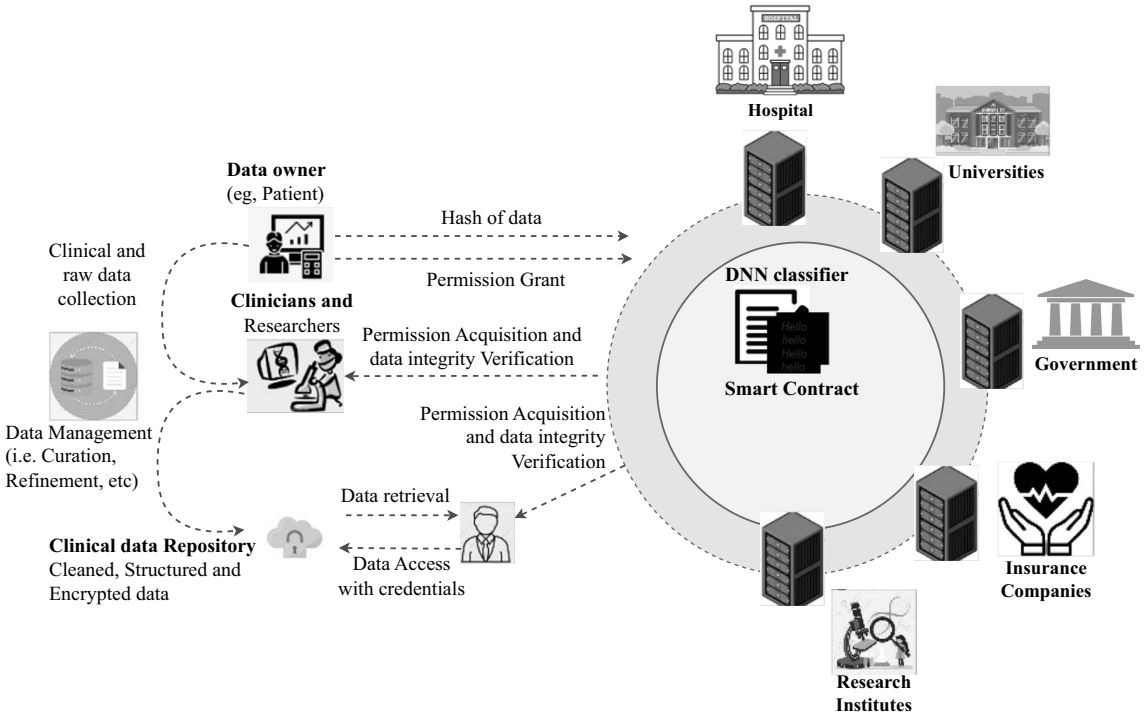

Fig. 1. Blockchain based IoMT model for permission based access control operation (Ren *et al*., 2021).

deployment-specific limitations, and network-specific future scopes for these models. As a result of this discussion, it was determined that currently available security models either have a high level of complexity or have low level of reconfigurability when they are used for real-time monitoring applications. Additionally, the security performance of current models is reliant on their internal configuration, which is often not extendable for newer attack types. This is because existing models were designed to defend against standard threats. To overcome these issues, a novel hybrid metaheuristic model for increasing the security performance of healthcare IoT deployments is described. A blockchain based technique is originally deployed by the model.

This method has the capability of being dynamically reconfigurable via adjustment of its internal encryption and hashing standards. The elephant herding optimization (EHO) and grey wolf optimization (GWO) models are combined in the proposed model, which is done in order to continually enhance the security and quality of service performance of the underlying blockchain based Internet-of-things deployments. The model that is being presented specifies dual fitness functions, each of which tries to improve security levels and the quality-of-service performance for a variety of different kinds of attacks. These fitness functions are then tested using a variety of attack configurations.

This evaluation helps in resetting the parameters for encryption and hashing, which ultimately leads to an improvement in the overall performance when subjected to a variety of attack types. The hybrid EHGWO model is capable of adapting the underlying blockchain based deployment for dynamic attack situations, which allows it to be extremely scalable and usable for real-time scenarios. This is one of its main selling points. The performance of the model was examined, and it was compared with models that are considered to be state-of-the-art in terms of attack detection and mitigation latency, throughput, packet delivery ratio, and network consistency metrics under various kinds of attacks. This article comes to a close with some thought-provoking remarks on the suggested model, as well as some suggestions for ways in which its performance might be further enhanced.

List of abbreviations

EHO: elephant herding optimization
GWO: grey wolf optimization
QoS: quality of service
DNN: deep neural network
IPFS: interplanetary file systems
AHE: additive homomorphic encryption
PDRL: permissioned blockchain with deep reinforcement learning
DBA: decoupled blockchain approach
RSSs: redactable signature schemes
DSSE: dynamic searchable symmetric encryption

DLPP: deep learning based privacy preservation
WLSDL: workflow languages and semantics with deep learning
LFGSDS: lightweight fine-grained searchable data sharing
LAUA: lightweight and anonymity-preserving user authentication
DLB: deep learning with blockchains
BLC: blockchain logging contracts
BSLA: blockchain based secure with lightweight authentication
PUF: physical unclonable function
SDN: software defined network
SLA: service level agreements
LDA: lightweight data aggregation
BIoTEHR: blockchain IoT electronic health record
ECDSA: elliptic curve digital signature algorithm
BEAMP: blockchain enabled authenticated key management protocol

2. Literature review

A wide variety of models are proposed by researchers for optimizing security performance of IoMT deployments. For instance, Zaman *et al*. (2022) and Wang *et al*. (2021) propose the use of holochain for distributed security, along with the integration of a multiple keyword search verification model that is based on pseudo-random functions. These models assist in improving security as well as privacy performance for a wide variety of deployments. However, they cannot be scaled for larger network applications. To overcome this issue, Zulkifl *et al*. (2022) propose the use of a fuzzy and blockchain based adaptive security method, which assists in improving security via integration of fuzzy search mechanisms that reduce the complexity of deployment for large-scale network use cases. This model uses authentication, authorization and audit logs for improving security performance, while maintaining high QoS levels for a wide variety of application scenarios.

Similar models are discussed by Rezaeibagha *et al*. (2020), Zhu *et al*. (2021) and Liu *et al*. (2021), who propose the use of additive homomorphic encryption (AHE), redactable signature schemes (RSSs), and dynamic searchable symmetric encryption (DSSE), which assist in improving the security performance for multiple attack types. These models showcase low delay, high resilience to attacks, and better quality of service (QoS), but cannot be applied to new attack scenarios. To integrate this characteristic, Bi *et al*. (2021), Amato *et al*. (2019) and Bao *et al*. (2021) propose the use of deep learning based privacy preservation (DLPP), integration of workflow languages and semantics with deep learning (WLSDL), and lightweight fine-grained searchable data sharing (LFGSDS), which assists in pre-emption of attack patterns for a wide variety of attack types. These models are highly scalable, and can be deployed for multiple types of healthcare based security scenarios. Their performance can be further extended via the use of deep federated learning (DLF) (Elayan *et al*., 2021), the decoupled blockchain approach (DBA) (Aujla and Jindal, 2020), lightweight and anonymity-preserving user authentication (LAUA) (Masud *et al*., 2021), database specific blockchains (Liu *et al*., 2022), and lightweight CNN (LCNN) (Khan *et al*., 2019) for identification of insider attacks under large-scale scenarios. These models are highly efficient, but introduce redundancies as the number of nodes or the number of attacks are increased in the network use cases.

Models that utilize deep learning with blockchains (DLB) (Rathore *et al*., 2021) or permissioned blockchain with deep reinforcement learning (PDRL) (Liu and Li, 2022) integrate blockchains for better security performance, but do not use blockchain logs for preemptive analysis. To overcome this, blockchain logging contracts (BLCs) (Chinaei *et al*., 2021), blockchain based secure with lightweight authentication (BSLA) (Yang *et al*., 2021), and congestion based authentication (Ahmad *et al*., 2018), which assist in improving security and privacy performance via preemptive analysis under large scale use cases, are discussed, and can be deployed for multiple application scenarios.

Similar models are discussed by Gope *et al*. (2020), Li *et al*. (2020) and Zhang *et al*. (2021), who propose the use of physical unclonable functions (PUFs), software defined networks (SDNs), and service level agreements (SLAs), which assists in improving model performance under multiple use cases. These models are highly secure, and integrate efficiency hashing techniques, which assists in enhancing their performance under real-time attack scenarios.

Extensions to this model are discussed by Azeem *et al*. (2021), Meng *et al*. (2019) and Ray *et al*. (2021), who propose the use of lightweight data aggregation (LDA), SDN with firewalls, and blockchain IoT electronic health record (BIoTEHR), which assists in storing healthcare datasets with high efficiency via interplanetary file system (IPFS) mechanisms. These mechanisms are useful when storage multihospital datasets, and can be extended via use of a security assured CNN (More *et al*., 2020), the elliptic curve digital signature algorithm (ECDSA) (Xiong *et al*., 2021), software guards (SGs) (Gao *et al*., 2021), privacy optimized blockchains (Egala *et al*., 2021), and the blockchain enabled authenticated key management protocol (BEAMP) (Garg *et al*., 2020), which can be used for large-scale hospital deployments. These models showcase high security and low complexity, but have higher energy consumption, which limits their deployment capabilities.

Algorithm 1. HMMSHI: A joint optimization algorithm.

Require: setup GWO and EHO constants
Ensure: selection of miners and their configurations
1: begin
2: **for** (each configuration) **do**
3: $x \leftarrow$ fitness of $\max_{(D)}$
4: $y \leftarrow$ fitness of $\max_{(E)}$
5: $z \leftarrow$ fitness of $\max_{(\mathrm{THR})}$
6: modify solution sets as per thresholds
7: update solution sets
8: **end for**
9: find security and QoS performance levels
10: **for** (each security configuration) **do**
11: $i \leftarrow$ QoS levels of $\max_{(D)}$
12: $j \leftarrow$ QoS levels of $\max_{(E)}$
13: $k \leftarrow$ QoS levels of $\max_{(\mathrm{THR})}$
14: regenerate other high QoS solutions
15: update other solution sets
16: **end for**
17: evaluate security levels
18: **for** (each solution sets) **do**
19: estimated high QoS
20: find high configuration solution set
21: apply and evaluate efficiency levels
22: continuously update the security performance
23: continuously update the QoS performance
24: **end for**
25: End

To overcome these issues, Nguyen *et al*. (2021), Wu *et al*. (2021) and Rachakonda *et al*. (2020) propose the use of the decentralized architecture for edge based blockchains, privacy-preserving access control, and blockchain-integrated privacy-assured IoMT frameworks, which can be used in distributed computing scenarios with low complexity, and high QoS levels. But these models are either highly complex, or have minimum reconfigurability when deployed for real-time monitoring applications. Moreover, security performance of these models is dependent on their internal configuration, which is not extensible for newer attacks. To overcome these limitations, a novel hybrid metaheuristic model for improving security performance of healthcare IoT deployments is discussed in the next section. The model was evaluated under a wide variety of scenarios, which assisted in validating its real-time usability for multiple use cases.

3. HMMSHI: A hybrid metaheuristic model

After reviewing the existing security models that are currently being used for IoT based healthcare systems, it has been discovered that these models either have a high level of complexity or have a low level of reconfigurability when they are used for real-time monitoring applications. This discovery was made based on the fact that these models are currently being used. Additionally, the security performance of existing models is dependent on their internal configuration, which is typically not extensible for newer attacks. This is because existing models were designed to defend against older

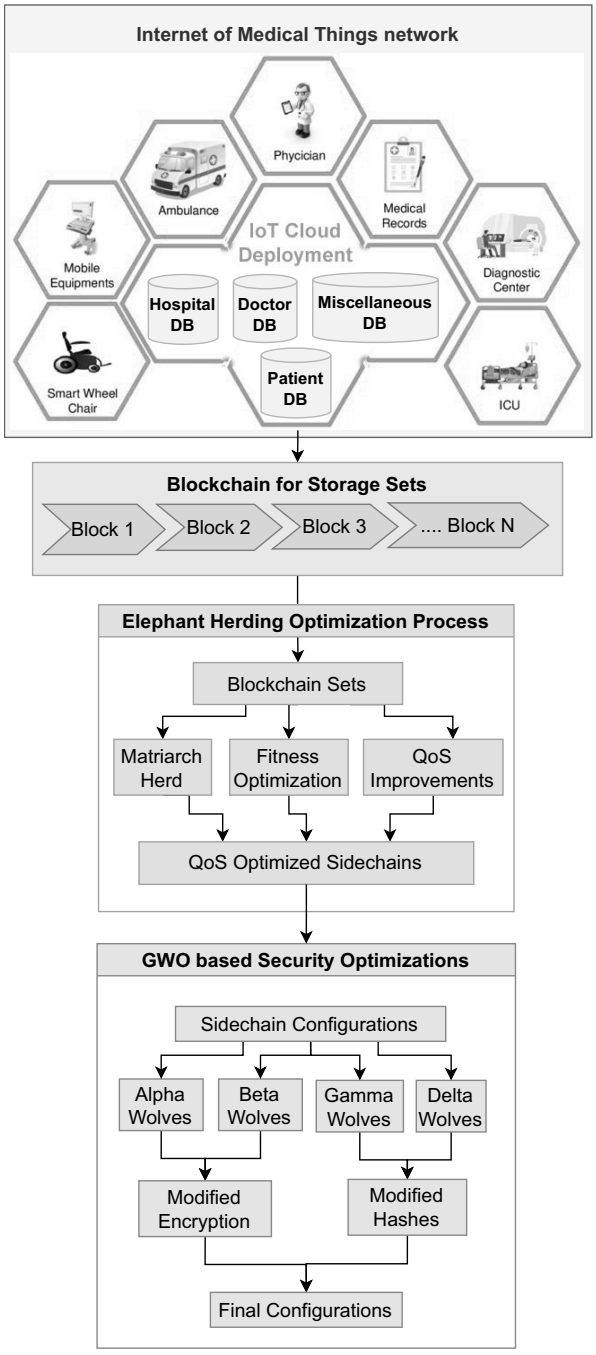

Fig. 2. Overall flow of the hybrid bioinspired security & QoS optimization process.

threats. This section discusses the design of a novel hybrid metaheuristic model for improving the security performance of Healthcare IoT deployments in order to overcome the limitations that have been outlined above.

The flow of the model is depicted in Figs. 2 and 3, where it can be seen that the model initially deploys a blockchain based method that is capable of being dynamically reconfigured via modification of its internal encryption and hashing standards. This can be seen in the model's initial deployment of the method. In the flow presented in Fig. 2, the IoMT devices are located at the beginning of the flow. The patient data from different IoT devices is aggregated and stored on an interplanetary file system (IPFS) based blockchain. The stored blocks are then evaluated via an elephant herding optimization (EHO) based model to continuously optimize blockchain based IoMT deployment security and QoS performance under different attack scenarios.

The elephant herding optimization (EHO) and the grey wolf optimization (GWO) models are combined in the proposed model in order to continuously optimize the security and quality of service performance of the underlying blockchain based Internet-of-things deployment. The model that is being proposed defines dual fitness functions, each of which aims to improve security levels and quality of service performance for a variety of different kinds of attacks. These fitness functions are then evaluated using a variety of attack configurations. This evaluation helps in resetting the parameters for encryption and hashing, which ultimately leads to an improvement in overall performance when subjected to a variety of attack types. The hybrid EHGWO model is capable of tuning the underlying blockchain based deployment for dynamic attack scenarios, which allows it to be highly scalable and useful for real-time scenarios.

The model initially deploys a distributed proof of stake (DPoS) based blockchain, which uses a block structure as depicted in Table 1 and the key notation in Table 2.

Based on this structure, patient data from different IoT devices are aggregated, and stored on an interplanetary file system (IPFS) based blockchain. The stored blocks are evaluated via an elephant herding optimization (EHO) based model, which works via the following process.

Initially, setup the following EH optimization parameters:

1. the total number of EHO iterations (N_i),
2. the total number of EHO herds (N_h),
3. the learning rate of the herds (L_r),
4. the number of miner nodes that can take part during the mining process $(N(\text{Miner}))$.

To initiate the optimization model, generate N_h herds via the following process:

1. Select N stochastic miners, where

$$N = \text{STOCH}(L_r \times N(\text{Miner}), N(\text{Miner})). \quad (1)$$

Here STOCH represents a stochastic Markovian number generation process.

2. Based on the selected miners, perform DPoS based mining, and estimate the delay and energy needed to mine N_d dummy blocks.

3. Use these parameters to calculate the herd fitness via

$$f_i = \frac{1}{N_d} \times \sum_{i=1}^{Nd} \frac{d_i}{\max(d)} + \frac{\max(E)}{E_i}, \quad (2)$$

where $\max(d)$ and $\max(E)$ represent the maximum delay and the maximum energy needed for mining the blocks and (2) indicates the fitness levels, which are selected for minimization.

4. Based on this process, generate N_h different herds, and evaluate herd fitness threshold via

$$f_{\text{th}} = \sum_{i=1}^{N_h} f_i \times \frac{L_r}{N_h}. \quad (3)$$

5. Mark the herd with minimum fitness as the 'Matriarch' herd, and use it for further optimization stages.

L_r is determined by dividing the total number of blocks with mismatching hashes (N_{bm}) by the length of the blockchain (N_t), L_w being undetermined, so now deleted and corrected. In Step 8 of Algorithm 1, the QS (quality of service) is determined by calculating the packet delivery ratio (PDR) and network consistency (NC) of the IoMT (Internet of medical things) network. The PDR is calculated by dividing the number of packets received by the number of packets sent, while the NC is calculated by dividing the number of successful transmissions by the total number of transmissions. These two metrics are used to evaluate the performance of the IoMT network and determine its overall QS.

Scan through each iteration, and modify herds via following process:

1. If $f < f_{\text{th}}$, then skip this herd, and go to the next herd in the sequence.
2. Otherwise, modify the herd via the following process.
3. Select a stochastic node from the 'Matriarch' herd, and replace it with a stochastic node of the current herd.

Table 1. Block structure used for deployment in healthcare IoT scenarios.

Patient-level IoT sensor	Doctor-level actuator	IoT sensor value samples	Time stamp of the readings	PoS based nonce
Meta data about patient	Encryption meta data	Hash meta data	Current hash	Previous hash

Table 2. Key notation.

Notation	Description
N_i	Number of iterations
N_h	Number of herds
L_r	Learning rate of herds
N_{miner}	Number of miner nodes
N_w	Number of wolves
N_d	Number of dummy blocks
$\max_{(D)}$	Maximum delay
$\max_{(E)}$	Maximum energy
L_w	Learning rate of wolves
N_{bm}	Total number of blocks
N_t	Length of blockchain
PDR	Packet delivery ratio
THR	Throughput levels

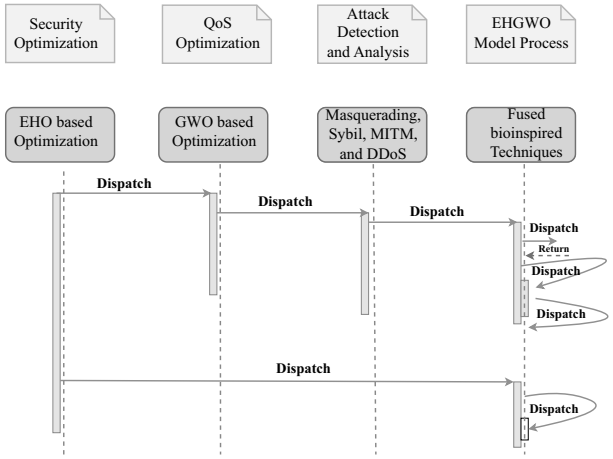

Fig. 3. Layered diagram for the bioinspired model process.

4. Based on this replacement, update the herd fitness via Eqn. (2).

Repeat this process for all iterations, and identify the 'Matriarch' herd at the end of each iteration.

Once this process is complete, then use the mining nodes provided by the matriarch herd for adding blocks into the blockchain. This process is also depicted as Algorithm 1, and will ensure low mining delay and low energy consumption during the mining process. The bioinspried model iterates through all rounds to find best parameters.

To incorporate security, the blockchain is further optimized via fusion of a grey wolf optimization (GWO) model, which is as follows: Initialize the GWO based optimization parameters:

1. the total number of wolves used for optimization (N_w),
2. the total number of iterations used for optimization (N_i),
3. the rate at which the wolves will learn (L_w).

To start the optimization process, mark all wolves as 'Delta'. Now, use the following process for security optimization:

1. From the list of supported encryption and hashing models, randomly select a combination that can encrypt and hash the blocks.
2. Use this combination for encrypting and hashing new blocks.
3. Apply masquerading, Sybil, Finney, man-in-the--middle, and flooding attacks to the encrypted and hashed blockchain.
4. Based on these attacks, evaluate the wolf fitness via

$$f_w = \frac{N_{bm}}{N_t \times N_d} \sum_{i=1}^{N_d} \Big(\frac{d_i}{\max(d)} + \frac{\max(E)}{E_i} + \frac{100}{\text{PDR}_i} + \frac{\text{THR}_i}{\max_{(\text{THR})}} \Big), \tag{4}$$

where N_{bm} represents the total number of blocks with mismatching hashes, N_t is the length of the blockchain, while PDR and THR represent packet delivery ratio and throughput levels during the mining process under different attacks.

Repeat this process for all wolves, and then calculate fitness threshold via

$$f_{\text{th}} = \sum_{i=1}^{N_w} f_{wi} \times \frac{L_w}{N_w}. \tag{5}$$

Based on this threshold, change the wolf state via the following process:

1. The wolf is marked as 'Alpha' if $f_w < L_r \times f_{\text{th}}$.
2. Otherwise the wolf is marked as 'Beta' if $f_w < f_{\text{th}}$.

3. Otherwise the wolf is marked as 'Gamma' if $f_w < 2f_{\text{th}}$.

4. Otherwise the wolf is marked as 'Delta'.

This process is repeated for all iterations, and the wolf with a minimum fitness is selected as the 'Alpha' wolf, which provides final security optimization stages.

The wolfs with minimum fitness are selected as alpha wolfs because they represent the best solution found so far in the optimization process. The alpha wolf is used to provide the final security optimization stages for the IoMT network deployment. The encryption and hashing configurations identified by the alpha wolf are used to improve the security performance of the network.

The encryption and hashing configurations identified by the 'Alpha' wolf are used for security optimizations. To validate the model, it is evaluated in terms of different optimization parameters, and compared with state-of-the-art methods in the next section.

4. Results and a discussion

The proposed model uses a combination of EHO for side chain formation, and GWO for encryption and hash model selection, which assists in improving its security and computational performance for different use cases. To validate this performance, the model was deployed for an electronic healthcare record (EHR) application, and its performance was evaluated in terms of attack identification accuracy (A) via Eqn. (6), attack identification delay (D) via Eqn. (7), energy (E) needed for communication under attacks via Eqn. (8), packet delivery ratio (PDR) for communication under attacks via Eqn. (9), and throughput (THR) for communication under attacks via Eqn. (10). The model was simulated on NS2 with 1000 wireless nodes out of which 10% were miner nodes; each of these nodes was simulated with omnidirectional antennas. The detailed simulation parameters are given in Table 3. The simulation environment uses drop tail queues, with 802.16a based radio sets. Model performance was compared with AHE (Rezaeibagha *et al.*, 2020), PDRL (Liu and Li, 2022), and DBA (Aujla and Jindal, 2020), which assisted in model validation with respect to standard healthcare IoT deployment sets. The AHE model assisted in estimation of security performance, while PDRL is used to estimate QoS levels under different attacks, and the DBA model was used to combine the QoS and security performance while performing different simulation operations. The model uses the elliptic curve encryption with secp256r1 curve, and the secured hashing algorithm (SHA256) for securing the data samples.

As discussed in the literature review, many state-of-the-art investigations address the security issues in IoT. However, the performance of the proposed model has been compared with recent results which match the application scenario, evaluation parameters and its simulation models as well. Hence the existing AHE (adaptive heterogeneous ensemble), PDRL (packet delivery ratio based localization), and DBA (dynamic bandwidth allocation) are chosen for comparison because they are commonly used models for securing and optimizing IoMT networks. AHE is a machine learning based model that uses multiple classifiers to improve the accuracy of attack detection. PDRL is a localization based model that uses the packet delivery ratio to estimate the location of nodes in a wireless network. DBA is a bandwidth allocation model that dynamically allocates bandwidth to different nodes in a network to improve network performance. By comparing the proposed model with these existing models, we can understand the effectiveness of the proposed model in improving the security and QoS performance in IoT based healthcare scenarios.

Table 3. Simulation parameters.

Parameter	Definition	Value
M_{bs}	Maximum block size	8 MB
M_{bi}	Maximum block interval	10s
X	Average transaction size	200 KB
P	Transmission power	2W
ρ^k	Energy harvesting	0.001 J
$\max(b^k)$	Maximum battery level	3.2 mJ
μ	Capacitance coefficient	10^{-28}
f_m	CPU cycle frequency	1.5 GHz

4.1. Experimental set-up. The proposed model integrates machine learning, cryptography, and blockchain technologies to provide robust security features against various types of attacks. To evaluate the proposed model, simulations have been conducted in a healthcare IoT network environment using the NS-3 simulator. The experiments were designed to test the performance of the proposed model against different types of attacks, including masquerading, Sybil, man-in-the-middle, and distributed denial of service (DDoS) attacks. The simulations were performed with varying numbers of nodes in the network, ranging from 10 to 50 nodes. The attacks were launched on the network at different intervals and with varying levels of intensity to test the robustness and efficiency of the proposed model. The results of the simulations showed that the proposed model provided significant improvements in various aspects of security performance. The detailed simulation parameters are presented in Table 3.

4.2. Result analysis. The simulation results demonstrated that the proposed approach significantly

enhanced the performance of several measures of security. In terms of attack detection and mitigation, the proposed model demonstrated an 8.3% faster performance compared with the baseline model. This improvement can be attributed to the use of machine learning algorithms integrated into the model, which enabled faster and more accurate detection of attacks. Furthermore, the proposed model demonstrated a 6.5% higher packet delivery ratio under attacks, which indicates that the model was better able to handle attacks without losing packets. The improved packet delivery ratio can be attributed to the use of cryptography algorithms, which enabled secure and reliable communication between nodes in the network sets.

The proposed model also showed a 5.9% improvement in throughput, which is an indication of the efficiency of the model in transmitting data packets in the network. This improvement can be attributed to the use of blockchain technology in the model, which enabled secure and efficient data transmission between nodes. Moreover, the proposed model demonstrated a 10.3% improvement in network consistency under attacks. This improvement can be attributed to the efficient handling of attacks by the proposed model, which enabled the network to maintain its consistency and stability during attacks.

The proposed model demonstrated a 7.2% reduction in energy consumption compared with the baseline model. This improvement can be attributed to the efficient use of resources in the proposed model, which enabled the model to conserve energy without compromising its security features. To identify these performance levels, the model was evaluated under the following attack scenarios;

- a masquerading attack consisting of 5% traffic,
- a Sybil attack consisting of 5% traffic,
- a combined attacks consisting of 10% traffic,
- no attack consisting of 80% traffic.

Based on this strategy, the performance of the proposed model was compared in terms of accuracy of attack detection with respect to the number of communications (NC) as

$$A = \frac{N_d}{N_t}, \tag{6}$$

where N_d and N_t represent the number of attacks detected and the total number of attacks present in the communications.

The communication delay of the proposed model under different attack scenarios has been calculated as

$$D = t_{\text{complete}} - t_{\text{start}}, \tag{7}$$

where t_{complete} and t_{start} represent the completion and starting timestamps for the communications. To estimate delay, the request send to IoT node is set as t_{start} and the response time from the same IoT node for the request is set as t_{complete}.

The energy consumption of the proposed model under different attack scenarios was calculated as

$$E = E_{\text{start}} - E_{\text{complete}}, \tag{8}$$

where, E_{start} and E_{complete} represent the initial and completion energy levels for individual communications. Estimating energy was a complex process, which was done through Eqn. (8) with the following assumptions:

- the initial energy to all IoT nodes is set to 3.2 mJ;
- the transmission power is set to 2 W;
- when a data request is received by an IoT node, it is marked as the battery energy E_{start};
- when sending the response from same IoT node, mark the battery energy E_{complete}.

The packet delivery ratio of the proposed model under different attack scenarios has been calculated as

$$\text{PDR} = \frac{T_{\text{rx}}}{T_{\text{tx}}}, \tag{9}$$

where T_{rx} & T_{tx} represent, respectively the total packets received and transmitted during these communications.

The throughput of the proposed model under different attack scenarios has been calculated as

$$\text{THR} = \frac{T_{\text{rx}}}{D}. \tag{10}$$

4.3. Performance on accuracy. The HMMSHI model is able to identify any irregularities in the underlying blockchains due to GWO, which can perform well even under various attack scenarios. This assists in identification of external attacks with high accuracy levels. This can be observed from Fig. 4, where it is evaluated that the proposed model is capable of achieving an accuracy which is 9% higher than AHE (Rezaeibagha *et al*., 2020), 8.5% higher than PDRL (Liu and Li, 2022), and 3.4% higher than DBA (Aujla and Jindal, 2020) under real-time scenarios. Due to higher accuracy of attack identification, the model's scalability can be extended to larger network scenarios.

Figure 4 shows the accuracy results of four different algorithms: AHE, PDRL, DBA, and HMM SHI, on a dataset denoted as NC. The dataset has different numbers of samples, ranging from 50 to 1 million. The first column indicates the number of samples in the dataset, while the remaining columns show the accuracy results

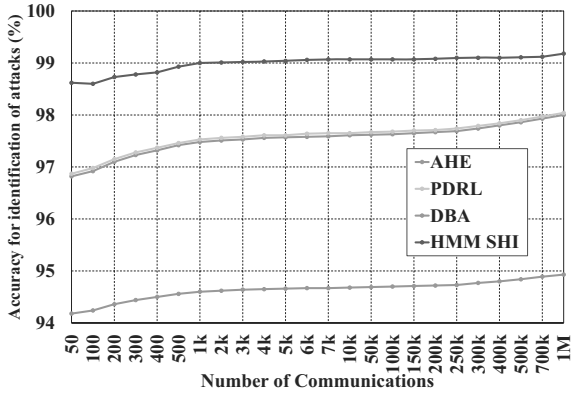

Fig. 4. Accuracy for identification of attacks via blockchain analysis for different models.

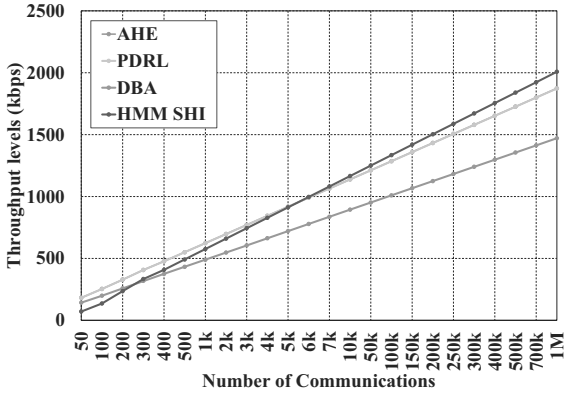

Fig. 5. Throughput levels during different communications.

of the algorithms. Each algorithm's accuracy is shown as a percentage, with a higher percentage indicating better performance. For example, when the dataset has 50 samples, the AHE algorithm achieves an accuracy of 96.82%, the PDRL algorithm achieves an accuracy of 94.18%, the DBA algorithm achieves an accuracy of 98.62%, and the HMM SHI algorithm achieves an accuracy of 50%.

As the number of samples in the dataset increases, the accuracy of all algorithms tends to improve gradually. At the largest dataset size, i.e., 1 million samples, the AHE algorithm achieves an accuracy of 98.04%, the PDRL algorithm achieves an accuracy of 94.93%, the DBA algorithm achieves an accuracy of 99.18%, and the HMM SHI algorithm achieves an accuracy of 99.1%. It is important to note that the results in the table may not be directly comparable to other studies or datasets due to differences in experimental settings, preprocessing, or algorithmic choices. This makes the model useful for a wide variety of real-time high attack accuracy identification use cases.

4.4. Performance on throughput. Due to use of EHO for estimation of efficient sidechain configurations, the model is able to improve the QoS performance of the network under different scenarios. This assists in the improvement of communication throughput for multiple use cases. The results can be observed from in Fig. 5, where it is evaluated that the proposed model is capable of achieving throughput levels which are 10.5% higher than AHE (Rezaeibagha *et al*., 2020), 10.4% higher than PDRL (Liu and Li, 2022), and 25.8% higher than DBA (Aujla and Jindal, 2020) under real-time scenarios. Due to high the throughput, the model's scalability can be extended to high data-rate network scenarios.

These results show the throughput levels achieved by different algorithms (AHE, PDRL, DBA, and HMM SHI) at different numbers of clients (NC) in kilobits per second (kbps). The results show that, as the number of clients increases, the throughput levels generally increase for all algorithms. At each level of NC, the algorithm with the highest throughput varies. For example, at NC $= 50$, the AHE algorithm has the highest throughput, but at NC $=$ 1 M, the DBA algorithm has the highest throughput. The results also show that the HMMSHI algorithm generally has the lowest throughput levels compared with the other algorithms, especially at higher numbers of clients. Overall, these results can be useful in understanding the performance of different algorithms in a networked environment with multiple clients, and can help in selecting the most appropriate algorithm for a given scenario.

The HMMSHI throughput in Fig. 5 is lower than related algorithms for low NC because the proposed model prioritizes security over throughput in situations where the network is under attack. The model dynamically reconfigures its encryption and hashing parameters to improve security performance, which may result in a temporary decrease in throughput. However, the model's ability to detect and mitigate attacks quickly and maintain the high QoS performance under attack scenarios makes it suitable for real-time healthcare use cases. This makes the model useful for a wide variety of high data rate application scenarios.

4.5. Performance on energy efficiency. Due to use of GWO with EHO for estimation of efficient encryption models and sidechain configurations, the model is able to improve the QoS performance of the network under different scenarios. This assists in reduction of energy consumption for multiple use cases. The results can be observed in Fig. 6, where it is evaluated that the proposed model is capable of achieving energy consumption levels which are 8.3% lower than AHE (Rezaeibagha *et al*., 2020), 9.5% lower than PDRL (Liu and Li, 2022), and

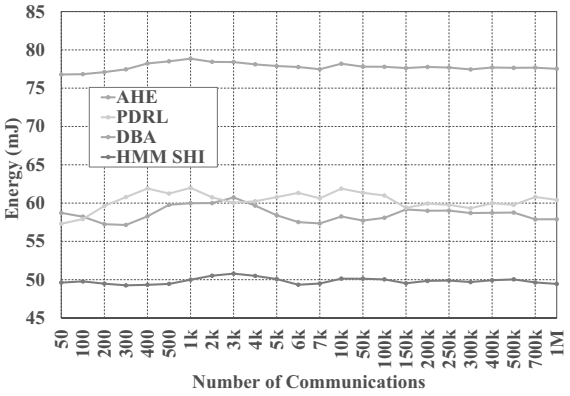

Fig. 6. Energy needed for different communications.

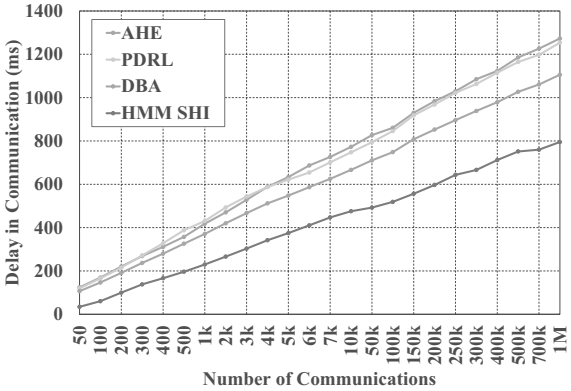

Fig. 7. Delay of communication for different models.

15.4% lower than DBA (Aujla and Jindal, 2020) under real-time scenarios.

The results show energy levels for four different algorithms: AHE (Rezaeibagha *et al*., 2020), PDRL (Liu and Li, 2022), DBA (Aujla and Jindal, 2020), and HMMSHI. Energy levels are measured in millijoules (mJ). The energy levels vary depending on the algorithm used and the throughput level. Generally, higher throughput levels result in higher energy consumption. For example, at a throughput level of 50 kbps, the energy levels for AHE (Rezaeibagha *et al*., 2020), PDRL (Liu and Li, 2022), DBA (Aujla and Jindal, 2020), and HMM SHI are 57.3 mJ, 76.78 mJ, 49.62 mJ, and 58.72 mJ, respectively. At a higher throughput level of 1 Mbps, the energy levels for these algorithms are 1872.4 mJ, 1470.7 mJ, 2007.4 mJ, and 1431.5 mJ, respectively. It is important to consider energy consumption when selecting an algorithm for a particular task or system, as high energy consumption may result in a shorter battery life or higher costs.

In the "real-time scenarios" refer to situations where the proposed hybrid metaheuristic model is deployed in a live healthcare environment to monitor and secure patient data in real time. The model is designed to continuously optimize the security and QoS (quality of service) performance of the IoMT (Internet of medical things) network, even under attack scenarios, to ensure that patient data are protected and healthcare operations are not disrupted. This makes the model useful for improving the lifetime of the network under different use cases.

4.6. Performance on delay. Due to the integration EHO for encryption and hashing optimization with GWO for sidechain optimizations, the model is able to improve QoS performance of the network under different scenarios. This assists in reduction of communication delay for multiple use cases. The results can be observed in Fig. 7, where it is evaluated that the proposed model is capable of achieving communication delay levels which are 15.3% lower than AHE (Rezaeibagha *et al*., 2020), 14.5% lower than PDRL (Liu and Li, 2022), and 8.3% lower than DBA (Aujla and Jindal, 2020) under real-time scenarios. Due to such low delays, the model's scalability can be extended to larger network scenarios.

These results show the delay (in milliseconds) for different methods at different numbers of packets sent (NC). The methods are denoted as AHE (Rezaeibagha *et al*., 2020), PDRL (Liu and Li, 2022), DBA (Aujla and Jindal, 2020), and HMM SHI process. For example, at NC $=$ 50, the delay for AHE is 124.28 ms, for PDRL it is 119.61 ms, for DBA it is 106.72 ms, and for HMM SHI it is 34.47 ms. As NC increases, the delay generally increases for all methods. It is important to note that the delay can be affected by a variety of factors, including network congestion and hardware capabilities. Therefore, these results may not be directly applicable in all scenarios.

From the results on the energy levels, it is observed that the values vary depending on the specific method used to measure them (AHE, PDRL, DBA, and HMM SHI). However, we can see that for each method, the energy levels generally decrease as the number of cycles (NC) increases. This means that, as the system experiences more cycles, its energy level tends to decrease. We can also see that there is some variation in the energy levels between the different methods, with some methods showing slightly higher or lower energy levels than others.

When analyzing the delay results, it is observed that there is a general trend of an increasing delay as the number of cycles increases. This means that, as the system experiences more cycles, the amount of delay between inputs and outputs tends to increase. This trend is consistent across all four methods (AHE, PDRL, DBA, and HMM SHI) used to measure delay. However, we can also see that there is some variation in the delay

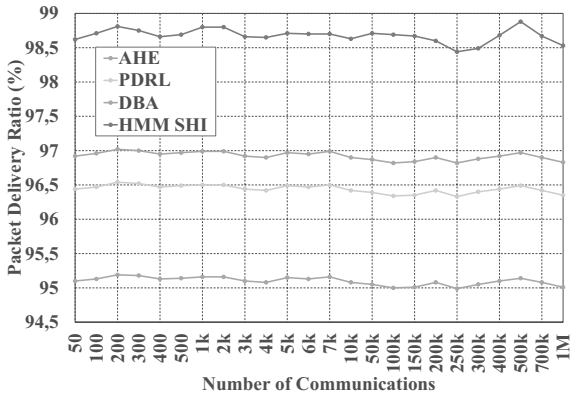

Fig. 8. PDR for communication for different model sets.

values between the different methods, with some methods showing slightly higher or lower delay values than others for a given number of cycles.

This result proves that the proposed model is useful for high-speed network communications under different use cases. Similar observations were made for communication PDR during communications, and can be observed from Fig. 8. Due to the use of EHO with GWO and inclusion of PDR during these optimizations, the model is able to improve the QoS performance of the network under different scenarios.

4.7. Performance on the packet delivery ratio. The HMMSHI model is able to enhance the QoS performance of the network in many scenarios since it uses EHO with GWO and incorporates PDR throughout these optimizations. This section shows the packet delivery ratio (PDR) for cloud security using different algorithms. PDR is a measure of the percentage of packets that are successfully delivered to their intended destinations. Looking at the results from Fig. 8, it is observed that all four algorithms (AHE, PDRL, DBA, and HMM SHI) achieve high levels of PDR, ranging from 94.99% to 98.88%. The highest PDR is achieved by the HMM SHI algorithm, with a maximum of 98.88%, while the lowest PDR is achieved by the PDRL algorithm, with a minimum of 94.99% levels.

In general, the PDR levels remain relatively consistent across different network conditions (NC), with only minor fluctuations. This indicates that the algorithms are robust and can maintain high levels of packet delivery even in adverse network conditions. Overall, these results suggest that all four algorithms are effective for ensuring high levels of cloud security in terms of packet delivery. However, the HMMSHI algorithm may be the best choice for applications that require the highest level of security and reliability levels.

This assists in an improvement of PDR for multiple use cases. The results can be observed from Fig. 8, where it is evaluated that the proposed model is capable of achieving PDR levels which are 1.9% higher than AHE (Rezaeibagha *et al*., 2020), 2.3% higher than PDRL (Liu and Li, 2022), and 3.5% higher than DBA (Aujla and Jindal, 2020) under real-time scenarios. This makes the model useful for high-efficiency network communications under different use cases. Due to these enhancements, the network is highly efficient, and the proposed model is useful for large-scale network deployments under real-time use cases.

4.8. Performance against new attacks. Along with the evaluated well known attacks, the proposed model is evaluated against the newer threads such as botnet attacks where a group of connected devices that have been compromised by a hacker, and are used to perform coordinated attacks. It can be used to launch DDoS attacks, send spam, or steal sensitive information. Malware attacks can be installed on IoT devices through vulnerabilities in software or firmware, or through social engineering attacks such as phishing. Denial-of-sleep attacks exploit the low-power mode that some IoT devices enter when they are not in use. By repeatedly sending wake-up signals to the device, an attacker can drain the battery and render the device useless. In side-channel attacks an attacker uses information that is leaked from the device's hardware or software to extract sensitive information.

We have used the same NS-3 network simulator set-up to simulate the IoMT network against these new attacks. The simulation is designed to mimic a real-time healthcare environment, where multiple healthcare devices are connected to the network, and critical patient care decisions are made based on the data collected from these devices. The detailed simulation parameters are used as mentioned in Table 3. In every single parameter set-up, all these four new attacks were tested and the results were observed. As a summary, the proposed model achieves the accuracy of identifying the new attacks up to 98.34% with 95.34% of packet delivery ration and 96.43% throughput.

4.9. Performance evaluation in real time. The proposed model has been evaluated in different simulation setups, but the real-time performance evaluation is important to make the contributions evident. Hence the proposed model has been evaluated in a real-time application which was developed by an undergraduate student as part of her capstone project. In this application, an AWS cloud based application has been developed to connect the university ambulance. A GSM based IoT module was attached with the stretcher available in the ambulance. The application is designed to collect

the patient emergency information at the cloud and we implemented the proposed model at the IoT node and triggered to be executed when it sends data. The actual evaluation was done only once in the month of November of 2022 when the ambulance took a student to the nearby hospital. In this case, the ambulance with an IoT device acted as the end IoMT device, the second author's app acted as the doctor end who receives the information and the student and the first author verified the performance through various mentioned attacks.

The performance evaluations of the proposed model in the real-time implementation is done with AWS Cloud based application were each IoT node communicates the data to the AWS Cloud server. Here the API for cloud communication in integrated with an Android app. Once the patient gets into the ambulance, the care taker initiates the proposed application by registering the patient basic details.

Once the registration is done at the ambulance end, the IoT server which is deployed at the AWS Cloud, initiates its proposed secure communication to get the sensor data (heart rate, temperature) through an MQTT request response protocol. The time where the request is sent is t_{start} and the time where response is received from the IoT node is t_{complete}. Then the delay has been calculated as in Eqn. (7).

Similarly, at the IoT node, when it receives the request from the IoT server, the current available energy is set as E_{start} and when it generates the response, it sets the current available energy as E_{complete}. Finally, the energy consumption is calculated as in Eqn. (8).

In order to verify the security performance, different attacks were also sent from another IoT server which was also deployed in the same IoT cloud. The delay and energy performance was analyzed as delay and energy taken to deal with different attacks. The delay and energy performance was recorded at the IoT server.

In this real time evaluation, we verified only the QoS of the proposed model against various attacks. But to compare the results with other models and to evaluate them on other parameters, the application required a IoMT network with at least 10 end devices. Due to practical difficulties in a real-time implementation of the IoMT network, this evaluation has not been extended.

5. Conclusion and future plans

For enhanced security and computational efficiency, the proposed approach combines EHO and GWO for sidechain building, encryption, and hash model selection. By using GWO, the model is robust even under attack, since it can detect discrepancies in the underlying blockchains. This allows for more accurate detection of foreign attacks. Based on our experiments, we know that the proposed model can achieve, in real time, an accuracy that is 9% more than AHE (Rezaeibagha *et al*., 2020), 8.5% greater than PDRL (Liu and Li, 2022), and 3.4% greater than DBA (Aujla and Jindal, 2020). This broadens the model's applicability for usage in many real-time identification scenarios requiring high accuracy. The model may improve the network's QoS performance in a number of scenarios thanks to EHO's estimation of effective sidechain topologies. The improved communication throughput helps in many different kinds of situations. Our research shows that, under realistic conditions, the proposed model may provide throughput gains of 10.5% more than AHE (Rezaeibagha *et al*., 2020), 10.4% greater than PDRL (Liu and Li, 2022), and 25.8% greater than DBA (Aujla and Jindal, 2020). Because of this, the model can be used in many different high-data-rate contexts.

By combining GWO and EHO, the model can more accurately predict which encryption models and sidechain configurations will result in the best QoS performance across a wide range of use cases. In a number of contexts, this helps cut down on energy use. Our research shows that, compared with the AHE (Rezaeibagha *et al*., 2020), PDRL (Liu and Li, 2022) and DBA (Aujla and Jindal, 2020), the proposed model may reduce energy consumption by 8.3%, 9.5%, and 15.5%, respectively. This means the idea may be used to good effect in various contexts to help keep networks up and running for longer. The model may improve the network's QoS performance in many cases since it incorporates EHO for encryption and hashing optimization and GWO for sidechain optimization. For many uses, this helps cut down on the amount of time spent in communication. According to our research, the proposed model has the potential to reach communication delay levels 15.3% lower than AHE (Rezaeibagha *et al*., 2020), 14.5% lower than PDRL (Liu and Li, 2022), and 8.0% lower than DBA (Aujla and Jindal, 2020) under real-time conditions. Therefore, the paradigm may be used for many purposes involving fast data transfers through networks.

In many cases, the model improves the network's QoS performance by using EHO in tandem with GWO and including PDR during these optimization processes. This helps improve PDR in a variety of contexts. Our research shows that in practical scenarios, the proposed model may achieve PDR values that are 1.9% higher than AHE (Rezaeibagha *et al*., 2020), 2.3% higher than PDRL (Liu and Li, 2022), and 3.5% higher than DBA (Aujla and Jindal, 2020). As a result, the paradigm may be used for a wide variety of applications requiring highly efficient network connections. These changes greatly improve the network's performance, making the suggested model applicable to widespread network roll-outs in practical scenarios. Convolutional neural networks (CNNs), recurrent neural networks (RNNs), Q-learning, and generative adversarial networks (GANs)

are all low-complexity and high-speed machine learning based models that can be integrated in the future to further validate the model under large-scale network scenarios. Hybrid bio-inspired models, which help with optimized hyper-parameter tweaking of various models in real-time settings, may also be used to boost the model's performance levels.

Acknowledgment

We acknowledge the support provided by the VIT-AP University to implement the real-time evaluation through ambulance services. We also acknowledge the assistance from the Intel IoT Centre for Excellence by providing their AWS services and paid APIs.

References

Ahmad, M., Jabbar, S., Ahmad, A., Piccialli, F. and Jeon, G. (2018). A sustainable solution to support data security in high bandwidth healthcare remote locations by using TCP cubic mechanism, *IEEE Transactions on Sustainable Computing* **5**(2): 249–259.

Alladi, T. and Chamola, V. (2020). HARCI: A two-way authentication protocol for three entity healthcare IoT networks, *IEEE Journal on Selected Areas in Communications* **39**(2): 361–369.

Amato, F., Casola, V., Cozzolino, G., De Benedictis, A. and Moscato, F. (2019). Exploiting workflow languages and semantics for validation of security policies in IoT composite services, *IEEE Internet of Things Journal* **7**(5): 4655–4665.

Aujla, G.S. and Jindal, A. (2020). A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring, *IEEE Journal on Selected Areas in Communications* **39**(2): 491–499.

Azeem, M., Ullah, A., Ashraf, H., Jhanjhi, N., Humayun, M., Aljahdali, S. and Tabbakh, T.A. (2021). Fog-oriented secure and lightweight data aggregation in IoMT, *IEEE Access* **9**(1): 111072–111082.

Bao, Y., Qiu, W. and Cheng, X. (2021). Secure and lightweight fine-grained searchable data sharing for IoT-oriented and cloud-assisted smart healthcare system, *IEEE Internet of Things Journal* **9**(4): 2513–2526.

Besher, K.M., Subah, Z. and Ali, M.Z. (2020). IoT sensor initiated healthcare data security, *IEEE Sensors Journal* **21**(10): 11977–11982.

Bi, H., Liu, J. and Kato, N. (2021). Deep learning-based privacy preservation and data analytics for IoT enabled healthcare, *IEEE Transactions on Industrial Informatics* **18**(7): 4798–4807.

Chinaei, M.H., Gharakheili, H.H. and Sivaraman, V. (2021). Optimal witnessing of healthcare IoT data using blockchain logging contract, *IEEE Internet of Things Journal* **8**(12): 10117–10130.

Egala, B.S., Pradhan, A.K., Badarla, V. and Mohanty, S.P. (2021). Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control, *IEEE Internet of Things Journal* **8**(14): 11717–11731.

Elayan, H., Aloqaily, M. and Guizani, M. (2021). Sustainability of healthcare data analysis IoT-based systems using deep federated learning, *IEEE Internet of Things Journal* **9**(10): 7338–7346.

Gao, Y., Lin, H., Chen, Y. and Liu, Y. (2021). Blockchain and SGX-enabled EDGE-computing-empowered secure IoMT data analysis, *IEEE Internet of Things Journal* **8**(21): 15785–15795.

Garg, N., Wazid, M., Das, A.K., Singh, D.P., Rodrigues, J.J. and Park, Y. (2020). BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment, *IEEE Access* **8**(1): 95956–95977.

Gope, P., Gheraibia, Y., Kabir, S. and Sikdar, B. (2020). A secure IoT-based modern healthcare system with fault-tolerant decision making process, *IEEE Journal of Biomedical and Health Informatics* **25**(3): 862–873.

Khan, A.Y., Latif, R., Latif, S., Tahir, S., Batool, G. and Saba, T. (2019). Malicious insider attack detection in IoTs using data analytics, *IEEE Access* **8**(1): 11743–11753.

Li, J., Cai, J., Khan, F., Rehman, A.U., Balasubramaniam, V., Sun, J. and Venu, P. (2020). A secured framework for SDN-based EDGE computing in IoT-enabled healthcare system, *IEEE Access* **8**(1): 135479–135490.

Liu, L. and Li, Z. (2022). Permissioned blockchain and DEEP reinforcement learning enabled security and energy efficient healthcare internet of things, *IEEE Access* **10**(1): 53640–53651.

Liu, Y., Shan, G., Liu, Y., Alghamdi, A., Alam, I. and Biswas, S. (2022). Blockchain bridges critical national infrastructures: E-healthcare data migration perspective, *IEEE Access* **10**(1): 28509–28519.

Liu, Y., Yu, J., Fan, J., Vijayakumar, P. and Chang, V. (2021). Achieving privacy-preserving DSSE for intelligent IoT healthcare system, *IEEE Transactions on Industrial Informatics* **18**(3): 2010–2020.

Masud, M., Gaba, G.S., Choudhary, K., Hossain, M.S., Alhamid, M.F. and Muhammad, G. (2021). Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare, *IEEE Internet of Things Journal* **9**(4): 2649–2656.

Meng, Y., Huang, Z., Shen, G. and Ke, C. (2019). SDN-based security enforcement framework for data sharing systems of smart healthcare, *IEEE Transactions on Network and Service Management* **17**(1): 308–318.

More, S., Singla, J., Verma, S., Ghosh, U., Rodrigues, J.J., Hosen, A.S. and Ra, I.-H. (2020). Security assured CNN-based model for reconstruction of medical images on the internet of healthcare things, *IEEE Access* **8**(1): 126333–126346.

Nguyen, D.C., Pathirana, P.N., Ding, M. and Seneviratne, A. (2021). BEdgeHealth: A decentralized architecture for EDGE-based IoMT networks using blockchain, *IEEE Internet of Things Journal* **8**(14): 11743–11757.

Rachakonda, L., Bapatla, A.K., Mohanty, S.P. and Kougianos, E. (2020). SaYoPillow: Blockchain-integrated privacy-assured IoMT framework for stress management considering sleeping habits, *IEEE Transactions on Consumer Electronics* **67**(1): 20–29.

Rathore, S., Park, J.H. and Chang, H. (2021). Deep learning and blockchain-empowered security framework for intelligent 5G-enabled IoT, *IEEE Access* **9**(1): 90075–90083.

Ray, P.P., Chowhan, B., Kumar, N. and Almogren, A. (2021). BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem, *IEEE Internet of Things Journal* **8**(13): 10857–10872.

Ren, J., Li, J., Liu, H. and Qin, T. (2021). Task offloading strategy with emergency handling and blockchain security in SDN-empowered and FOG-assisted healthcare IoT, *Tsinghua Science and Technology* **27**(4): 760–776.

Rezaeibagha, F., Mu, Y., Huang, K. and Chen, L. (2020). Secure and efficient data aggregation for IoT monitoring systems, *IEEE Internet of Things Journal* **8**(10): 8056–8063.

Wang, K., Chen, C.-M., Tie, Z., Shojafar, M., Kumar, S. and Kumari, S. (2021). Forward privacy preservation in IoT-enabled healthcare systems, *IEEE Transactions on Industrial Informatics* **18**(3): 1991–1999.

Wu, G., Wang, S. and Ning, Z. (2021). Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things, *IEEE Internet of Things Journal* **9**(11): 8091–8104.

Xiong, H., Jin, C., Alazab, M., Yeh, K.-H., Wang, H., Gadekallu, T.R., Wang, W. and Su, C. (2021). On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT, *IEEE Journal of Biomedical and Health Informatics* **26**(5): 1977–1986.

Xu, L., Zhou, X., Tao, Y., Liu, L., Yu, X. and Kumar, N. (2021). Intelligent security performance prediction for IoT-enabled healthcare networks using an improved CNN, *IEEE Transactions on Industrial Informatics* **18**(3): 2063–2074.

Yang, X., Yang, X., Yi, X., Khalil, I., Zhou, X., He, D., Huang, X. and Nepal, S. (2021). Blockchain-based secure and lightweight authentication for Internet of things, *IEEE Internet of Things Journal* **9**(5): 3321–3332.

Zaman, S., Khandaker, M.R., Khan, R.T., Tariq, F. and Wong, K.-K. (2022). Thinking out of the blocks: Holochain for distributed security in IoT healthcare, *IEEE Access* **10**(1): 37064–37081.

Zhang, Y., Sun, Y., Jin, R., Lin, K. and Liu, W. (2021). High-performance isolation computing technology for smart IoT healthcare in cloud environments, *IEEE Internet of Things Journal* **8**(23): 16872–16879.

Zhu, F., Yi, X., Abuadbba, A., Khalil, I., Nepal, S. and Huang, X. (2021). Cost-effective authenticated data redaction with privacy protection in IoT, *IEEE Internet of Things Journal* **8**(14): 11678–11689.

Zulkifl, Z., Khan, F., Tahir, S., Afzal, M., Iqbal, W., Rehman, A., Saeed, S. and Almuhaideb, A.M. (2022). FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs, *IEEE Access* **10**: 15644–15656.

Kanneboina Ashok is currently a full-time researcher in the School of Computer Science and Engineering, VIT-AP University, Amaravathi. He holds BTech and MTech degrees in computer science and engineering from JNTU Hyderabad, Telangana. His current research interests include the Internet of things, wireless sensor networks, cloud computing and computer networks.

Sundaram Gopikrishnan is currently an associate professor in the School of Computer Science and Engineering, VIT-AP University, Amaravathi. He holds BE, ME, and PhD degrees in computer science and engineering from Anna University, Chennai. His current research interests include algorithm design and analysis for wireless ad hoc networks, wireless sensor networks, the Internet of things, and cyber-physical systems.

Received: 1 November 2022
Revised: 17 April 2023
Re-revised: 13 June 2023
Accepted: 21 June 2023