Journal of Robotics and Control (JRC)
Volume 6, Issue 2, 2025
ISSN: 2715-5072, DOI: 10.18196/jrc.v6i2.25181

Effectual Energy Optimization, Fault-Tolerant Attack Detection, and Data Aggregation in Healthcare IoT Using Enhanced Waterwheel Archimedes and Deep Siamese Maxout Forward Harmonic Networks

Ganesh Srinivasa Shetty [1*], Raghu N [2]
[1] Research Scholar and Assistant Professor Senior, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru, India
[1] Assistant Professor, Department of Electronics and Communication Engineering, Shri Madhwa Vadhiraja Institute of Technology, Bantakal, India
[2] Associate Professor, Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru
Email: [1] ganeshshetty27@gmail.com, [2] raghu1987n@gmail.com
*Corresponding Author

Abstract*—The Internet of Medical Things (IoMT) has emerged as a transformative technology for improving healthcare delivery and patient outcomes. However, IoMT systems face significant challenges, including high latency, energy inefficiency, and vulnerability to cyberattacks, which compromise data security and patient privacy. Existing methods for attack detection and secure routing in IoMT often suffer from high latency, limited fault tolerance, and insufficient accuracy in identifying sophisticated attacks. To address these challenges, this paper proposes two novel approaches: the Improved Waterwheel Archimedes Optimization Algorithm (WWAOA) for secure routing and the Deep Siamese Maxout Forward Harmonic Network (DSMFHN) for attack detection in healthcare IoT. The Improved WWAOA integrates the Waterwheel Plant Algorithm (WWPA) with the Archimedes Optimization Algorithm (AOA) to optimize cluster head (CH) selection and secure routing. It considers key fitness parameters such as energy consumption, link lifetime (LLT), trust, delay, distance, and fault tolerance to enhance network efficiency and resilience. The DSMFHN combines Siamese Neural Networks (SNN) and Deep Maxout Networks (DMN) with forward harmonic analysis to detect attacks with high accuracy and low false positive rates. Additionally, data aggregation is performed using Bidirectional Long Short-Term Memory (BiLSTM) with adaptive weightage based on fault and malicious node detection. Experimental results demonstrate that the proposed methods outperform existing techniques. The Improved WWAOA achieves a minimal delay of 0.557 ms, maximal energy efficiency of 0.182 J, a packet delivery ratio (PDR) of 93.894%, and a trust value of 87.152. Meanwhile, the DSMFHN achieves a high accuracy of 92.598%, a true positive rate (TPR) of 91.643%, and a low false positive rate (FPR) of 0.156. These results highlight the effectiveness of the proposed methods in addressing the critical challenges of latency, energy efficiency, and security in healthcare IoT systems.

Keywords—Internet of Medical Things; Cluster Head Selection; Secure Routing; Siamese Neural Network; Deep Maxout Network.

I. INTRODUCTION

The medical The Internet of Medical Things (IoMT) has revolutionized healthcare by enabling seamless connectivity among medical devices, facilitating real-time monitoring, and improving patient care. IoMT systems integrate wearable and implantable medical devices, sensors, and communication technologies to enhance healthcare efficiency. However, as IoMT adoption grows, it faces critical challenges, including security vulnerabilities, fault tolerance issues, and inefficient data aggregation, which hinder its reliability and scalability [1][68]. Additionally, IoMT is the prospective of existing healthcare schemes, wherein all clinical devices are monitored and connected over an internet through healthcare experts. It provides quicker and low expensive of healthcare as it progresses [2]. IoMT refers to a branch of IoT that is devoted to healthcare industries. It can also be stated as the collection of clinical devices linked to the internet for providing health-related services. Fundamentally, IoMT is the linked structure of health systems like software applications as well as services and clinical devices [3]. Owing to the probable contribution of IoMT devices, the healthcare industry costs are decreased. This healthcare industry saves much cost by depending upon IoMT devices, particularly for telehealth and chronic diseases [4]. Specifically, IoMT devices such as clinical implantable and wearable sensors that comprise related key components of IoMT network are susceptible to diverse kinds of securable risks and they pose vital threats to patient's safety and privacy [5][6]. The network's fault tolerance is commonly specified as the reliability of accessibility of IoT systems in working criteria [7][8]. IoMT devices are integral to modern healthcare but are highly susceptible to security vulnerabilities that pose significant risks to patient safety and privacy [71].

The highly dependable IoT network with much tolerability leads a network to higher acceptance of such networks. IoT networks corresponding to the mission criticality models should be tolerable to extend about 99% [7]. IoT network's fault tolerance can be evaluated based on failure rate, success rate, power depletion rate as well as False Alarm Rate (FAR) and an estimation of these measures. Furthermore, various computational systems are to be employed including Fault Tree Analysis (FTA) for linearity systems, probability schemes, hybrid techniques that integrate probability and linearity approaches, bipartite flow graph modeling, and empirical models [8][9]. In an IoT network, nodes having batteries accommodate the converters for checking and receiving information from an environment. The nodes transfer sensible data separately by forming a wireless network and utilizing incorporated wireless radio. They are linked to exterior networks or the internet for transmitting sensible information to remote users. Cluster routing [10][11] is an excellent choice for sensor networks than flattened routing. In the cluster-enabled schemes, scalability is highly significant and these techniques attempt to decrease overheads [12]. In the cluster routing model, one or several CHs are considered for individual clusters to distribute network loads. It is due to responsibility of CHs for gathering information from the member nodes and then, forwarding it to Base Station (BS). In addition, cluster-enabled routing techniques can be better than other routing approaches based upon scalability, less consumption of energy, and enhanced management of sensing nodes. For increasing energy conservation amongst sensing nodes, energy-effective routing models must be taken into consideration [13].

With an enhancement in count as well as sorts of devices linked to IoT systems, its privacy and security are seriously threatened [14][15]. Security refers to the protection of systems against malfunctioning or thievery of software, hardware or various attacks. The node's reliability or security in IoT is highly important owing to the addition or removal of nodes from a network over a certain time [16]. Cyberattacks on IoMT devices can lead to theft of sensitive information and disruptions in critical healthcare services, necessitating advanced detection and mitigation techniques [69][70]. At present, Machine Learning (ML) approaches, particularly Deep Learning (DL) with excellent classification capability, have been expansively utilized for problems such as detection of attacks [17][18][66][67]. In particular, DL systems can efficaciously learn signs of diverse types of attacks [19]. DL approaches have been employed successfully in larger data models for assisting data mining and analytics by acknowledging complicated and hidden patterns. In addition, DL schemes are capable of identifying various newer sorts of attacks that have never been trained or learned previously [20][21]. In IoT, aggregation of data is significant due to the collection of varied data from diverse sources and the requirement of much energy for sending information. One of the solutions for reducing energy is to aggregate and process data before transmission. Therefore, summarized and aggregated information is transferred. Data aggregation or data collection executes a process of gathering information from multiple sensors. Moreover, aggregation of data is highly important in data deliverance utilizing effectual ways with minimum data latencies [22].

Among the primary concerns in IoMT networks is fault tolerance, which ensures network reliability by mitigating node failures and disruptions. Traditional IoMT architectures often suffer from high failure rates due to resource constraints and dynamic network conditions. Additionally, the security of IoMT devices is a significant challenge, as cyberattacks, including Distributed Denial of Service (DDoS) and Sybil attacks, pose serious threats to patient data confidentiality and system integrity. Furthermore, efficient data aggregation is crucial for minimizing communication overhead, reducing latency, and conserving energy in resource-limited IoMT environments. Existing solutions, including machine learning-based attack detection and traditional clustering algorithms, exhibit limitations in addressing these challenges comprehensively.

To overcome these limitations, this research proposes an improved approach combining the Improved Waterwheel Archimedes Optimization Algorithm (WWAOA) for secure routing and Deep Siamese Maxout Forward Harmonic Network (DSMFHN) for attack detection. The Improved WWAOA optimizes cluster head (CH) selection and secure routing based on parameters such as energy efficiency, Link Life Time (LLT), trust, delay, distance, and fault tolerance. By integrating the Waterwheel Plant Algorithm (WWPA) with the Archimedes Optimization Algorithm (AOA), Improved WWAOA enhances network reliability and prolongs node lifespan. Meanwhile, DSMFHN, which incorporates Siamese Neural Networks (SNN) and Deep Maxout Networks (DMN) with harmonic analysis, enhances the accuracy of attack detection while reducing false positives, thereby improving security in healthcare IoT networks.

A. Research Objectives and Contributions

This study aims to address the aforementioned challenges through the following objectives:

1. **Enhance Fault Tolerance and Energy Optimization** – Develop an improved cluster-based routing mechanism using Improved WWAOA to optimize CH selection and extend network lifetime.
2. **Improve Attack Detection Accuracy** – Implement DSMFHN to detect security threats with high accuracy and low false positive rates.
3. **Optimize Data Aggregation** – Leverage adaptive weight-based aggregation using BiLSTM to improve the efficiency of data transmission and reduce energy consumption.

The key contributions of this research include:

- Proposing **Improved WWAOA** for fault-tolerant, energy-efficient cluster-based routing in IoMT networks.
- Developing **DSMFHN** for robust attack detection, integrating deep learning techniques for enhanced classification accuracy.

- Implementing an adaptive **BiLSTM-based data aggregation approach** to optimize network resource utilization.
- Conducting extensive simulations and comparative evaluations using benchmark datasets (BoT-IoT and NSL-KDD) to validate the proposed methods.

The manifested sections are structured as: Literature view of traditional detection methods and their limitations are explained in section 2, IoMT system model is described in section 3, Improved WWAOA and DSMFHN methodology is elucidated in section 4, results of DSMFHN are presented in section 5 whereas section 6 reveals conclusion of DSMFHN.

II. MOTIVATION

IoT is a quickly developing domain that comprises of worldwide connected network structure based on internet. IoMT is the division of IoT that contains healthcare devices, which are crucial in processing, storing, transmitting, and monitoring sensible data. However, it faces newer problems regarding data protection and privacy due to various attacks. This motivated to present a detection model by reviewing traditional schemes. In this section, various techniques developed for detecting attacks in healthcare IoT are interpreted.

A. Literature Survey

Nalayini, P. and Meena, V [23] designed Optimization based Data Aggregation and fault Tolerance with Energy Management (ODFTEM) for routing. This technique was employed to assure an effectual utilization of network resources and reduced communication overhead in IoT networks. However, it did not address the privacy considerations and thus, this method led to security vulnerabilities. Vanani, M.M. and Dehkordi, P.K., [24] introduced the Fault Tolerance and Reliable Transaction Algorithm (FTRTA) for enhancing reliability along with an aid of fault tolerance. This model extraordinarily performed better in enhancing fault tolerance, even though it was not effective in assisting the quality of data transmission and routing. Aravind, K. and Maddikunta, P.K.R., [25] presented a Self-Adaptive Dingo Optimizer with Brownian motion (SDO-BM) for choosing optimum CH. This scheme attained improved fault tolerance as well as mitigation of energy hole, but still it was not applicable for multiple IoT environments.

Al-Abadi, A.A.J., *et al.* [26] developed an enhanced random forest classifier with a K-means clustering (ERF-KMC) for preventing and detecting attacks in IoMT. This method assured that transferred clinical information was exact, though it did not enhance security and reliability of IoMT networks. Wang, J., *et al.* [16] introduced privacy-preserving data aggregation (PDAM) for detecting malevolent data mining attacks. This approach assisted data privacy against interior adversaries that include remote control centers and gateways. Nevertheless, it developed extra latency in data transmission and processing. Kumar, M., *et al.* [27] designed End-to-End Homomorphic Encryption (EEHE) for identifying attacks on certain nodes. This scheme required low energy, but it failed to detect location-enabled wormhole attacks. Dener, M., [28] presented Secure Data Aggregation Protocol for Wireless Sensor Networks in IoT Resistant to Denial of Service (DOS) attacks (SDA-RDOS) to enhance security and network lifespan. It improved reliability and reduced the probability of corruption, unauthorized accessing, or data loss. However, this method increased algorithm overhead, and thus, the effectiveness of data aggregation was affected.

H Peng et al, proposed CBF-IDS effectively addresses class imbalance in intrusion detection systems by integrating CNN and BiLSTM architectures with a focal loss function, enhancing the classification of minority classes. It demonstrates superior performance across multiple benchmark datasets, achieving accuracy of up to 99.53% on the CIC-IDS2017 dataset [29]. S. Moustakidis proposed a hybrid intrusion detection system demonstrated high efficiency in categorizing cyber threats specific to IoMT environments, highlighting the importance of adaptive learning methods in intrusion detection systems (IDS) [30]. Saif et al explored the role of feature engineering in improving the performance of machine learning (ML) and deep learning (DL) models for detecting botnet attacks in IoMT networks. Their analysis emphasized the critical role of optimized features in achieving higher detection accuracy [31]. The study evaluates machine learning techniques for detecting cyber attacks in IoMT, showcasing their effectiveness in improving intrusion detection accuracy in healthcare networks. It emphasizes the importance of lightweight models tailored for resource-constrained IoMT environments [32]. Khan et al. introduced an ensemble learning-based detection framework that utilized fog-cloud architecture for real-time threat mitigation. This approach effectively balanced computational load while addressing the latency and resource constraints of IoMT systems [33]. Hameed et al. developed a lightweight attack detection framework suitable for fog-based IoMT systems. Their model demonstrated excellent performance in early detection while minimizing resource utilization, making it ideal for resource-constrained environments [34]. Punithavathi et al. proposed a cryptographic approach using hash-based algorithms for malware detection, focusing on securing IoMT data transmission while minimizing computational energy costs [35]. Nayak et al. integrated Bayesian optimization with extreme learning machines to design a sophisticated detection framework for cyberattacks. Their model outperformed traditional IDS approaches in terms of accuracy and computational efficiency [36]. H. Alavizadeh et al applied deep reinforcement learning models, specifically Q-learning, to detect cyber threats targeting sensitive health data. This approach achieved significant improvements in accuracy and adaptability to evolving attack patterns [37]. Askari et al. developed a novel scheduling algorithm using non-orthogonal multiple access (NOMA) in three-tier wireless body area networks (WBANs). Their approach minimized energy consumption while ensuring reliable real-time monitoring [38]. Sivaranjini et al. proposed a compressed sensing-based approach to reduce computational and energy overhead in wearable devices. Their method significantly extended the operational lifespan of IoMT devices while maintaining measurement accuracy [39]. Jaaz et al. introduced a fuzzy-based clustering algorithm optimized with the Whale Optimization Algorithm. Their model enhanced

energy efficiency and network lifetime, proving effective for 5G-enabled IoMT systems [40].

Mohammed Maray, *et al.* [64] established a TPFT framework in healthcare IoT. Here, in the first phase, IoT data was scheduled and then a bidirectional fault-tolerant mechanism was utilized for node-aware and task-aware fault tolerances. This model performed well on latency, failure rate probability and utilization of resources. However, the security issues were the major drawbacks of the methods. However, this method increased algorithm overhead and thus, the effectiveness of data aggregation was affected. G. Sripriyanka and Anand Mahendran [65] established an ICDC-Net. Here, for ensuring the security of data OFBC was used. The loss of OFBC was optimized using the HGWO-PSO to prevent DDoS attacks. The disease classification was done by ResNet50. Minimum attack detection error rates and high attack detection accuracy were the major advantages of the model. However, this model required more training for generalization. Table I shows a review of the existing methods.

The proposed work aims to address these gaps by introducing an Improved WWAOA for secure routing and DSMFHN for attack detection. The Improved WWAOA, by integrating the WWPA with the AOA, ensures optimized CH selection and secure routing based on key fitness parameters, including link lifetime, energy, trust, delay, distance, and fault tolerance. The DSMFHN model, which combines SNN, DMN, and forward harmonic analysis, provides robust attack detection with high accuracy, precision, and low false-positive rates. These contributions aim to enhance both the security and performance of IoMT networks by addressing issues of latency, energy consumption, and reliability while ensuring a higher level of trust and efficient resource utilization.

III. IoMT System Model

Fig. 1 represents the general IoMT network structure employed for managing security functions and forecast attacks utilizing DL or ML approaches. IoMT system [41] structure comprises patient sensor devices, network traffic collector, IoT gateway, Intrusion Detection System (IDS), security operators, and DL/ML data processing pipeline for monitoring various attacks. The sensor devices include a pulse rate detector, temperature sensor, blood pressure, heart rate detector, respiration rate monitoring device, and ECG device. The IoT network models like Advanced Message Queuing Protocol (AMQP) and MQ Telemetry Transport (MQTT) are utilized for sending data from the sensing device of IoT to the remote servers. IoT gateway's intention is to gather sensor data by wired or wireless communication and transmit information to remote areas. IDS includes analytical capacities and data processing for detecting intrusions in IoMT network. Continual analysis and monitoring are essential at the IDS level for tuning alerts and decreasing false positives. IoMT system applications include monitoring of remote patients as well as physical locations for saving and curing patient's health.

A. Energy Model

For modeling an efficacious routing system, it is crucial to identify consumed energy [42] by individual nodes to process the packets. This energy comprises the overall energy required for forwarding, receiving and transmitting packets on preferred route. Moreover, the node has to utilize energy for accepting an entering packet or expecting for approaching events. The energy consumed at node k on link $e(k,t) \in Y$ to process a packet can be modeled as,

$$Y_k = Y_{lg}^k + Y_{tg}^k + Y_{rg}^k + Y_{sg}^k = \left(T_{lg}^{'k} Z_{lg} + \left(Z_{tg} + Z_{rg}\right)\frac{PL}{DR} + T_{sg}^{'k} Z_{sg}\right) BV \quad (1)$$

Here, Y_{lg}^k indicates consumed energy while listening, Y_{tg}^k depicts consumed energy while transmitting, Y_{rg}^k implies consumption of energy for receiving, and Y_{sg}^k manifests consumption of energy for sleeping. Z_{lg}, Z_{tg}, Z_{rg} and Z_{sg} mentions consumption current during listening, transmission, receiving as well as sleeping. Moreover, BV reveals node's battery voltage, PL specifies the length of packets, and DR describes the data rate. $T_{lg}^{'k}$ and $T_{sg}^{'k}$ refers to the values computed based on Beacon Order and Superframe Order whereas Y_k symbolize consumed energy from the energy consumption model.

TABLE I. Review of Existing Methods

Reference	Method	Advantages	Disadvantages
Nalayini, P. and Meena, V., [1]	ODFTEM	Effectual utilization of network resources and reduced communication overhead	Did not address the privacy considerations
Vanani, M.M. and Dehkordi, P.K., [2]	FTRTA	Enhanced reliability along with an aid of fault tolerance	Not effective in assisting the quality of data transmission and routing
Aravind, K. and Maddikunta, P.K.R., [3]	SDO-BM	Improved fault tolerance as well as mitigation of energy hole	Not applicable for multiple IoT environments
Sastry, J.K.R., *et al.* [4]	Relay-based network	Enhanced the count of devices and the data traffic without affecting performance	Complications to network management and structure
Mohammed Maray, *et al.* [64]	TPFT	Performed well on latency, failure rate probability and utilization of resources	Security issues were the major drawbacks.
Al-Abadi, A.A.J., *et al.* [5]	ERF-KMC	Assured transferred clinical information was exact	Did not enhance security and reliability
Wang, J., *et al.* [6]	PDAM	Assisted data privacy against interior adversaries	Extra latency in data transmission and processing
Kumar, M., *et al.* [7]	EEHE	Required low energy	Failed to detect location-enabled wormhole attacks
Dener, M., [8]	SDA-RDOS	Improved reliability and reduced the probability of corruption, unauthorized accessing or data loss	Increased algorithm overhead
G. Sripriyanka and Anand Mahendran [65]	ICDC-Net	Minimum attack detection error rates and high attack detection accuracy	Required more training for the generalization

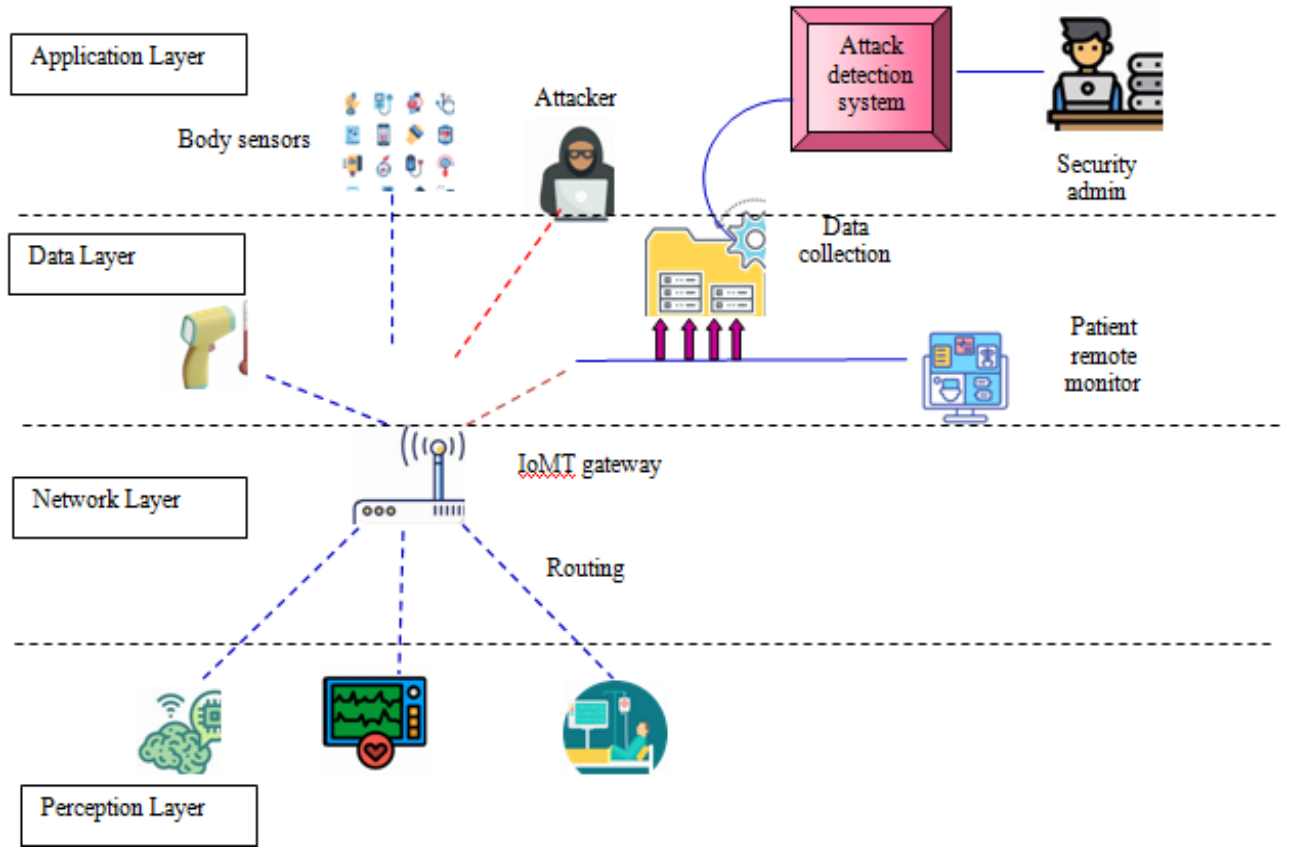

Fig. 1. IoMT network structure

B. *Mobility Model*

The mobility model [43] is present to interpret nodes's moving patterns and their velocity, acceleration, and location differences over a specific time. The movement patterns have a critical rolein identifying performance of routing techniques. In addition, it is utilized to emulate movable patterns of the intended real-world application in a logical mode.

Consider an initial location of nodes k and t are (v_1, v_1) and (v_2, v_2) at a specific time. The Euclidean distance C_{kt} amid nodes $k(v_1, v_1)$ and $t(v_2, v_2)$ at time $Ti = 0$ is illustrated by,

$$C_{kt} = \sqrt{|v_1 - v_2|^2 + |v_1 - v_2|^2} \quad (2)$$

C. *Trust Model*

Trust [44][45] can be evaluated by computing Indirect Trust (IT), Direct Trust (DT) historical trust, and recent trust of parent and child nodes.

D. *Link Life Time Model*

An evaluation of LLT [46] is accomplished at all hops during route navigation of path requisition packets. When node *P* implies the former hop of the packet for node, the information is enclosed based upon position as well as movement to route requisition packets. After that, LLT is evaluated while *Q* node receives this packet.

E. *Fault Model*

Fault tolerance [47] specifies the capability of the model for continual operation in an effectual manner even in an occurrence of attacks or faults when maintaining its performance and functionality.

IV. PROPOSED IMPROVED WWAOA AND DSMFHN FOR SECURE ROUTING AND ATTACK DETECTION IN HEALTHCARE IOT

In the present years, healthcare is an important problem for various persons. IoT supports several clinical applications that include earlier diagnosing as well as real-time monitoring. Healthcare expenses can be decreased by employing secure approaches for identifying attacks rapidly. Fig. 2 illustrates a pictorial view of DSMFHN for attack detection in healthcare IoT. In this research, DSMFHN is introduced to detect attacks in healthcare IoT. Initially, IoMT system model simulation is carried out. After that, the selection of CH as well as secure routing is conducted employing WWAOA, which is designed by joining WWPA with AOA. Moreover, fitness parameters concerned for executing CH selection and secure routing are energy, LLT, distance, trust, delay and fault tolerance. Then, attack detection is accomplished by DSMFHN which is modeled by incorporating SNN and DMN with harmonic analysis. Finally, data aggregation is performed, whereupon weights are determined by BiLSTM using adaptive weightage based upon fault and malevolent nodes.

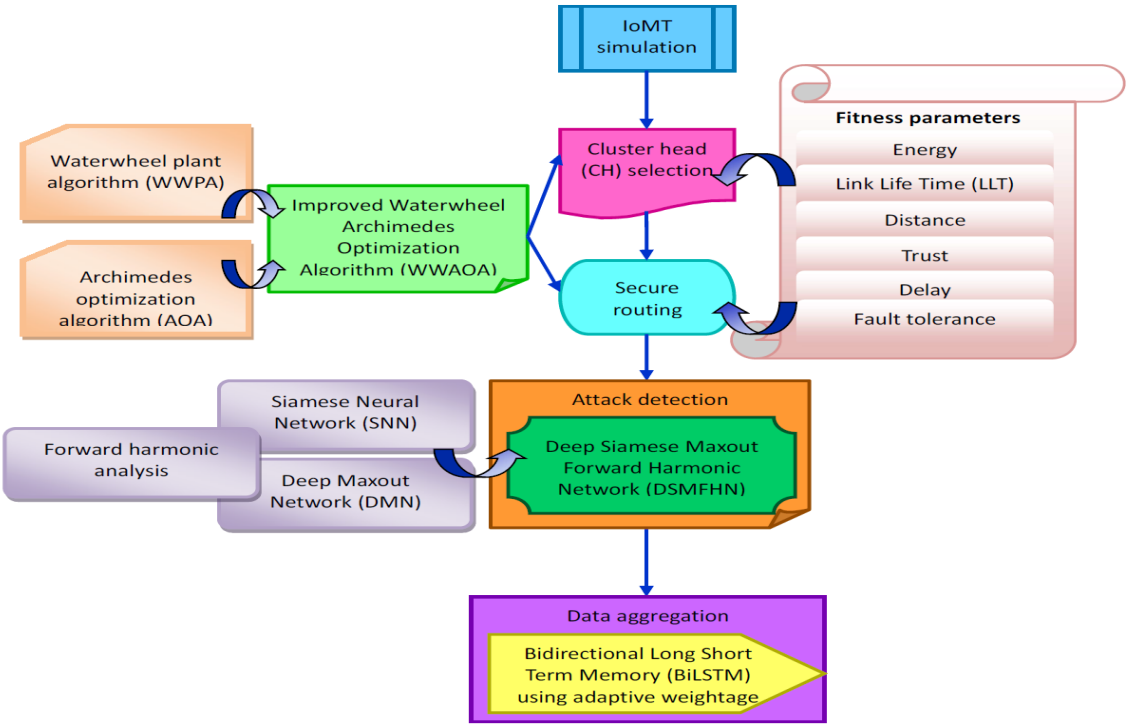

Fig. 2. Pictorial view of DSMFHN for attack detection in healthcare IoT

A. *CH Selection*

CH selection specifies a process of selecting certain nodes within the network of interlinked clinical devices to behave as CHs. These CHs have an important part in data processing, maintaining and monitoring communication as well as security within IoMT environments. Here, CH selection is done by Improved WWAOA that is designed by combining WWPA with AOA. The CH selection process may not effectively consider the energy consumption of each node, leading to the depletion of energy in certain nodes too quickly, which reduces the overall lifetime of the network. In this research, the Improved WWAOA incorporates energy as a key fitness parameter in the CH selection process. By considering energy consumption along with other parameters like LLT and trust, the algorithm ensures that nodes with sufficient energy levels are selected as CHs, thereby optimizing energy use and extending the network's lifespan.

1) Solution encoding: Solution encoding illustrates to a representation form that can be utilized for encoding probable solutions during CH selection process. Fig. 3 specifies solution encoding for CH selection.

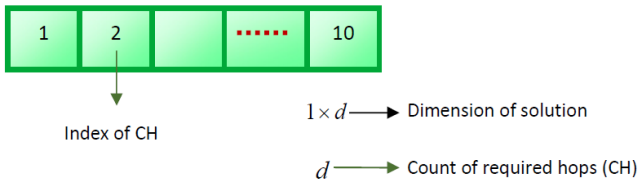

Fig. 3. Solution encoding for CH selection

2) Fitness function: Fitness function generally evaluates the suitability of node for becoming CH based upon various criteria. The various fitness parameters considered are energy, LLT, distance, trust, delay and fault tolerance. A fitness measure should be maximal and an expression is represented by,

$$f = \frac{(1-Y_k)+(1-C_{kt})+(1-L_{kt})+R_{kt}+E_{kt}+F_{kt}}{6} \quad (3)$$

Here, Y_k, E_{kt} and F_{kt} implies energy, LLT and fault tolerance. Moreover, C_{kt}, L_{kt} and R_{kt} mentions distance, delay and trust that are formulated as follows.

Distance specifies to a spatial closeness of Sensor Nodes (SNs) to probable CHs, which can be calculated as,

$$C_{kt} = \left\| \acute{A}_k - \acute{A}_t \right\|_{Nr} \quad (4)$$

Here, $\acute{A}_k$ indicates k^{th} CH and $\acute{A}_t$ reveals t^{th} node whereas Nr specifies normalization factor.

Delay illustrates to a time taken for the data to transfer amongst nodes in network that are modeled as,

$$L_{kt} = \frac{1}{\acute{V}} \sum_{k=1}^{nn} \aleph_k \quad (5)$$

Here, $\acute{V}$ symbolizes overall nodes in the cluster whereas nn indicates total nodes.

Trust refers to a level of credibility, confidence or reliability that the nodes have in probable CHs and it can be given by,

$$R_{kt} = \frac{1}{4}[K_{kt} + B_{kt} + O_{kt} + X_{kt}] \quad (6)$$

Here, K_{kt}, B_{kt}, O_{kt} and X_{kt} represents Direct Trust, recent trust, historical trust and Indirect Trust.

3) Algorithmic steps of WWAOA: WWPA [48] is modeled based on natural attributes of waterwheel plants during hunting expeditions. For identifying prey, the WWPA

employs plants as searching agents. WWPA determined a highly proportionate balancing amongst exploitation and exploration. AOA [49] is designed with an inspiration from Archimedes's Principle. This mimics a principle of a floating force exerting upwards on certain object, entirely or partly immersed in fluids, is proportional to displaced fluid's weights. AOA is the higher performance optimization algorithm concerning converging speed as well as balancing of exploitation-exploration, as it proficiently suitable to resolve difficult problems. Here, WWPA and AOA are integrated to design WWAOA that is well-suited for selecting CH owing to its effective performance in diverse situations. An updated expression of Improved WWAOA can be formulated as (7),

$$y_m^{w+1} = \frac{(I_1 \times \Re \times acc_{m-norm}^{w+1} \times \mu - 1)\left(K(2O + \ell_2)\right) + I_1 \times \Re \times acc_{m-norm}^{w+1} \times \mu \times y_{\Re}}{I_1 \times \Re \times acc_{m-norm}^{w+1} \times \mu} \quad (7)$$

Here, ℓ_1 and ℓ_2 denotes rand variable ranges between (0,2) and (0,1), O implies exponential variable having value in a range (0,1), $\Re$ illustrates uniformly distributed random number whereas I_1 mentions constant that is equal to 2. K depicts diameter of circle and acc_{m-norm}^{w+1} are expressed by,

$$K = \ell_1 . y_m(w) + 2O \quad (8)$$

$$acc_{m-norm}^{w+1} = AB \times \frac{acc_m^{w+1} - min(acc)}{max(acc) - min(acc)} + XY \quad (9)$$

Here, AB and XY implies a range of normalization.

B. Secure Routing Utilizing WWAOA

Secure routing is defined as an execution of routing strategies and models that not only assist an effectual data transmission amongst IoMT devices, but also combine mechanisms for detecting, preventing, and responding to diverse cybersecurity risks. Secure routing intends to assure confidentiality, availability, and integrity of sensible clinical data being transferred through interlinked medical devices. Here, secure routing is performed employing WWAOA, which is devised by integrating WWPA with AOA. The fitness parameters taken into concern for secure routing are energy, LLT, distance, trust, delay, and fault tolerance.

C. Attack Detection Utilizing DSMFHN

Security attacks pose crucial threats to IoT devices in healthcare systems that enable unauthorized accessing, system downtime, data violations, and other susceptibilities, which compromise patient's safety and privacy. Here, attack detection into Sybil attack and Distributed Denial of Service (DDoS) attack is performed utilizing DSMFHN. However, DSMFHN is introduced by incorporating SNN and DMN with harmonic analysis.

Fig. 4 presents a general overview of DSMFHN for attack detection. Firstly, input data G is multiplied by weight T_1 and therefore, a summation of weight $\sum T_1$ is obtained. Likewise, input data G is fed to SNN and thereafter, the outcome is again multiplied with $\sum T_1$ to get SNN output. On the other side, input data G is subjected to DMN and acquired resultant is multiplied with weight T_2. Therefore, DMN outcome is obtained and then, forward harmonic analysis is applied to SNN output and DMN output to achieve a detected outcome.

1) SNN model: SNN [50] employs distinctive architecture for ranking similarity amongst inputs naturally. SNN comprises twin networks that accept different inputs but are combined by the energy operation at the top. The energy function evaluates a few metrics amid higher-level feature depiction on the individual side. The parameters amongst twin networks are connected. An input given to SNN is G and Fig. 5 reveals an architectural model of SNN.

SNN contains N layers, wherein an individual layer has D_n units in which $I_{1,n}$ indicates a hidden vector in a layer n for the initial twin and $I_{2,n}$ specifies the an equivalent for the next twin. Rectified Linear Unit (ReLU) is exclusively employed in an initial $N-2$ layers and sigmoid unit in residual layers.

The framework comprises series of convolutional (conv) layers, individual layer utilizes a channel having filters of varying sizes and an unchangeable stride of 1. This network uses ReLU activation operation to output feature maps, selectively pursued by max-pooling having filter size as well as stride of 2. Hence, s^{th} filter map in an individual layer draws the beneath form.

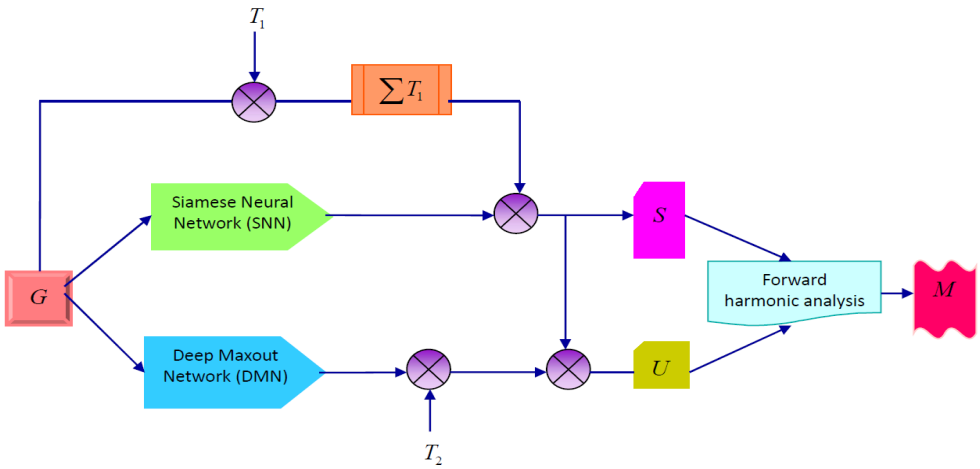

Fig. 4. General overview of DSMFHN for attack detection

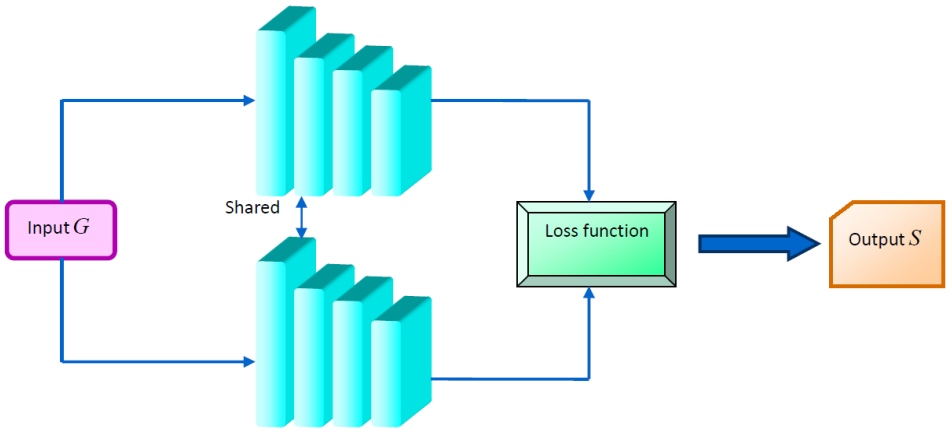

Fig. 5. Architectural model of SNN

$$\alpha_{1,v}^{(s)} = max - pool\left(max\left(0, H_{n-1,n}^{(s)} * I_{1,(n-1)} + A_n\right), 2\right) \quad (10)$$

$$\alpha_{2,v}^{(s)} = max - pool\left(max\left(0, H_{n-1,n}^{(s)} * I_{2,(n-1)} + A_n\right), 2\right) \quad (11)$$

Here, $H_{n-1,n}$ refers to a dimensional (3D) tensor depicting feature maps for the layer n and $*$ indicates valid conv function related to restoring only those outcome units that are resultant of entire overlap amongst individual conv filters as well as input feature maps.

The components in the last conv layer are flattened to a vector. This conv layer is pursued by a fully-connected (FC) layer and another layer evaluating induced distance measure amongst individual Siamese twin that is fed to a sigmoid output element. An outcome from SNN is specified by,

$$S = \left[\sigma\left(\sum_i \varpi_i \left|G_{1,N-1}^{(i)} - G_{2,N-1}^{(i)}\right|\right)\right] * \left(\sum T_1 * G\right) \quad (12)$$

Where σ denotes sigmoid activation operation and S is an output obtained from SNN. This last layer instigates the metric on a trained feature space of $(N-1)^{th}$ hidden layer and records its similarity amid two feature vectors. ϖ_i implies extra parameters, which are learned using the system during a process of training, weighting the importance of element-wise distance. It illustrates last N^{th} FC layer for a network that combines two siamese twins.

a) Loss function: Let us consider V as mini-batch dimension, wherein j indexes j^{th} mini-batch. Assume $r\left(z_1^{(j)}, z_2^{(j)}\right)$ as length-V vector that comprises labels for mini-batch in which $r\left(z_1^{(j)}, z_2^{(j)}\right) = 1$. Whenever z_1 and z_2 are obtained from similar character classes or else $r\left(z_1^{(j)}, z_2^{(j)}\right) = 0$. An objective of regularized cross-entropy is imposed on the binary classifier as follows.

$$\acute{L}\left(z_1^{(j)}, z_2^{(j)}\right) = r\left(z_1^{(j)}, z_2^{(j)}\right) log\acute{g}\, P\left(z_1^{(j)}, z_2^{(j)}\right) + \left(1 - r\left(z_1^{(j)}, z_2^{(j)}\right)\right) log\left(1 - \acute{P}\left(z_1^{(j)}, z_2^{(j)}\right)\right) + \varsigma^T |h|^2 \quad (13)$$

b) Optimization: The objective is fused with a standard backpropagation approach, whereupon gradient is additive over twin networks owing to joined weights [53]. A dimension of mini-batch is unchanged with a learning rate ∂_i, momentum ϕ_i and N_2 regularization weights ς_i specified layer-wise and thus, update rule in epoch T can be given by,

$$h_{si}^{(T)}\left(z_1^{(j)}, z_2^{(j)}\right) = h_{si}^{(T)} + \Delta h_{si}^{(T)}\left(z_1^{(j)}, z_2^{(j)}\right) + 2\varsigma_i |h_{si}| \quad (14)$$

$$\Delta h_{si}^{(T)}\left(z_1^{(j)}, z_2^{(j)}\right) = -\partial_i \nabla \hbar_{si}^{(T)} + \phi_i \Delta h_{si}^{(T-1)} \quad (15)$$

Here, $\nabla \hbar_{si}^{(T)}$ mentions partial derivative regarding weight amongst i^{th} neuron in a few layer and s^{th} neurons in succeeding layers.

2) DMN model: DMN [51] is a sort of Neural Network (NN) structure that employs maxout activation operation. This network provides robust configuration, which can make learning problems simpler by offering a flexible activation process. DMN can probably yield enhanced performance over conventional networks, specifically in DL tasks that need capturing complicated patterns [52]. An input subjected to DMN is G and structural depiction of DMN is shown in Fig. 6.

a) ReLU: At first, ReLU is exploited in Restricted Boltz-mann Machines (RBM), which can be revealed by,

$$\omega_b = \begin{cases} \kappa_b, if\, \kappa_b \geq 0 \\ 0, if\, \kappa_b \geq 0 \end{cases} \quad (16)$$

Here, κ_b indicates the input offered to a neuron whereas ω_b depicts its output.

b) Maxout: Maxout refers to ReLU's common variant that acquires higher operations on $\beta(\beta = 2)$ trainable linearity mechanisms. For specified input $\kappa \in M^{\lambda}$, the attained maxout unit's outcome can be represented by,

$$x_b(\kappa) = \underset{P\in[1,\beta]}{max}\, \xi_{bP} \quad (17)$$

Here, $\xi_{bP} = \kappa^H N_{\dots bP} + Y_{bP}, N \in M^{\lambda \times \vartheta \times \beta}$ and $Y \in M^{\vartheta \times \beta}$ symbolizes trainable parameters. Furthermore, b mentions total linearity sub-hidden element.

c) DMN: DMN is a class of trainable activation operations with multiple layered formations. For specified input $\kappa \in M^{\lambda}$, hidden unit activation can be modeled by,

$$E_{b,P}^{o} = \max_{P\in[1,\beta\psi]} E_{b,P}^{o-1^H} N_{\dots bP} + Y_{bP} \quad (18)$$

$$U = \left[\left[\max_{P\in[1,\beta\psi]} E_{b,P}^{o-1^H}\right] * T_2\right] * S \quad (19)$$

Substitute Eq. (12) in Eq. (19), therefore equation becomes,

$$U = \left[\left[\max_{P\in[1,\beta\psi]} E_{b,P}^{o-1^H}\right] * T_2\right] * \left[\sigma\left(\sum_i \varpi_i \left|G_{1,N-1}^{(i)} - G_{2,N-1}^{(i)}\right|\right)\right] * (\sum T_1 * G) \quad (20)$$

$$x_b = \max_{P\in[1,\beta_o]} E_{b,P}^{o} \quad (21)$$

Here, β_ϑ manifests overall elements in ϑ^{th} layers where as o illustrates entire layers in DMN. An outcome obtained from DMN is described as U.

3) Forward Harmonic Analysis: Harmonic analysis [54] is the prevailing analytical tool that permits manipulation and understanding of operations regarding frequency elements. The harmonic analysis provides a robust model for detecting attacks that influence frequency domain attributes. Fourier transform identifies anomalous spikes (e.g., sudden high-frequency bursts in DDoS).

For certain time series $l_{(1)}, l_{(2)}, \dots, l_{(c)}, \dots, l_{(q)}$, a standard expression of harmonic analysis is presented as,

$$l_{(c)} = p_0 + \sum_{\delta=1}^{\rho} (p_\delta . \boldsymbol{cos}(2\pi\delta c/q) + g_\delta . \boldsymbol{sin}(2\pi\delta c/q)) \quad (22)$$

Let us consider, $q = 2$ and $\rho = 1$, therefore equation becomes,

$$l_{(c)} = p_0 + p_1 \boldsymbol{cos}\,\pi\, c + g_1 \boldsymbol{sin}\,\pi\, c \quad (23)$$

Here, $sin\,\pi = 0$ and $sin(2\pi) = 0$, hence an above equation is formulated by,

$$g_1 = l_{(1)} * 0 + l_{(2)} * 0 \quad (24)$$

$$l(c+1) = p_0 + p_1 \boldsymbol{cos}(\pi c) + g_1 \boldsymbol{sin}(\pi c) \quad (25)$$

$$p_0 = \frac{1}{2}[l(c-1) + l(c)] \quad (26)$$

$$p_1 = -l(c-1) + l(c) \quad (27)$$

Substitute Eq. (26) and Eq. (27) in Eq. (25), thus equation becomes,

$$l(c+1) = \tfrac{1}{2}[l(c-1) + l(c)] + \left(-l(c-1) + l(c)\right)\boldsymbol{cos}(\pi c) \quad (28)$$

$$l(c+1) = l(c)\left[\tfrac{1+2\,\boldsymbol{cos}(\pi c)}{2}\right] + l(c-1)\left[\tfrac{1-2\,\boldsymbol{cos}(\pi c)}{2}\right] \quad (29)$$

Let us consider,

$$l(c) = S,\ l(c-1) = U \text{ and } l(c+1) = M$$

Substitute above expressions in Eq. (29), thus equation can be revealed by,

$$M = S\left[\tfrac{1+2\,\boldsymbol{cos}(\pi c)}{2}\right] + U\left[\tfrac{1-2\,\boldsymbol{cos}(\pi c)}{2}\right] \quad (30)$$

Substitute Eq. (12) and Eq. (20) in the above expression and therefore equation becomes,

$$M = \left[\left[\sigma\left(\sum_i \varpi_i \left|G_{1,N-1}^{(i)} - G_{2,N-1}^{(i)}\right|\right)\right] * (\sum T_1 * G)\right]\left[\left[\tfrac{1+2\,\boldsymbol{cos}(\pi c)}{2}\right] + \left[\left[\left[\max_{P\in[1,\beta\psi]} E_{b,P}^{o-1^H}\right] * T_2\right] * \left[\tfrac{1-2\,\boldsymbol{cos}(\pi c)}{2}\right]\right]\right] \quad (31)$$

Here, S denotes an outcome from SNN, U indicates DMN output, and M specifies the detected outcome after applying harmonic analysis to both SNN and DMN outputs.

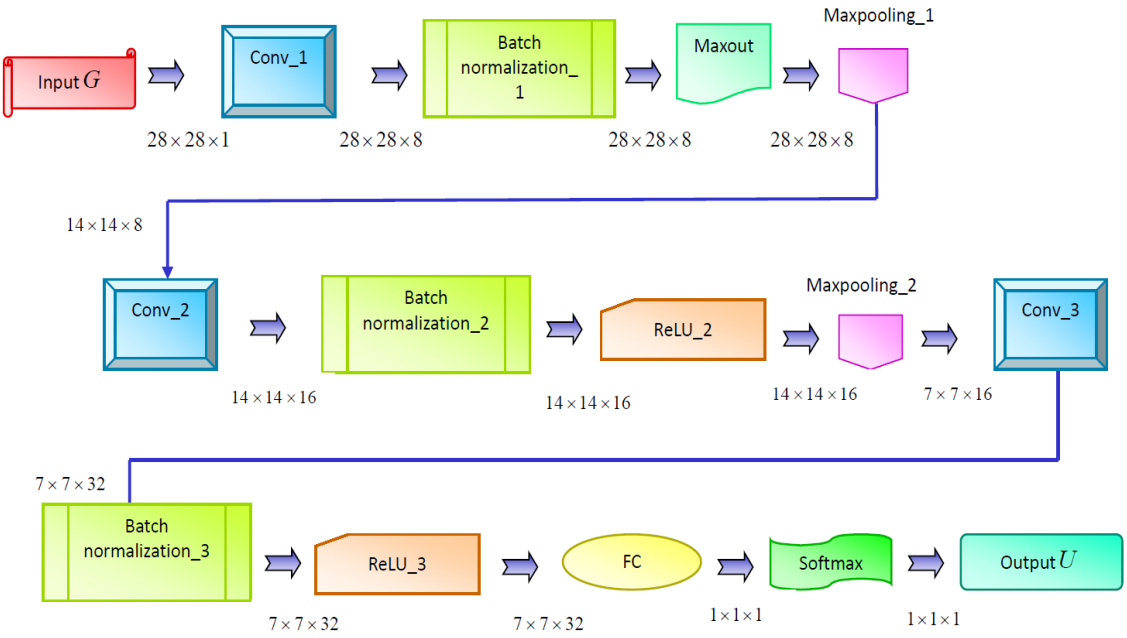

Fig. 6. Structural illustration of DMN

D. Data Aggregation

Data aggregation [55] refers to a process of incorporating, evaluating, and aggregating data from numerous interlinked medical devices, health information systems, and sensors for identifying patterns, probable security risks, and anomalies. In IoMT, effectual data aggregation is important to enhance resilience and security against attacks [56]. Here, data aggregation is conducted, whereupon weights are identified by BiLSTM [57] [58] using adaptive weightage based upon fault and malevolent nodes. The inputs given to BiLSTM are energy, LLT, distance, trust, delay, and fault tolerance [59] [60]. Assume data aggregation is accomplished at BS and it can be mentioned by,

$$Y_k' = \frac{1}{zi}\sum_{\substack{k=1\\t=1}}^{zi} H_k' * K_k' \tag{32}$$

Here, H_k' signifies sensed value by k^{th} node whereas K_k' mentions the weight of k^{th} node. The weights of each node are based upon malevolent activities that are computed regarding delay and trust. Moreover, weights from individual sensing nodes are aggregated by employing the adaptive weightage technique.

V. Results and Discussion

The outcomes of Improved WWAOA and DSMFHN designed for secure routing and attack detection in IoMT are interpreted in this part.

A. Experiment Setup

An experimental implementation of Improved WWAOA and DSMFHN is carried out in MATLAB tool. Table II shows the parameter details of the Improved WWAOA and DSMFHN.

TABLE II. Parameter Details

Parameter	Value
Number of Nodes	50,100
Area	100X100m^2
Initial Energy	1 J
data packet size	512–1024 bytes
maximum number of rounds	1000
MovementRange	10
Node density	0.8
Node failure rate per round	0.05
Transmission range	30 m
size of message	4000 bits
transmitted energy	150*0.000000001 J
Data Aggregation Energy	5*0.000000001 J
Optimal Election Probability of a node to become cluster head	0.1

B. Dataset Description

The considered datasets for analysis are BoT-IoT and NSL-KDD datasets that are interpreted beneath.

1) BoT-IoT dataset: BoT-IoT dataset [61] contains source files categorized regarding orts of attacks and additional categorization for best guidance in a labeling procedure. Here, the pcap files captured are about 72.000.000 records having 69.3 GB file size. Moreover, it has extracted flow traffic of about 16.7 GB size in a format of csv. In addition, it includes various attacks ordered additionally in terms of a utilized model.

2) NSL-KDD dataset: NSL-KDD dataset [62] comprises training as well as testing sets with binary labels in a format of ARFF. Furthermore, it consists of attack-type labeling and its difficulty levels in CSV format.

C. Simulation Outcomes

Fig. 7 illustrates the simulation outcomes of Improved WWAOA for 50 nodes. In the below figure, small squares denote nodes and their corresponding large square mentions CHs whereas red line represents transferring of data from source to its destination.

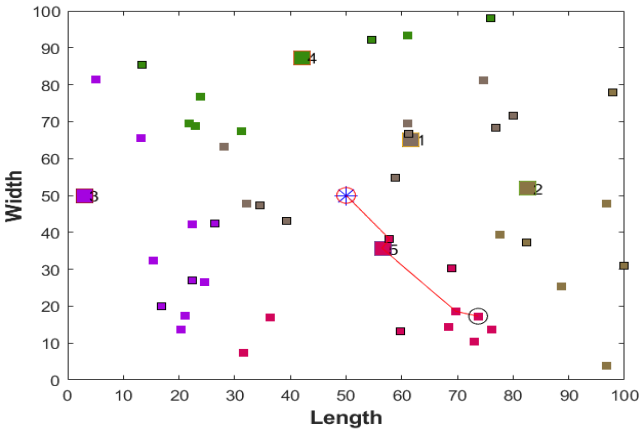

Fig. 7. Simulation outcomes of Improved WWAOA for 50 nodes

D. Evaluation Metrics

The metrics such as delay, energy, PDR, and trust are taken into consideration to evaluate Improved WWAOA. Likewise, performance measures considered to assess DSMFHN are accuracy, FPR, and TPR.

1) Delay: Delay specifies to a total time taken by the DPs to move for moving from source to destination over the specific network that is evaluated employing Eq. (12).

2) Energy: Energy is signified as a capacity of the routing protocol to determine shortest route for the transmission of data.

3) PDR: PDR is a metric that can be stated as a percentage of the DPs acquired by the destination node.

$$PDR = \frac{no.\ of\ packets\ received}{no.\ of\ packets\ sent} \times 100 \tag{33}$$

4) Trust: Trust mentions to an assurance level that the node has in reliability of other nodes in a network for forwarding data and it is calculated using Eq. (6).

5) Accuracy: Accuracy [63] is stated as an exactness of the system for detecting connections between normal and attacks that can be computed by,

$$Acc = \frac{True_{PT} + True_{NT}}{True_{PT} + True_{NT} + False_{PT} + False_{NT}} \tag{34}$$

Here, $True_{PT}$ and $False_{PT}$ represents true positive and false positive whereas $True_{NT}$ and $False_{NT}$ implies true negative and false negative.

6) FPR: FPR [63] specifies to a proportion of benign instances or legitimate activities that are inaccurately detected as attacks by the system and it is estimated as,

$$FPR = \frac{False_{PT}}{False_{PT} + True_{NT}} \quad (35)$$

7) TPR: TPR [59] measures an efficacy of the system in accurately detecting normal attacks, which is calculated by,

$$TPR = \frac{True_{PT}}{True_{PT} + False_{NT}} \quad (36)$$

E. Comparative Techniques

The existing approaches taken into concern for assessing Improved WWAOA are ODFTEM [23], FTRTA [24], SDO-BM [25], Relay-based network [7] and WWAOA-Resilient_consensus_BiLstm. In addition, comparative approaches considered to show DSMFHN's effectiveness are ERF-KMC [26], PDAM [16], EEHE [27] and SDA-RDOS [28].

F. Comparative Evaluation

The comparison estimation of Improved WWAOA and DSMFHN is performed regarding BoT-IoT and NSL-KDD datasets.

1) Analysis regardingBoT-IoT dataset: The analysis of Improved WWAOA is accomplished for 50 nodes by varying number of rounds and evaluation of DSMFHN is accomplished regarding training data.

a) Assessment regarding 50 nodes

Fig. 8 describes an analysis of Improved WWAOA according to performance metrics by changing number of rounds. In this section, values attained by comparative methods and Improved WWAOA for number of rounds=910 are interpreted. Fig. 8(a) shows an estimation of Improved WWAOA concerning delay. Improved WWAOA achieved delay of 0.627ms whereas ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM achieved 0.956, 0.797, 0.777, 0.725 and 0.653. This improvement is due to the algorithm's ability to optimize task scheduling and minimize latency during communication. Efficient node selection and routing paths also contributed to reduced delays. Assessment of Improved WWAOA regarding energy is delineated in Fig. 8(b). Energy achieved by ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM is 0.071J, 0.088J, 0.088J, 0.100J and 0.127J whereas Improved WWAOA attained 0.130J. This is achieved by balancing the workload across nodes and utilizing optimal routes to conserve energy. The adaptive approach of algorithm ensures minimal energy depletion. Fig. 8(c) exposes evaluation of Improved WWAOA with regards to PDR. PDR acquired by Improved WWAOA is 92.903% while PDR achieved by ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM is 76.109%, 79.461%, 84.259%, 86.906% and 91.984%. The improvement is attributed to robust routing protocols and efficient handling of packet retransmissions, ensuring reliable data delivery. Analysis of Improved WWAOA in relative of trust is exhibited in Fig. 8(d). ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM attained 68.473, 68.916, 74.831, 78.780 and 85.377 whereas Improved WWAOA obtained trust of 87.093. This enhancement stems from the algorithm's effective trust evaluation mechanism, which considers both direct and indirect trust factors to ensure secure and reliable node interactions.

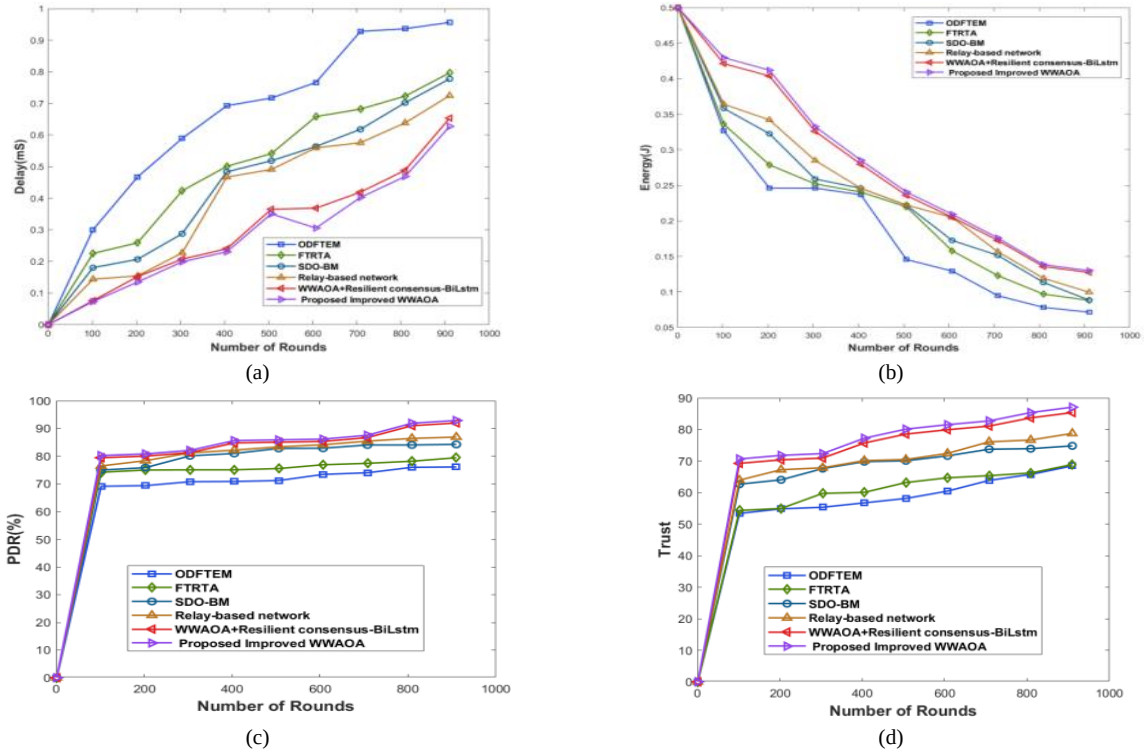

Fig. 8. Comparative analysis of Improved WWAOA regarding BoT-IoT dataset, a) Delay, b) Energy, c) PDR, d) Trust

b) Assessment regarding training data

Evaluation of DSMFHN with regards to metrics by changing training data is indicated in Fig. 9. This part represents the values obtained by classical schemes and DSMFHN for 90% of training data. Fig. 9(a) displays the estimation of DSMFHN with consideration of accuracy. The acquired accuracy by DSMFHN is 92.598% whereas ERF-KMC, PDAM, EEHE, and SDA-RDOS obtained 85.726%, 86.942%, 87.908%, and 88.918%. This shows an improvement in performance by 7.422%, 6.109%, 5.065% and 3.975%. Estimation of DSMFHN regarding FPR is revealed in Fig. 9(b). FPR acquired by DSMFHN is 0.156 while ERF-KMC, PDAM, EEHE, and SDA-RDOS attained 0.192, 0.186, 0.162 and 0.161. Fig. 9(c) interprets an analysis of DSMFHN with respect to TPR. TPR attained by DSMFHN is 91.643% whereas ERF-KMC, PDAM, EEHE, and SDA-RDOS achieved 86.983%, 87.993%, 88.903%, and 89.132%. It manifests enhancement of performance by 5.085%, 3.983%, 2.990% and 2.741%.

2) Analysis Regarding NSL-KDD Dataset: An Improved WWAOA is evaluated based on 50 nodes by changing number of rounds and DSMFHN is assessed in terms of training data.

a) Assessment regarding 50 nodes

Assessment of Improved WWAOA with relation to measures by varying number of rounds is illustrated in Fig. 10. The values obtained by traditional models and Improved WWAOA while number of rounds=910 are explicated in this section. Fig. 10(a) reveals estimation of Improved WWAOA regarding delay. Delay achieved by Improved WWAOA is 0.557ms while delay obtained by ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM is 0.947ms, 0.848ms, 0.835ms, 0.660ms and 0.592ms. The significant reduction in delay is attributed to the optimization of communication overheads and efficient round management. Evaluation of Improved WWAOA based upon energy is described in Fig. 10(b). ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM obtained 0.072J, 0.075J, 0.084J, 0.097J and 0.179J whereas Improved WWAOA achieved energy of 0.182J. The increased energy usage reflects the trade-off for achieving higher performance metrics, indicating the system's robustness. Fig. 10(c) signifies an assessment of Improved WWAOA by means of PDR. Improved WWAOA attained PDR of 93.894% whereas ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM obtained76.790%, 80.420%, 84.067%, 87.072% and 92.965%. This improvement highlights the model's efficiency in delivering packets reliably, even under varying network conditions. Estimation of Improved WWAOA in respective of trust is indicated in Fig. 10(d). Trust acquired by ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM is 66.712, 67.722, 73.733, 77.285 and 85.435 whereas Improved WWAOA achieved 87.152. The enhanced trust score demonstrates the robustness and reliability of the proposed model in maintaining secure and trustworthy communication across rounds.

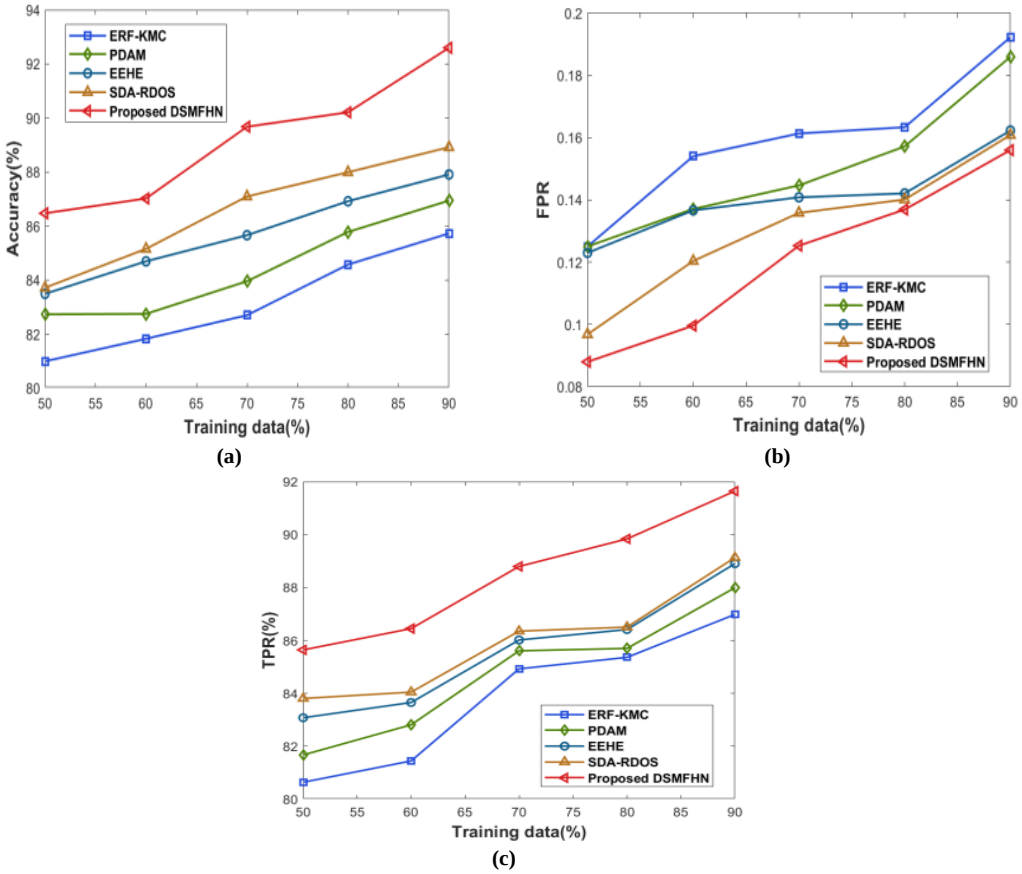

Fig. 9. Comparative assessment of DSMFHN regarding BoT-IoT dataset, a) Accuracy, b) FPR, c) TPR

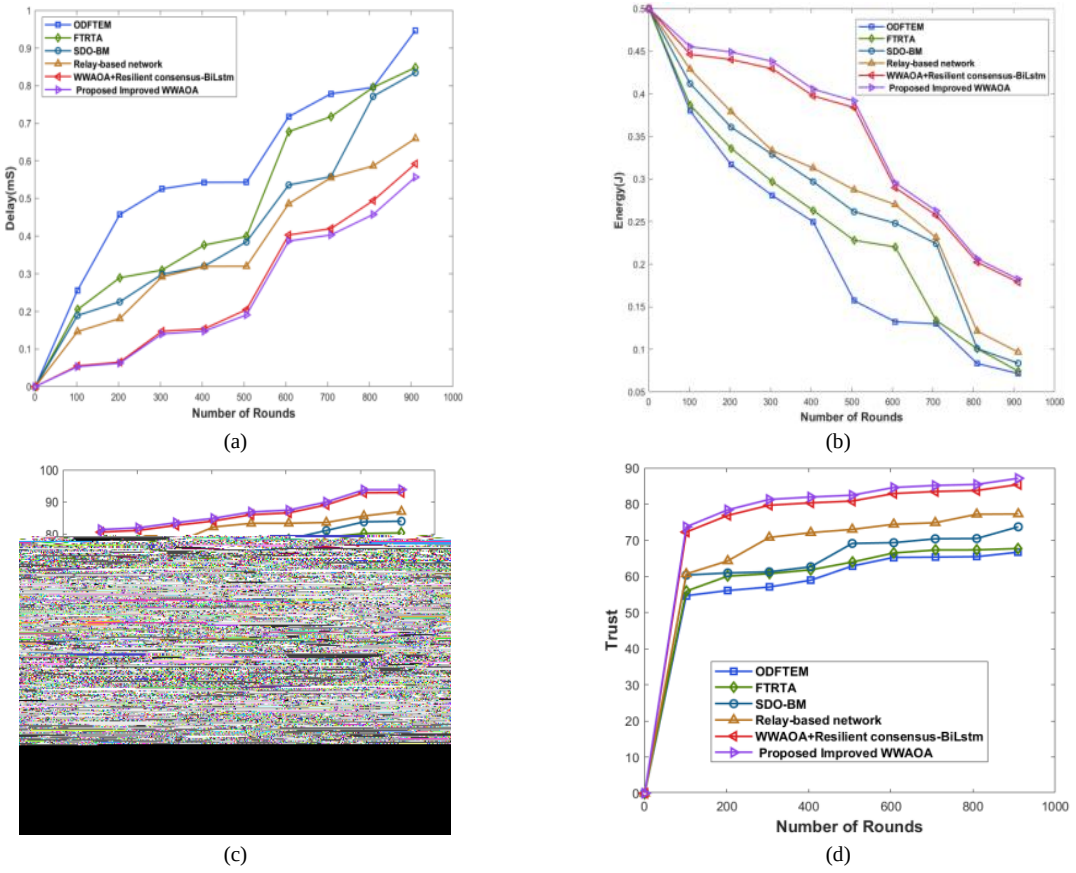

Fig. 10. Comparative analysis of Improved WWAOA regarding NSL-KDD dataset, a) Delay, b) Energy, c) PDR, d) Trust

b) Assessment regarding training data

Fig. 11 presents an estimation of DSMFHN with relation to metrics by varying training data. This section manifests the values attained by classical approaches and DSMFHN while training data is 90%. Assessment of DSMFHN with regarding to accuracy is described in Fig. 11(a). DSMFHN acquired accuracy of91.708% whereas ERF-KMC, PDAM, EEHE and SDA-RDOS attained 85.897%, 87.333%, 87.662% and 88.576%. This explains enhancement in performance by 6.336%, 4.770%, 4.412% and 3.415%. The superior accuracy reflects the model's capability to generalize effectively across the dataset. Analysis of DSMFHN with relation to FPR is signified in Fig. 11(b). ERF-KMC, PDAM, EEHE and SDA-RDOS acquired 0.214, 0.202, 0.198 and 0.192 whereas DSMFHN obtained FPR of 0.156. The reduced FPR indicates better precision in distinguishing true negatives from false positives. Fig. 11(c) depicts an evaluation of DSMFHN considering TPR. TPR attained by DSMFHN is 91.792% while ERF-KMC, PDAM, EEHE and SDA-RDOS acquired 85.118%, 87.217%, 88.475% and 89.493%. It mentions performance improvement by 7.271%, 4.984%, 3.614% and 2.504%. It showcases the model's strength in correctly identifying true positives.

G. Comparative Discussion

Table III mentions the assessment values acquired by ODFTEM, FTRTA, SDO-BM, Relay-based network, WWAOA-based Resilient Consensus BiLSTM and Improved WWAOA. When number of rounds=910, delay achieved by Improved WWAOA is 0.557ms whereas ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM acquired 0.947ms, 0.848ms, 0.835ms, 0.660ms and 0.592ms. A minimal delay obtained by Improved WWAOA reveals that it enhanced efficiency and speed of data transfer across the networks. For number of rounds=910, ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM achieved energy of 0.072J, 0.075J, 0.084J, 0.097J and 0.179J while Improved WWAOA attained 0.182J. A high energy illustrates that Improved WWAOA enhanced battery life and assured the sustainability of network. Improved WWAOA acquired PDR of 93.894% while number of rounds=910 whereas ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM obtained 76.790%, 80.420%, 84.067%, 87.072% and 92.965%. A maximum PDR indicates that Improved WWAOA ensured higher proportion of the DPs sent from source node to reach their destination. When considering number of rounds=910, trust obtained by ODFTEM, FTRTA, SDO-BM, Relay-based network and WWAOA-based Resilient Consensus BiLSTM is 66.712, 67.722, 73.733, 77.285 and 85.435 while Improved WWAOA attained 87.152. The attained high trust specifies that Improved WWAOA made better routing decisions and avoided routing by means of distrustful nodes. These outcomes clearly prove the effectiveness of Improved WWAOA for identifying shorter path for transmission of data. Moreover, Improved WWAOA acquired minimum delay of 0.557ms as well as maximum energy, PDR and trust of 0.182J, 93.894% and 87.152 for NSL-KDD dataset while number of rounds=910.

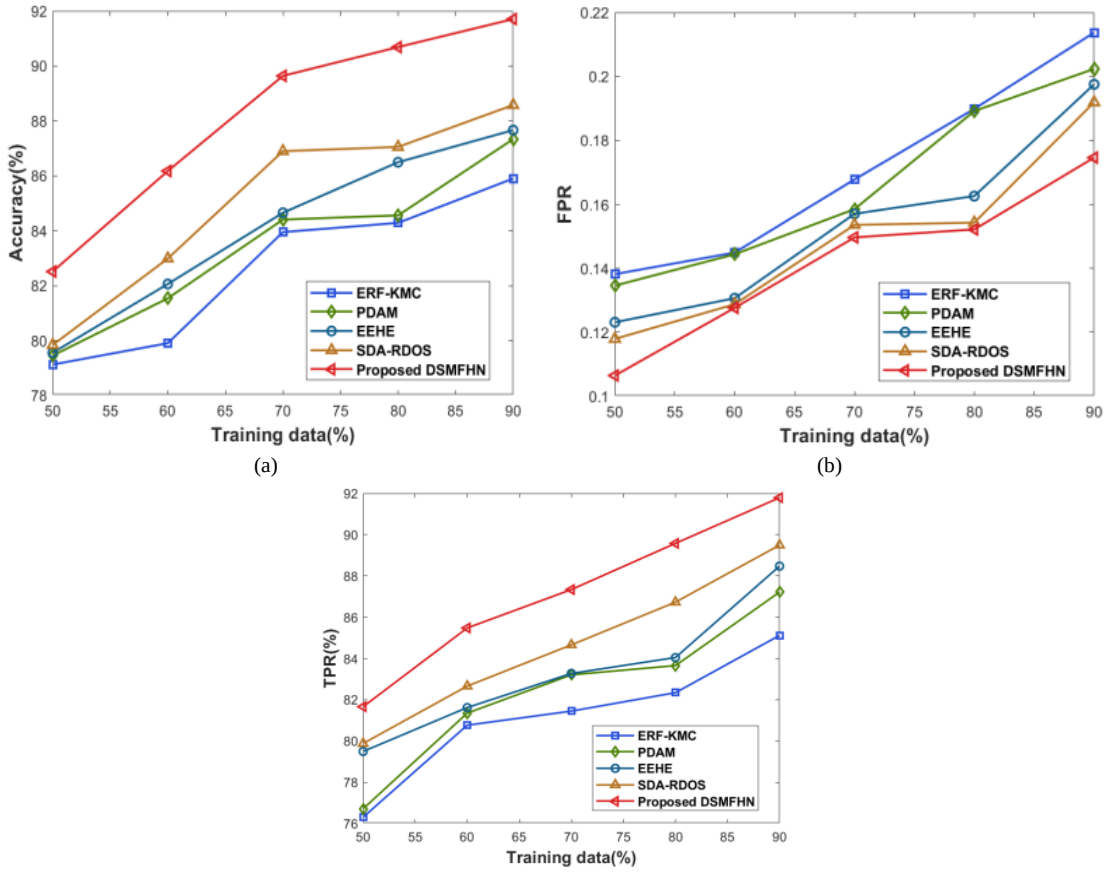

Fig. 11. Comparative analysis of DSMFHN regarding NSL-KDD dataset, a) Accuracy, b) FPR, c) TPR

TABLE III. COMPARATIVE DISCUSSION OF IMPROVED WWAOA

Setups	Metrics/ Methods	ODFTEM	FTRTA	SDO-BM	Relay-based network	WWAOA+Resilientconsensus_BiLSTM	Proposed WWAOA
BoT-IoT dataset	*Delay (ms)*	0.956	0.797	0.777	0.725	0.653	**0.627**
	Energy (J)	0.071	0.088	0.088	0.100	0.127	**0.130**
	PDR (%)	76.109	79.461	84.259	86.906	91.984	**92.903**
	Trust	68.473	68.916	74.831	78.780	85.377	**87.093**
NSL-KDD dataset	*Delay (ms)*	0.947	0.848	0.835	0.660	0.592	**0.557**
	Energy (J)	0.072	0.075	0.084	0.097	0.179	**0.182**
	PDR (%)	76.790	80.420	84.067	87.072	92.965	**93.894**
	Trust	66.712	67.722	73.733	77.285	85.435	**87.152**

The discussion of attack detection approaches such as ERF-KMC, PDAM, EEHE, SDA-RDOS, and designed DSMFHN for conducted evaluations are elaborated in Table IV. For considered training data=90%, the accuracy obtained by DSMFHN is 92.598% whereas ERF-KMC, PDAM, EEHE, and SDA-RDOS obtained 85.726%, 86.942%, 87.908%, and 88.918%. A maximum accuracy represents that DSMFHN efficiently identified and responded to various security risks with a higher level of precision. FPR acquired by DSMFHN is 0.156 while training data is 90% whereas ERF-KMC, PDAM, EEHE, and SDA-RDOS obtained 0.192, 0.186, 0.162, and 0.161. The minimum FPR specifies that DSMFHN reduced unnecessary alerts and ensured genuine risks were addressed and identified promptly. When training data=90%, TPR achieved by DSMFHN is 91.643% while ERF-KMC, PDAM, EEHE, and SDA-RDOS achieved 86.983%, 87.993%, 88.903%, and 89.132%. A high TPR achieved by DSMFHN ensured that it identified and mitigated the actual attacks efficaciously. It can be recognized that DSMFHN is the best model for detecting attacks in healthcare IoT. Furthermore, DSMFHN obtained maximal accuracy and TPR of 92.598% and 91.643% as well as minimal FPR of 0.156 for BoT-IoT dataset while training data is 90%.

The advantages of the designed method are discussed as follows. The Improved WWAOA enhances secure routing by optimizing fitness parameters, such as LLT, energy, trust, delay, distance, and fault tolerance. The devised algorithm minimizes delay, which is crucial for healthcare IoT applications. The DSMFHN ensures reliable communication by achieving high PDR and trust level. The BiLSTM with adaptive weightage used to improve fault tolerance and reduce the impact of malevolent nodes during data aggregation. Additionally, the algorithm is designed to handle complex IoMT environments with multiple devices, making it suitable for large-scale healthcare networks.

TABLE IV. COMPARATIVE DISCUSSION OF DSMFHN

Setups	Metrics/ Methods	ERF-KMC	PDAM	EEHE	SDA-RDOS	Proposed DSMFHN
BoT-IoT dataset	*Accuracy (%)*	85.726	86.942	87.908	88.918	**92.598**
	FPR	0.192	0.186	0.162	0.161	**0.156**
	TPR (5)	86.983	87.993	88.903	89.132	**91.643**
NSL-KDD dataset	*Accuracy (%)*	85.897	87.333	87.662	88.576	**91.708**
	FPR	0.214	0.202	0.198	0.192	**0.175**
	TPR (%)	85.118	87.217	88.475	89.493	**91.792**

VI. CONCLUSION

Healthcare is one of the excellent applications of IoT. Owing to diverse challenges, the healthcare domain has become a discussion point for addressing several features of IoT in past years. Recently, several conventional models developed for healthcare IoT have experienced distinctive security challenges due to various attacks. In this research, DSMFHN is introduced for attack detection in healthcare IoT. Initially, simulation of IoMT system model is accomplished. Thereafter, CH selection and secure routing are performed employing Improved WWAOA that is devised by combining WWPA with AOA. Furthermore, fitness parameters taken into consideration for CH selection and secure routing are energy, LLT, distance, trust, delay, and fault tolerance. After that, attack detection is executed by DSMFHN, which is presented by merging SNN and DMN with harmonic analysis. Finally, data aggregation is done, wherein weights are identified by BiLSTM utilizing adaptive weightage based upon fault and malevolent nodes.

In addition, Improved WWAOA obtained a minimum delay of 0.557ms as well as maximal energy, PDR, and trust of 0.182J, 93.894%, and 87.152 for number of rounds=910 for NSL-KDD dataset. Furthermore, DSMFHN achieved maximum accuracy and TPR of 92.598% and 91.643% as well as minimum FPR of 0.156 for BoT-IoT dataset while training data is 90%. In the future, an efficacy of introduced scheme will be evaluated for identifying IoMT attacks utilizing blockchain technology.

VII. FUTURE WORK

In the future, this study will be extended to explore the integration of advanced federated learning techniques, aiming to further enhance data privacy and security within IoMT environments. Additionally, the scalability of the proposed methods will be assessed in large-scale IoMT networks comprising heterogeneous devices. Finally, real-world deployment and validation of the proposed system will be conducted in diverse healthcare scenarios to ensure its practical feasibility and effectiveness.

REFERENCES

[1] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," in *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707-8718, 2021, doi: 10.1109/JIOT.2020.3045653.

[2] S. Razdan and S. Sharma, "Internet of medical things (IoMT): Overview, emerging technologies, and case studies," *IETE technical review*, vol. 39, no. 4, pp. 775-788, 2022.

[3] N. Dilawar, M. Rizwan, F. Ahmad, and S. Akram, "Blockchain: securing internet of medical things (IoMT)," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, 2019.

[4] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdić, "Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine," in *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3810-3822, 2018, doi: 10.1109/JIOT.2018.2849014.

[5] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in internet of medical things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, p. e4049, 2022.

[6] J. P. A. Yaacoub *et al*., "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, pp. 581-606, 2020.

[7] J. K. R. Sastry, B. Ch, and R. R. Budaraju, "Implementing Dual Base Stations within an IoT Network for Sustaining the Fault Tolerance of an IoT Network through an Efficient Path Finding Algorithm," *Sensors*, vol. 23, no. 8, p. 4032, 2023.

[8] P. Sharma and P. K. Gupta, "Optimization of IoT-fog network path and fault tolerance in fog computing based environment," *Procedia Computer Science*, vol. 218, pp. 2494-2503, 2023.

[9] Z. Zeng, L. Chang, and Y. Liu, "A fault tolerance data aggregation scheme for fog computing," *International Journal of Information and Computer Security*, vol. 17, no. 3-4, pp. 351-364, 2022.

[10] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, "A Review on the Security of the Internet of Things: Challenges and Solutions," *Wireless Pers. Commun*., vol. 119, no. 3, pp. 2603–2637, 2021, doi: 10.1007/s11277-021-08348-9.

[11] J. Liu, Y. Liu, and Y. Zhang, "A Clustering-Based Data Collection Wireless Sensor Network Using Concurrent Transmission," in *IEEE Access*, vol. 12, pp. 135398-135410, 2024, doi: 10.1109/ACCESS.2024.3462743

[12] M. Sadrishojaei, N. J. Navimipour, M. Reshadi, and M. Hosseinzadeh, "A new preventive routing method based on clustering and location prediction in the mobile internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10652-10664, 2021.

[13] S. M. Amini and A. Karimi, "Two-level distributed clustering routing algorithm based on unequal clusters for large-scale Internet of Things networks," *The Journal of Supercomputing*, vol. 76, no. 3, pp. 2158-2190, 2020.

[14] M. Esmaeili, S. H. Goki, B. H. K. Masjidi, M. Sameh, H. Gharagozlou, and A. S. Mohammed, "Ml-ddosnet: Iot intrusion detection based on denial-of-service attacks using machine learning methods and nsl-kdd," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 8481452, 2022.

[15] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electronics*, vol. 9, no. 6, p. 916, 2020.

[16] J. Wang, L. Wu, S. Zeadally, M. K. Khan, and D. He, "Privacy-preserving data aggregation against malicious data mining attack for IoT-enabled smart grid," *ACM Transactions on Sensor Networks (TOSN)*, vol. 17, no. 3, pp. 1-25, 2021.

[17] R. Kozik, M. Choraś, M. Ficco, and F. Palmieri, "A scalable distributed machine learning approach for attack detection in edge computing environments," *Journal of Parallel and Distributed Computing*, vol. 119, pp. 18-26, 2019.

[18] S. Sadhwani, B. Manibalan, R. Muthalagu, and P. Pawar, "A lightweight model for DDoS attack detection using machine learning techniques," *Applied Sciences*, vol. 13, no. 17, p. 9937, 2023.

[19] J. Wang, Y. Liu, and H. Feng, "IFACNN: efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks," *Math. Biosci. Eng*, vol. 19, no. 2, pp. 1280-1303, 2022.

[20] T. V. Khoa *et al*., "Deep Transfer Learning: A Novel Collaborative Learning Model for Cyberattack Detection Systems in IoT Networks,"

in *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8578-8589, 2023.

[21] S. Kavitha and N. Uma Maheswari, "Network anomaly detection for NSL-KDD dataset using deep learning," *Information Technology in Industry*, vol. 9, no. 2, pp. 821-827, 2021.

[22] S. Abbasian Dehkordi, K. Farajzadeh, J. Rezazadeh, R. Farahbakhsh, K. Sandrasegaran, and M. Abbasian Dehkordi, "A survey on data aggregation techniques in IoT sensor networks," *Wireless Networks*, vol. 26, no. 2, pp. 1243-1263, 2020.

[23] P. Nalayini and V. Meena, "Optimization based Data Aggregation and Fault Tolerance with Energy Management for Fog Enabled Heterogeneous IoT Environment," *Research Square*, 2024.

[24] M. M. Vanani and P. K. Dehkordi, "FTRTA: Fault Tolerance and Reliable Transmissions Algorithm for IoT," *Research Square*, 2022.

[25] K. Aravind and P. K. R. Maddikunta, "Dingo optimization based cluster based routing in internet of things," *Sensors*, vol. 22, no. 20, p. 8064, 2022.

[26] A. A. J. Al-Abadi, M. B. Mohamed, and A. Fakhfakh, "Enhanced Random Forest Classifier with K-Means Clustering (ERF-KMC) for Detecting and Preventing Distributed-Denial-of-Service and Man-in-the-Middle Attacks in Internet-of-Medical-Things Networks," *Computers*, vol. 12, no. 12, p. 262, 2023.

[27] M. Kumar, M. Sethi, S. Rani, D. K. Sah, S. A. AlQahtani, and M. S. Al-Rakhami, "Secure Data Aggregation Based on End-to-End Homomorphic Encryption in IoT-Based Wireless Sensor Networks," *Sensors*, vol. 23, no. 13, p. 6181, 2023

[28] M. Dener, "SDA-RDOS: A New Secure Data Aggregation Protocol for Wireless Sensor Networks in IoT Resistant to DOS Attacks," *Electronics*, vol. 11, p. 4194, 2022.

[29] H. Peng, C. Wu, and Y. Xiao, "CBF-IDS: Addressing Class Imbalance Using CNN-BiLSTM with Focal Loss in Network Intrusion Detection System," *Applied Sciences*, vol. 13, no. 21, p. 11629, 2023.

[30] S. Moustakidis and P. Karlsson, "A novel feature extraction methodology using Siamese convolutional neural networks for intrusion detection," *Cybersecurity*, vol. 3, no. 1, p. 16, 2020.

[31] S. Saif, N. Yasmin, and S. Biswas, "Feature Engineering Based Performance Analysis of ML and DL Algorithms for Botnet Attack Detection in IoMT," *International Journal of System Assurance Engineering and Management*, vol. 14, pp. 512–522, 2023.

[32] M. Narang, A. Jatain, and N. Punetha, "A Study on Cyberattack Detection in IoMT Using Machine Learning Techniques," *SSRN Electronic Journal*, 2023.

[33] F. Khan *et al*., "A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT," *IEEE Transactions on Industrial Informatics*, vol. 19, pp. 10125–10132, 2023.

[34] S. S. Hameed *et al*., "A Hybrid Lightweight System for Early Attack Detection in the IoMT Fog," *Sensors (Basel, Switzerland)*, vol. 21, 2021.

[35] R. Punithavathi *et al*., "Crypto Hash Based Malware Detection in IoMT Framework," *Intelligent Automation & Soft Computing*, 2022.

[36] J. Nayak *et al*., "Extreme Learning Machine and Bayesian Optimization-Driven Intelligent Framework for IoMT Cyberattack Detection," *Journal of Supercomputing*, vol. 78, pp. 14866–14891, 2022.

[37] H. Alavizadeh, H. Alavizadeh, and J. Jang-Jaccard, "Deep q-learning based reinforcement learning approach for network intrusion detection", *Computers*, vol. 11, no. 3, p. 41, 2022.

[38] Z. Askari *et al*., "Energy-Efficient and Real-Time NOMA Scheduling in IoMT-Based Three-Tier WBANs," *IEEE Internet of Things Journal*, vol. 8, pp. 13975–13990, 2021.

[39] G. N. K. Reddy, M. S. Manikandan, N. V. L. N. Murty, and L. R. Cenkeramaddi, "Unified Quality-Aware Compression and Pulse-Respiration Rates Estimation Framework for Reducing Energy Consumption and False Alarms of Wearable PPG Monitoring Devices," *IEEE Access*, vol. 11, pp. 41708-41740, 2023.

[40] Z. A. Jaaz *et al*., "Optimization Technique Based on Cluster Head Selection Algorithm for 5G-Enabled IoMT Smart Healthcare Framework for Industry," *Paladyn, Journal of Behavioral Robotics*, vol. 13, pp. 99–109, 2022.

[41] H. A. Babaeer and S. A. Al-Ahmadi, "Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking," in *IEEE Access*, vol. 8, pp. 92098-92109, 2020.

[42] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, "Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review," *Journal of Network and Computer Applications*, vol. 190, p. 103118, 2021.

[43] R. Chaganti, A. Mourade, V. Ravi, N. Vemprala, A. Dua, and B. Bhushan, "A particle swarm optimization and deep learning approach for intrusion detection system in internet of medical things," *Sustainability*, vol. 14, no. 19, p. 12828, 2022.

[44] S. Hao, Y. Hong, and Y. He, "An Energy-Efficient Routing Algorithm Based on Greedy Strategy for Energy Harvesting Wireless Sensor Networks," *Sensors*, vol. 22, no. 4, p. 1645, 2022.

[45] Y. Pramitarini, R. H. Y. Perdana, K. Shim, and B. An, "DLSMR: Deep Learning-Based Secure Multicast Routing Protocol against Wormhole Attack in Flying Ad Hoc Networks with Cell-Free Massive Multiple-Input Multiple-Output," *Sensors*, vol. 23, no. 18, p. 7960, 2023.

[46] M. Z. Hussain, Z. M. Hanapi, A. Abdullah, M. Hussin, and M. I. H. Ninggal, "An efficient secure and energy resilient trust-based system for detection and mitigation of sybil attack detection (SAN)," *PeerJ Computer Science*, vol. 10, p. e2231, 2024.

[47] S. Azad, M. Mahmud, K. Z. Zamli, M. S. Kaiser, S. Jahan, and M. A. Razzaque, "iBUST: An Intelligent Behavioural Trust Model for Securing Industrial Cyber-Physical Systems," *Expert Systems with Applications*, vol. 238, pp. 121676, 2024

[48] K. Muthulakshmi, K. Kalirajan, J. Jean Justus, and P. Sivamalar, "QoS Aware Data Congestion Control Routing in Mobile Ad Hoc Networks for Intelligent Transportation Systems," *Tehnički vjesnik*, vol. 31, no. 1, pp. 240-246, 2024.

[49] J. Hu, X. Yang, and L.-X. Yang, "A Framework for Detecting False Data Injection Attacks in Large-Scale Wireless Sensor Networks," *Sensors*, vol. 24, no. 5, p. 1643, 2024.

[50] A. A. Abdelhamid *et al*., "Waterwheel plant algorithm: A novel metaheuristic optimization method," *Processes*, vol. 11, no. 5, p. 1502, 2023.

[51] F. A. Hashim, K. Hussain, E. H. Houssein, M. S. Mabrouk, and W. Al-Atabany, "Archimedes optimization algorithm: a new metaheuristic algorithm for solving optimization problems," *Applied intelligence*, vol. 51, pp. 1531-1551, 2021.

[52] S. V. Pingale and S. R. Sutar, "Remora based Deep Maxout Network model for network intrusion detection using Convolutional Neural Network features," *Computers and Electrical Engineering*, vol. 110, p. 108831, 2023.

[53] B. Alnajjar, A. M. Kadim, R. A. Jaber, N. A. Hasan, E. Q. Ahmed, M. S. M. Altaei, and A. L. Khalaf, "Wireless Sensor Network Optimization Using Genetic Algorithm," *Journal of Robotics and Control (JRC)*, vol. 3, no. 6, pp. 827-835, Nov. 2022.

[54] X. Zhao, L. Wang, M. Yang, Y. Chen, and J. Xiang, "A Novel Small-Sample Fault Diagnosis Method for Rolling Bearings via Continuous Wavelet Transform and Siamese Neural Network," in *IEEE Sensors Journal*, vol. 24, no. 15, pp. 24988-24996, 2024.

[55] W. Sun, F. Su, and L. Wang, "Improving deep neural networks with multi-layer maxout networks and a novel initialization method," *Neurocomputing*, vol. 278, pp. 34-40, 2019.

[56] Y. Fang, J. Gao, Z. Liu, and C. Huang, "Detecting Cyber Threat Event from Twitter Using IDCNN and BiLSTM," *Applied Sciences*, vol. 10, no. 17, p. 5922, 2020.

[57] S. Arora, I. Batra, A. Malik, A. K. Luhach, W. S. Alnumay, and P. Chatterjee, "SEED: Secure and energy efficient data-collection method for IoT network," *Multimedia Tools and Applications*, vol. 82, no. 2, pp. 3139-3153, 2023.

[58] A. Tehrani, M. Yadollahzadeh-Tabari, A. Zehtab-Salmasi, and R. Enayatifar, "Wearable sensor-based human activity recognition system employing bi-LSTM algorithm," *The Computer Journal*, vol. 67, no. 3, pp. 961-975, 2024.

[59] H. F. Mahdi and B. J. Khadhim, "Enhancing IoT Security: A Deep Learning and Active Learning Approach to Intrusion Detection," *Journal of Robotics and Control (JRC)*, vol. 5, no. 5, pp. 1525-1535, 2024.

[60] A. Jaddoa, "Integration of Convolutional Neural Networks and Grey Wolf Optimization for Advanced Cybersecurity in IoT Systems," *Journal of Robotics and Control (JRC)*, vol. 5, no. 4, pp. 1189-1202, 2024.

[61] BoT-IoT dataset is taken from "https://ieee-dataport.org/documents/bot-iot-dataset", accessed on July 2024.

[62] NSL-KDD dataset is taken from, "https://www.unb.ca/cic/datasets/nsl.html", accessed on July 2024.

[63] M. Anwer, S. M. Khan, and M. U. Farooq, "Attack detection in IoT using machine learning. Engineering," *Technology & Applied Science Research*, vol. 11, no. 3, pp. 7273-7278, 2021.

[64] M. Maray, S. M. Rizwan, E. Mustafa, and J. Shuja, "Microservices enabled bidirectional fault-tolerance scheme for healthcare internet of things," *Cluster Computing*, vol. 27, pp. 4621–4633, 2024.

[65] G. Sripriyanka and A. Mahendran, "Securing IoMT: A Hybrid Model for DDoS Attack Detection and COVID-19 Classification," *IEEE Access*, vol. 12, pp. 17328-17348, 2024.

[66] Y. Y. Ghadi *et al*., "Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review," in *IEEE Access*, vol. 12, pp. 12699-12719, 2024.

[67] Y. Y. Ghadi *et al*., "The role of blockchain to secure internet of medical things," *Scientific Reports*, vol. 14, pp. 18422, 2024.

[68] T. Mazhar, S. F. A. Shah, S. A. Inam, J. B. Awotunde, M. M. Saeed, and H. Hamam, "Analysis of integration of IoMT with blockchain: issues, challenges and solutions," *Discover Internet of Things*, vol. 4, no. 21, 2024.

[69] T. Mazhar *et al*., "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," *Brain Sciences*, vol. 13, no. 4, p. 683, 2023.

[70] T. Mazhar *et al.*, "Analysis of Cyber Security Attacks and Its Solutions for the Smart grid Using Machine Learning and Blockchain Methods," *Future Internet*, vol. 15, no. 2, p. 83, 2023.

[71] Y. Y. Ghadi, S. F. A. Shah, T. Mazhar, T. Shahzad, K. Ouahada, and H. Hamam, "Enhancing patient healthcare with mobile edge computing and 5G: challenges and solutions for secure online health tools," *Journal of Cloud Computing*, vol. 13, 2024.