bioengineering

MDPI

Article

Transforming Smart Healthcare Systems with AI-Driven Edge Computing for Distributed IoMT Networks

Maram Fahaad Almufareh [1,*], Mamoona Humayun [2,*] and Khalid Haseeb [3]

[1] Department of Information System, College of Computer and Information Sciences, Jouf University, Sakaka 72388, Al-Jouf, Saudi Arabia
[2] School of Computing, Engineering and the Built Environment, University of Roehampton, London SW15 5PH, UK
[3] Department of Computer Science, Islamia College Peshawar, Peshawar 25120, Pakistan; khalid.haseeb@icp.edu.pk
* Correspondence: mfalmufareh@ju.edu.sa (M.F.A.); mamoona.humayun@roehampton.ac.uk (M.H.)

Abstract

The Internet of Medical Things (IoMT) with edge computing provides opportunities for the rapid growth and development of a smart healthcare system (SHM). It consists of wearable sensors, physical objects, and electronic devices that collect health data, perform local processing, and later forward it to a cloud platform for further analysis. Most existing approaches focus on diagnosing health conditions and reporting them to medical experts for personalized treatment. However, they overlook the need to provide dynamic approaches to address the unpredictable nature of the healthcare system, which relies on public infrastructure that all connected devices can access. Furthermore, the rapid processing of health data on constrained devices often leads to uneven load distribution and affects the system's responsiveness in critical circumstances. Our research study proposes a model based on AI-driven and edge computing technologies to provide a lightweight and innovative healthcare system. It enhances the learning capabilities of the system and efficiently detects network anomalies in a distributed IoMT network, without incurring additional overhead on a bounded system. The proposed model is verified and tested through simulations using synthetic data, and the obtained results prove its efficacy in terms of energy consumption by 53%, latency by 46%, packet loss rate by 52%, network throughput by 56%, and overhead by 48% than related solutions.

Keywords: healthcare system; trustworthiness; cyber threats; security; smart technologies

Academic Editor: Andrea Cataldo

Received: 13 October 2025
Revised: 30 October 2025
Accepted: 7 November 2025
Published: 11 November 2025

Citation: Almufareh, M.F.; Humayun, M.; Haseeb, K. Transforming Smart Healthcare Systems with AI-Driven Edge Computing for Distributed IoMT Networks. *Bioengineering* **2025**, *12*, 1232. https://doi.org/10.3390/bioengineering12111232

1. Introduction

Distributed networks with cloud processing have enabled vital capabilities for real-time sensing and computing of data from the real world, as well as for communication standards [1,2]. Advancements in IoMT enable the timely collection and maintenance of patient data through wireless technologies and interconnected health devices. Such intelligent systems are nowadays more flexible and offer a diverse range of services to their networked users [3]. They integrate computational algorithms and physical components via the Internet of Things (IoT) to monitor and control complex health operations [4,5]. By fusing cutting-edge technologies and edge computing, many network applications transform the efficiency and productivity of crucial operations [6–8]. However, the increasing reliance on IoMT networks presents new challenges, particularly in ensuring the security of sensitive patient data and maintaining low-latency, real-time performance. The automated process, equipped with smart

sensors, not only meets the application's requirements but also reduces operational costs for controlling devices [9–11]. In recent decades, considerable efforts have been made by researchers to address the significant challenges in developing lightweight smart solutions that maintain the timely availability of network resources [12–14]. AI-based schemes are widely explored for effective decision making and timely responses to automate systems in critical environments, leading to sustainable growth for smart cities [15–17]. The emerging technologies in IoT-based operations demand data protection against cyber threats to maintain authorized access to sensitive health records, supported by trusted devices [18–20]. This research study explores AI-driven techniques to propose evaluation of trusted devices, network threats, and anomalies that are reduced, addressing cyber attacks and enabling more consistent, distributed development for emerging health technologies. The following research inquiries are addressed by our research study.

i. How can the proposed system ensure data privacy and integrity with AI-enabled techniques without affecting network resources?
ii. What methods can healthcare applications explore to decrease congestion and provide a responsive system by optimizing resources through efficient communication and network scalability?
iii. What kind of potential threats can be addressed by healthcare applications using an AI model to reduce unauthorized access and vulnerabilities to cyber attacks?

Based on the aforementioned research questions, our proposed work contributes the following developments.

i. Design and implementation of smart healthcare solution using AI-powered security for ensuring privacy of health records while affecting its integrity in a distributed environment.
ii. Edge computing is integrated for real-time processing and increases the scalability of the IoMT network while reducing congestion among health devices, and improves the responsiveness of the system in critical conditions.
iii. AI-based models are explored to ensure network availability and provide a lightweight communication paradigm for coping with network disruptions in the presence of cyber threats affecting healthcare services.

Our research work is organized in the following sub-sections. Related work is explained in the context of problem formulation in Section 2. Section 3 discusses the developed algorithms. The experiments and their results are discussed in Section 4. In conclusion, Section 5 presents the findings of this study.

2. Literature Review

Medical equipment with IoMT devices interacts through wearable sensors and emerging technologies to sense and process medical records in real-time environments [21,22]. The patient's data is collected by health sensors promptly and forwarded to the nearest processing devices. Later, cloud servers perform diagnostic operations on it, enabling the rapid identification of any disease with the consultation of healthcare experts. However, in the entire process, data security is a crucial phase to ensure accurate data collection at the processing edge and prevent any alteration due to cyber threats [23,24]. The effective measurement of security levels is crucial for protecting patient privacy and ensuring reliability in a critical environment. The use of decentralized processing of health data, supported by edge-level computing, enhances the efficiency of decision making at the point of care, without relying on distant cloud servers [25–27]. Ref. [28] enhanced the performance of MWSNs by integrating dual-tier clustering and virtual network zones. A Dual Tier Cluster-Based Routing (DTC-BR) protocol was proposed, which divides the network

into virtual zones for improved connectivity and selects specific nodes as cluster heads for optimal data transmission. The simulations were conducted in MATLAB to analyze DTC-BR and assess various network metrics, including lifetime, scalability, and energy consumption. To select the optimal phantom node and determine a secure routing path for source location privacy in an IoT-enabled blockchain healthcare, Ref. [29] proposed a novel Fractional Flamingo Archery Optimization (FFAO). It integrates various performance and multi-objective optimization parameters to enhance network security and reliability. Furthermore, an additional layer is integrated into FFAO with the support of blockchain technology, addressing factors such as distance, energy, trust, and heterogeneity, to enhance adaptability and security. The authors of [30], focusing on sustainability, introduced a software architecture to enhance the data collection process through efficient IoT-based communication. It provides QoS-aware routing and enhances the effective utilization of network resources in smart cities. During the data collection phase, Chaotic Bird Swarm Optimization (CBSO) is employed to form sensor clusters, while the Improved Differential Search (IDS) method assesses node reliability and selects the most trustworthy node as the Cluster Head. In the data transport phase, the system ensures data security through lightweight signcryption, while the Optimal Data Routing (ODM) technique enhances data transmission paths within the network. In Ref. [31], the authors presented a sink-mobility-based energy-efficient data dissemination (SEEDI) protocol for IoMT, designed to address the hot-spot problem in static wireless body area networks (WBANs). In SEEDI, four continuously energy-powered body sensor nodes are deployed at the periphery of a rectangular network to collect data from nearby patients. The sink collects data from these nodes, which in turn gather information from the patients. Cluster Head (CH) selection for each patient is performed using the Remora Optimization Algorithm (ROA), which optimizes fitness parameters to enhance energy efficiency. The expansion of the IoMT has improved the functionality, connectivity, and intelligence of medical practices. However, this increased interconnectivity has made IoMT networks vulnerable to cyber attacks, particularly Distributed Denial-of-Service (DDoS) attacks. Existing intrusion detection systems (IDSs) struggle to address these advanced threats due to the dynamic nature of IoMT traffic. The authors of Ref. [32] presented a hybrid deep-learning-based intrusion detection system (HIDS-IoMT) that combines Convolutional Neural Networks (CNNs) for feature extraction and Long Short-Term Memory (LSTM) networks for sequence prediction. The proposed IDS is implemented on a Raspberry Pi device using a fog computing architecture, enabling decentralized processing to enhance responsiveness and reduce latency. To improve the efficiency and security of patient record management, Ref. [33] proposed a framework, Healthcare System using Private Blockchain-based Cloud IoT (HSPBCI), aiming to limit access to medical data by unauthorized devices. Additionally, it enhances block-based transaction encryption and decryption times with minimal overhead. The cloud blockchain network is created to identify unauthorized devices and increase the trustworthiness of communication. Table 1 outlines the contributions and limitations of the existing approaches.

Table 1. Summary of research contributions and limitations.

Existing Approaches	Contributions	Limitations
DTC-BR Protocol [28]	Enhances MWSN performance using dual-tier clustering and virtual network zones. The protocol divides the network into two zones: the main connectivity zone (MCZ) and the candidate cluster zone (CCZ), thereby improving energy efficiency and scalability.	May not be effective in highly dynamic environments with frequent topology changes.
FFAO [29]	Integrates multi-objective optimization criteria to strengthen the network stability and reliability. It improved the routing process while selecting the optimal path for transmitting IoT data.	May face additional challenges such as overheads, and network delay in coping with resource optimization.
QoS-aware Routing Strategy [30]	Proposes a software architecture for data collection and communication in IoT-enabled smart applications, utilizing Chaotic Bird Swarm Optimization (CBSO) for cluster formation and Improved Differential Search (IDS) to assess node reliability.	High computational complexity during the data collection phase may result in increased overhead for real-time applications.
SEEDI Protocol [31]	Presents a sink-mobility-based energy-efficient data dissemination protocol for IoMT, designed to address the hot-spot problem in static WBANs. It deploys energy-powered nodes at the periphery to collect patient data and uses the Remora Optimization Algorithm (ROA) to select cluster heads.	Faces challenges in highly dynamic environments with fluctuating traffic patterns, which may hinder real-time data transmission.
HIDS-IoMT Protocol [32]	Introduces a hybrid deep learning-based intrusion detection system (HIDS-IoMT) combining CNN for feature extraction and LSTM for sequence prediction, implemented on a Raspberry Pi with fog computing for decentralized processing.	High computational demands of deep learning models may result in slow performance on resource-constrained devices in real-time deployments.
HSPBCI framework [33]	Improves the security level for healthcare system with blockchain network and effective key management for authorized data access.	Limited in network scalability and enhanced data latency while processing high amount of health records.

3. Materials and Methods

In this section, we present an AI-driven model that integrates security exploration via Support Vector Machines (SVMs) to improve the accuracy and resilience of innovative healthcare systems. The distributed network combines various electronic medical equipment, health sensors, and edge devices to ensure real-time data processing and secure information transmission. Figure 1 illustrates the architecture design of the proposed model, which comprises three main phases. Initially, IoT-based innovative systems are constructed to collect environmental data for analysis and processing. Secondly, edge-level local processing is performed to ensure the timely delivery and responsive communication. Ultimately, a secure interface is developed through trusted computation across devices, ensuring reliability in distributed systems. The significant components of the proposed methodology are discussed as follows.

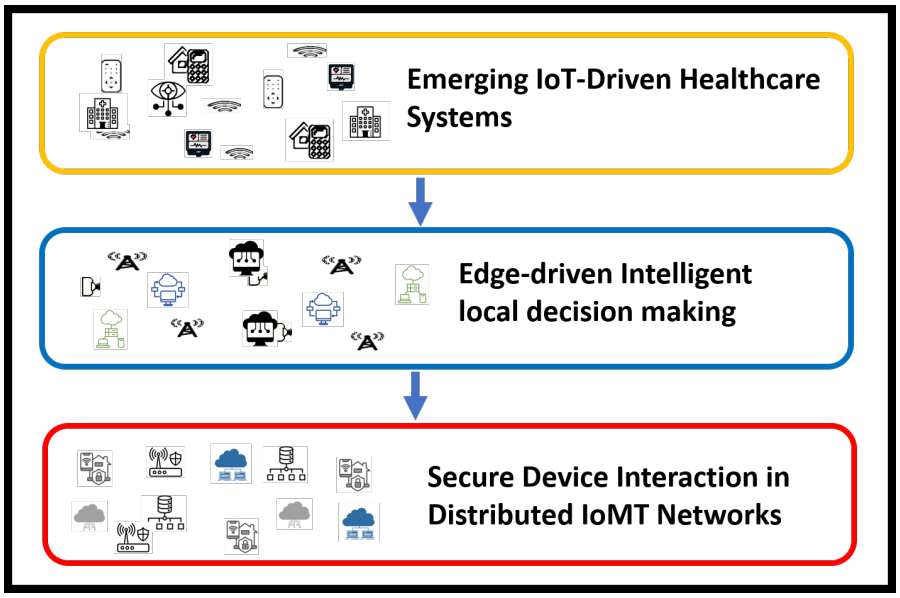

Figure 1. Phases of the proposed model for intelligent IoT communication with secure interfaces.

3.1. System Architecture for Distributed IoMT Networks

Our system architecture is composed of health sensors $D = \{d_1, d_2, \ldots, d_n\}$, edge nodes $E = \{e_1, e_2, \ldots, e_m\}$ that perform local processing and reduce the additional consumption of resources of constraint devices. Equations (1) and (2) model the devices, edge nodes, and the cloud for optimized communication and decrease the network overhead.

$$x_i \rightarrow e_j \quad \forall d_i \in D, \forall e_j \in E \tag{1}$$

$$e_j \rightarrow \text{Cloud} \quad \forall e_j \in E \tag{2}$$

The communication latency L between health devices and the cloud can be expressed using edge-level processing as given in Equation (3).

$$L = \frac{D}{R} + T_{proc} \tag{3}$$

where data size is denoted by D, communication rate is denoted by R, and processing time at the edge or cloud is represented by T_{proc}. The objective function F as given in Equations (4) and (5) aims to minimize the communication latency and energy consumption in the IoMT system, with α as a weight factor to balance both terms. The model is subject to a constraint on the total data load in the network.

$$F = \sum_{i=1}^{n} \left(\frac{d_i \in D}{R} + T_{\text{proc}} \right) + \alpha \sum_{i=1}^{n} E_i, \tag{4}$$

$$\text{subject to} \quad \sum_{i=1}^{n} d_i \leq C \tag{5}$$

3.2. AI-Enabled Secure Edge System for Distributed Decision Making

In this section, the proposed model enhances the security of a distributed system by leveraging Support Vector Machines (SVMs) to detect network anomalies. Based on the selected features, the SVM classifier classifies IoMT traffic into normal or anomalous groups. The decision function of the SVM classifier is defined in Equation (6).

$$f(\mathbf{x}) = \text{sign}\left(w^T x + b \right) \tag{6}$$

where $f(\mathbf{x})$ is the output of the classifier, x is the input feature vector, w is the weight vector, and b is the bias term. Based on the selected features, the SVM classifier classifies IoMT traffic into normal or anomalous groups. The decision function of the SVM classifier is defined in Equation (7).

$$f(\mathbf{x}) = \text{sign}(w_1 \cdot x_1 + w_2 \cdot x_2 + \cdots + w_n \cdot x_n + b) \tag{7}$$

where

- $f(\mathbf{x})$ is the classifier output (normal or anomalous).
- $\mathbf{x} = [x_1, x_2, \ldots, x_n]$ is the feature vector, which includes:
  - packet size (x_1) and transmission rate (x_2);
  - response time (x_3) and data flow patterns (x_4);
  - and other network characteristics.
- w_i is the weight associated with each feature x_i, and b is the bias term.

The final classification outcome is determined by the contribution of each feature, where the significance of each feature is captured by its corresponding weight w_i in the detection of anomalies for a distributed IoMT system. The decision function, as shown in Equation (8), computes the weighted sum of the features x_i along with the bias term b, and the classification is made based on the sign of the resulting value.

$$f(\mathbf{x}) = \text{sign}\left(\sum_{i=1}^{n} w_i \cdot x_i + b\right) \tag{8}$$

Algorithm 1 governs the anomaly detection using an SVM classifier for an IoMT-based healthcare system.

Algorithm 1: Anomaly detection using SVM for IoMT traffic.

Input: IoMT traffic features (Packet size x_1, Transmission rate x_2, Response time x_3, Data flow patterns x_4)
Output: Anomaly detection in Distributed Network

```
Function SVM_Anomaly_Detection(x):
    x1, x2, x3, x4 ← Extract features from IoMT traffic;
    x ← [x1, x2, x3, x4];
    Prediction ← SVM(x);
    ;     // Use the SVM classifier to detect anomalies based on input features.
    if Prediction = Anomalous then
        ;  // Flag traffic as anomalous if the prediction is anomalous.
        Flag as anomalous;
    else
        ;        // Flag traffic as normal if the prediction is normal.
        Flag as normal;
    return Prediction;
```

3.3. Integrating Edge Computing for Scalable IoMT System

In the next phase, edge computing is integrated into local devices to reduce latency and improve the efficacy of the proposed model. It improves system scalability by performing

processing locally and reduces data transmission to the cloud. The decision to offload tasks is based on the optimization criterion, as defined in Equation (9):

$$O(F) = \arg\min\left(L_{cloud} + E_{cloud}, L_{edge} + E_{edge}\right) \tag{9}$$

where L_{cloud}, L_{edge} represent the latency for cloud and edge processing, respectively, and E_{cloud}, E_{edge} are the energy consumption for cloud and edge processing. Furthermore, to ensure accurate edge processing, Equation (10) defines the error function.

$$E_{edge} = \frac{1}{n}\sum_{i=1}^{n}(f(x_i) - y_i)^2 \tag{10}$$

where

- E_{edge} is the error function measuring the performance of the edge node in processing the data.
- $f(x_i)$ is the predicted output for the input feature x_i, and y_i is the actual value.

Algorithm 2 presents a secure approach for task offloading and maintaining the authentic health services.

Algorithm 2: Edge computing for task offloading and error minimization.

Input: Task features: $L_{cloud}, L_{edge}, E_{cloud}, E_{edge}$
Output: Offloading decision and edge processing result

```
Function Edge_Offloading_Decision(F):
    Extract the features L_cloud, L_edge, E_cloud, E_edge from the input data F;
    Determine the offloading decision O by comparing latency and energy for
     cloud and edge processing;
    if Offload to edge then
        Process the task locally at the edge;
    else
        Offload the task to the cloud;
    Calculate the edge processing error E_edge;
    if Error is below threshold then
        Trust the edge processing;
    else
        Flag the task for review;
    return Offloading decision and edge processing error;
```

The proposed model achieves cyber resilience through system response and the timely detection of network threats by computing the resilience metric R_c. Equation (11) determines the detection time for N cyber attacks using the sum of individual detection times $T_{detection,i}$.

$$T_{detection} = \sum_{i=1}^{N}(t_{detected,i} - t_{start,i}) \tag{11}$$

where

- $t_{detected,i}$ is the time of detection for the i-th attack.
- $t_{start,i}$ is the time the i-th attack starts.
- $t_{detected}$ is the time when the system identifies the attack.
- t_{start} is the time when the attack begins.

On the other hand, the mitigation time $T_{mitigation}$ is the time taken to neutralize the attack and restore normal operations, as defined in Equation (12).

$$T_{mitigation} = \max(t_{restored} - t_{detected}) \tag{12}$$

where

- $t_{restored}$ is the time when the system returns to normal operation after mitigation.
- $t_{detected}$ is the time when the attack is first detected.

Equation (13) defines the cyber resilience metric R_c, which is generalized to account for multiple attack events and their respective detection and mitigation times.

$$R_c = \frac{\sum_{i=1}^{N_a} \left(T_d^{(i)} + T_m^{(i)} \right)}{T_{total}} \tag{13}$$

where

- N_a is the number of detected attack events.
- $T_d^{(i)}$ is the detection time for the i^{th} attack.
- $T_m^{(i)}$ is the mitigation time for the i^{th} attack.
- T_{total} is the system's total operational time, including both normal and attack-response phases.

Algorithm 3 outlines the procedure for computing the cyber resilience metric R_c in a distributed IoMT system.

Algorithm 3: Cyber resilience evaluation for distributed IoMT system.

Input: Attack events: $t_{start,i}$, $t_{detected,i}$, $t_{restored,i}$ for $i = 1 \ldots N_a$; Total time T_{total}
Output: Resilience metric R_c

Function `Evaluate_Cyber_Resilience(`$\mathcal{A}$`):`
  $T_{detection} \leftarrow 0$, $T_{mitigation} \leftarrow 0$;
  ; `// Detection time computation.`
  for $i \leftarrow 1$ ***to*** N_a **do**
    $T_{detection} \leftarrow T_{detection} + (t_{detected,i} - t_{start,i})$;
  ; `// Mitigation time computation.`
  for $i \leftarrow 1$ ***to*** N_a **do**
    $T_{mitigation} \leftarrow T_{mitigation} + (t_{restored,i} - t_{detected,i})$;
  ; `// Resilience metric calculation.`
  $R_c \leftarrow \frac{T_{detection} + T_{mitigation}}{T_{total}}$;
  if $R_c \leq \theta_{resilience}$ **then**
    System resilient;
  else
    Resilience degraded;
  return R_c;

4. Simulation Configuration

In this section, we evaluate the proposed model and baseline solutions under controlled simulation scenarios. Simulations are performed in a 3000×3000 m area with IoT sensors and edge nodes. We vary the number of malicious nodes from 10 to 20 to assess

the impact of privacy and security attacks on the system. Each configuration is executed 50 times independently and logged; the simulation round interval is 25 s. The simulation time per run is set to $T_{sim} = 3000$. Table 2 summarizes the default simulation parameters used in the experiments.

Table 2. Simulation parameters.

Parameter	Value/Description
Simulation area	3000×3000 m
Simulation duration	3000 s
Number of executions	50 independent runs
Round interval	25 s
Sensor nodes	20, 50, 100, 150, 200
Edge nodes	15
Sink nodes	3
Malicious nodes	5–15
Mobility model	Random waypoint
Packet size	128–1024 bytes
Transmission power	3–15 m
Initial energy	5000 mJ

Discussion

A significant improvement was noticed in terms of packet drop ratio by an average of 49% and 54% compared to existing methods, as shown in Figures 2 and 3. This is made possible by utilizing edge-based computing and performing local processing with a low computational cost. A distributed decision-making approach is employed, utilizing SVM-based anomaly detection, while efficiently managing resources and optimizing the utilization of communication links. Moreover, the computation of cyber threats helps identify the most stable forwarding paths, thereby ensuring higher data reception at the destination. The security mechanisms embedded in the model prevent malicious devices from sending false route request packets, thereby reducing the risk of malicious traffic in the IoMT network. Its network throughput is compared with existing schemes in Figures 4 and 5. The proposed model achieves average throughput improvements of 48% and 54% across varying sensor densities and transmission ranges, respectively. This improvement can be attributed to the integration of dynamic strategies that leverage distributed decision making and real-time data processing. The routing paths are optimized using a dynamic, weighted objective function that considers multiple feature extractions. Security policies are continuously updated via distributed evaluations, ensuring that unreliable or malicious nodes are excluded from the data-forwarding process. Figures 6 and 7 illustrate the energy consumption performance of the proposed model and existing work under varying sensor densities and transmission ranges. Upon comparison, the proposed model demonstrates a significant improvement in energy efficiency, reducing the additional usage of network resources by an average of 50% and 57%, respectively. This enhancement is attributed to the integration of SVM classifier-based anomaly detection, AI-driven edge decision making, and real-time data processing. The devices are continuously monitored at the edge, and an SVM classifier identifies potential cyber threats based on abnormal data patterns or malicious behavior. When such threats are detected, the system reformulates the communication routes by exploring surrounding environmental conditions and adjusting node parameters. Also, the edge nodes are responsible for validating the identities of connected devices before forwarding data to the cloud. Figures 8 and 9 compare the proposed model to existing approaches in terms of network overhead. Node overhead is a critical consideration when designing and implementing IoT-enabled distributed networks, especially

in resource-constrained environments. The experimental analysis demonstrates that the proposed model reduces node overhead by an average of 44% and 52% under varying sensor densities and transmission ranges. This improvement is attributed to learning-based decision making, which involves exploring various feature extractions of the device under dynamic conditions. This approach uses distributed, real-time decision-making algorithms to optimize communication and resource management at the edge. In Figures 10 and 11, the performance analysis of the proposed model is compared for latency over varying transmission ranges and health sensors. The results analysis reveals an improvement of the proposed model by an average of 42 and 50% and 49%, respectively. This is made possible through the exploration of the SVM algorithm for network intelligence and communication detection, utilizing key and dynamic features such as response time, data size, and data flow patterns, in healthcare applications. It timely detects unauthorized access in the system and reduces abnormal device behavior, ultimately improving the efficient delivery of health records. In addition, resources are utilized in a balanced manner, and their consumption is reduced to tackle network congestion and mitigate overloaded routes for the transmission of crucial e-health data.

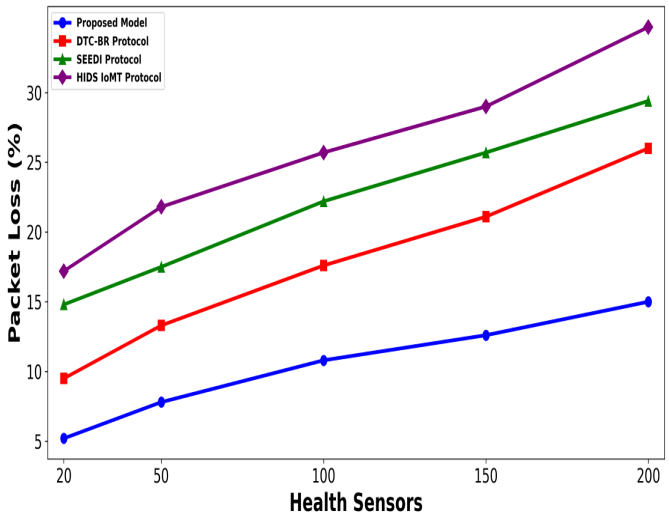

Figure 2. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for packet drop ratio under varying health sensors.

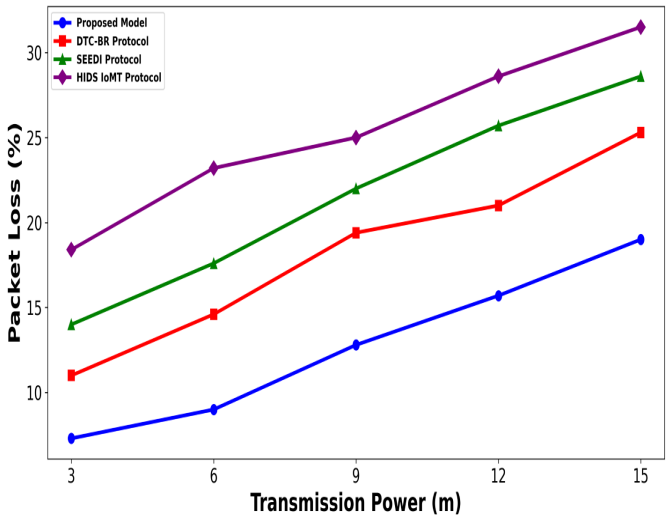

Figure 3. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for packet drop ratio under varying transmission range.

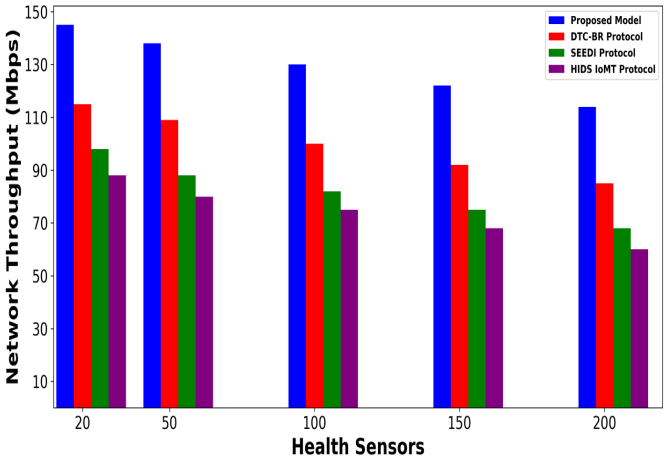

Figure 4. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for network throughput under varying health sensors.

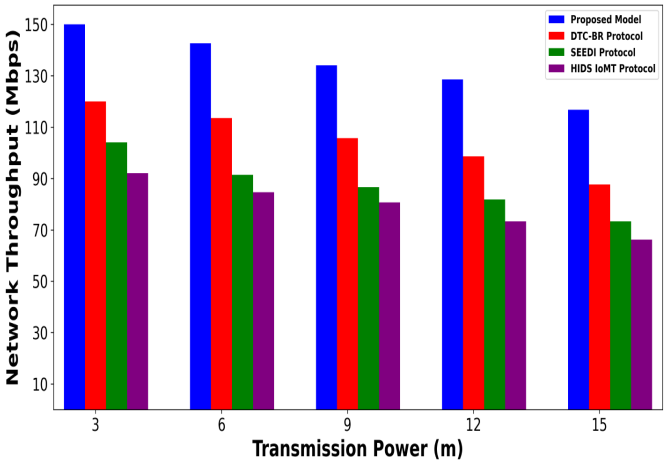

Figure 5. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for network throughput under varying transmission range.

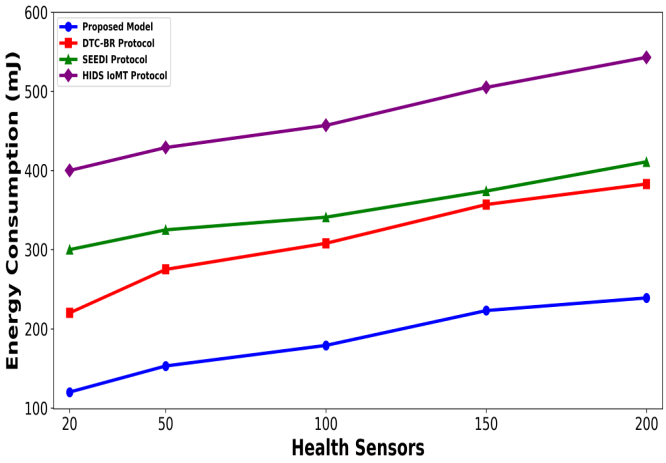

Figure 6. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for energy consumption under varying health sensors.

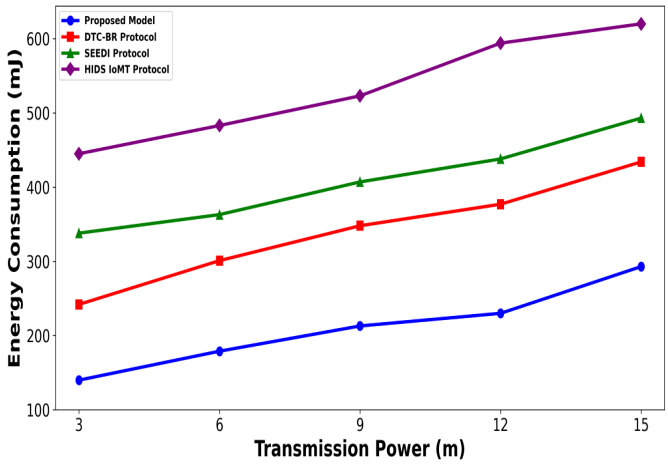

Figure 7. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for energy consumption under varying transmission range.

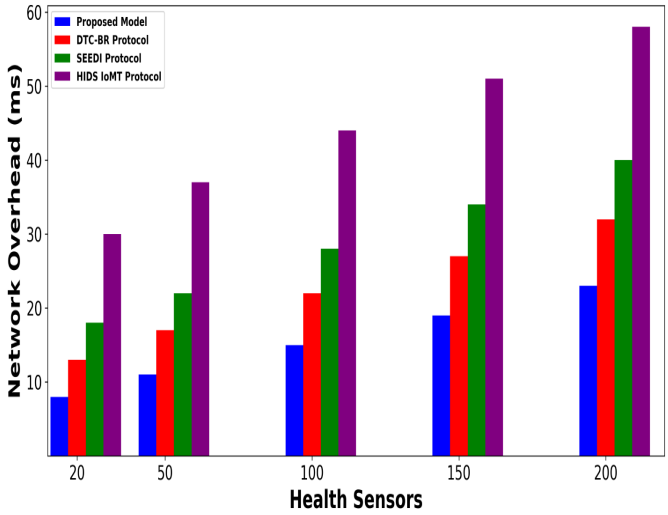

Figure 8. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for network overhead under varying health sensors.

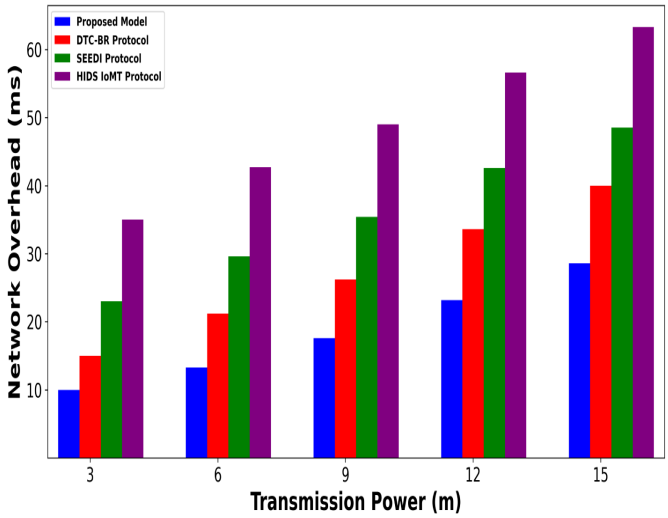

Figure 9. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for network overhead under varying transmission range.

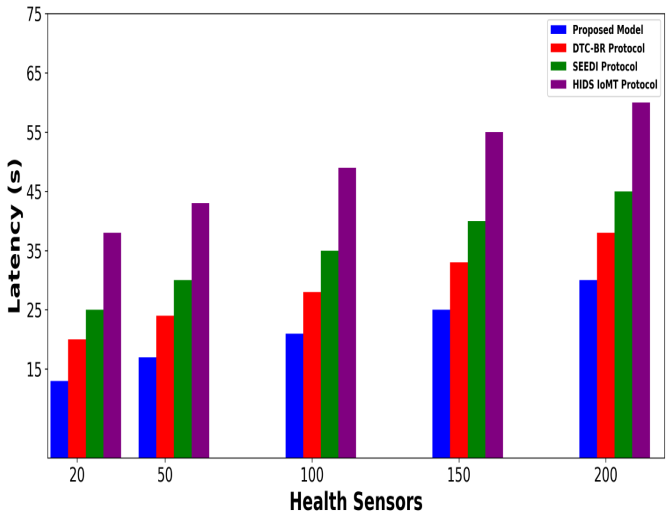

Figure 10. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for latency under varying health sensors.

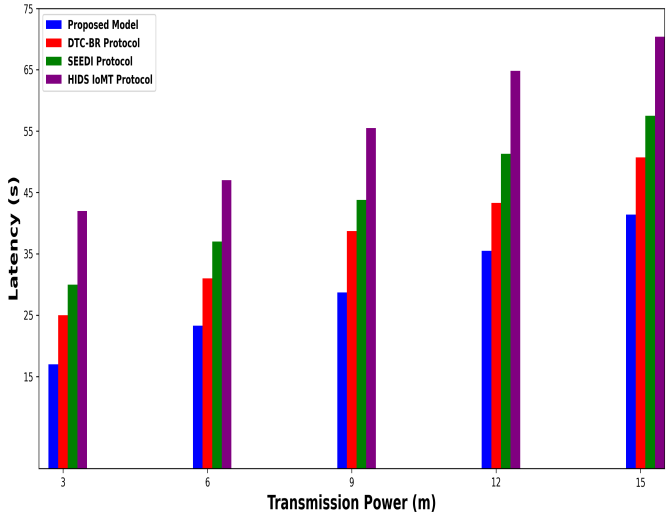

Figure 11. Performance of proposed model with DTC-BR Protocol, SEEDI Protocol, and HIDS-IoMT Protocol for latency under varying transmission range.

5. Conclusions

Smart applications with edge computing are interconnected using emerging technologies to sense and process the collected data. It timely provides the request to remote devices and facilitates advancing of the healthcare system. Many approaches have been proposed to address the timely delivery of patients' data to cloud systems, enabling the analysis of their condition and the personalization of treatments by healthcare providers. Although distributed computing across heterogeneous systems is one of the most challenging research problems addressed by most existing approaches, resource optimization with adaptive healthcare routing remains a pressing issue due to the limited processing and storage capabilities of IoMT networks. Moreover, securing the sensitive data against cyber threats without additional energy consumption is also a significant issue. We proposed an AI-enabled edge computing model for the timely detection of malicious threats in distributed healthcare applications, thereby enhancing the quality of service (QoS) for intermediate devices. The trust is also incorporated in an unpredictable environment, providing a more reliable communication paradigm that supports efficient system operations. Our future plan is to test the model with realistic collected data and integrate a

centralized controller to enhance network segmentation and adjust the security measures against massive network traffic.

Author Contributions: Conceptualization, M.F.A. and M.H.; formal analysis, M.F.A. and M.H.; methodology, M.H. and K.H.; supervision, M.H.; validation, M.F.A. and K.H.; writing—original draft, M.F.A. and K.H.; writing—review and editing, M.F.A. and M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant no. (DGSSR-2025-02-01292).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data is available in the manuscript.

Acknowledgments: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant no. (DGSSR-2025-02-01292).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ficili, I.; Giacobbe, M.; Tricomi, G.; Puliafito, A. From sensors to data intelligence: Leveraging IoT, cloud, and edge com-puting with AI. *Sensors* **2025**, *25*, 1763. [CrossRef] [PubMed]
2. Uddin, R.; Koo, I. Real-time remote patient monitoring: A review of biosensors integrated with multi-hop IoT systems via cloud connectivity. *Appl. Sci.* **2024**, *14*, 1876. [CrossRef]
3. Mathkor, D.M.; Mathkor, N.; Bassfar, Z.; Bantun, F.; Slama, P.; Ahmad, F.; Haque, S. Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innova-tive trends. *J. Infect. Public Health* **2024**, *17*, 559–572. [CrossRef]
4. Bolat-Akça, B.; Bozkaya-Aras, E. Digital twin-assisted intelligent anomaly detection system for Internet of Things. *Ad Hoc Netw.* **2024**, *158*, 103484. [CrossRef]
5. Chen, Z.; Sivaparthipan, C.B.; Muthu, B. IoT based smart and intelligent smart city energy optimization. Sustain. *Energy Technol. Assess.* **2022**, *49*, 101724.
6. Sharma, M.; Tomar, A.; Hazra, A. Edge computing for industry 5.0: Fundamental, applications, and research challenges. *IEEE Internet Things J.* **2024**, *11*, 19070–19093. [CrossRef]
7. Varriale, V.; Cammarano, A.; Michelino, F.; Caputo, M. Critical analysis of the impact of artificial intelligence integration with cutting-edge technologies for production systems. *J. Intell. Manuf.* **2025**, *36*, 61–93. [CrossRef]
8. Alamri, M.; Haseeb, K.; Humayun, M.; Alshammeri, M.; Alwakid, G.N.; Ramzan, N. Edge-Driven Disability Detection and Outcome Measurement in IoMT Healthcare for Assistive Technology. *Bioengineering* **2025**, *12*, 1013. [CrossRef]
9. Poyyamozhi, M.; Murugesan, B.; Rajamanickam, N.; Shorfuzzaman, M.; Aboelmagd, Y. IoT—A promising solution to energy management in smart buildings: A systematic review, applications, barriers, and future scope. *Buildings* **2024**, *14*, 3446. [CrossRef]
10. Wu, Y.; Dai, H.N.; Wang, H.; Xiong, Z.; Guo, S. A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1175–1211. [CrossRef]
11. Alshammeri, M.; Humayun, M.; Haseeb, K.; Alwakid, G.N. AI-Driven Sentiment-Enhanced Secure IoT Communication Model Using Resilience Behavior Analysis. *Comput. Mater. Contin.* **2025**, *84*, 433. [CrossRef]
12. Al-Jumaili, A.H.A.; Muniyandi, R.C.; Hasan, M.K.; Paw, J.K.S.; Singh, M.J. Big data analytics using cloud computing based frameworks for power management systems: Status, constraints, and future recommendations. *Sensors* **2023**, *23*, 2952. [CrossRef]
13. Cai, H.; Xu, B.; Jiang, L.; Vasilakos, A.V. IoT-based big data storage systems in cloud computing: Perspectives and chal-lenges. *IEEE Internet Things J.* **2016**, *4*, 75–87. [CrossRef]
14. Hashem, I.A.T.; Yaqoob, I.; Anuar, N.B.; Mokhtar, S.; Gani, A.; Khan, S.U. The rise of "big data" on cloud computing: Re-view and open research issues. *Inf. Syst.* **2015**, *47*, 98–115. [CrossRef]
15. Virmani, N.; Singh, R.K.; Agarwal, V.; Aktas, E. Artificial intelligence applications for responsive healthcare supply chains: A decision-making framework. *IEEE Trans. Eng. Manag.* **2024**, *71*, 8591–8605. [CrossRef]
16. Gala, D.; Behl, H.; Shah, M.; Makaryus, A.N. The role of artificial intelligence in improving patient outcomes and future of healthcare delivery in cardiology: A narrative review of the literature. *Healthcare* **2024**, *12*, 481. [CrossRef]

17. Mahmmod, B.M.; Naser, M.A.; Al-Sudani, A.H.S.; Alsabah, M.; Mohammed, H.J.; Alaskar, H.; Almarshad, F.; Hussain, A.; Abdulhussain, S.H. Patient monitoring system based on internet of things: A review and related challenges with open research issues. *IEEE Access* **2024**, *12*, 132444–132479. [CrossRef]
18. Olawade, D.B.; David-Olawade, A.C.; Wada, O.Z.; Asaolu, A.J.; Adereni, T.; Ling, J. Artificial intelligence in healthcare delivery: Prospects and pitfalls. *J. Med. Surg. Public Health* **2024**, *3*, 100108. [CrossRef]
19. Boisrond, K.; Tardif, P.M.; Jaafar, F. Ensuring the integrity, confidentiality, and availability of IoT data in Industry 5.0: A Systematic Mapping Study. *IEEE Access* **2024**, **12**, 107017–107045. [CrossRef]
20. Khan, A.Y.; Latif, R.; Latif, S.; Tahir, S.; Batool, G.; Saba, T. Malicious insider attack detection in IoTs using data analytics. *IEEE Access* **2019**, *8*, 11743–11753. [CrossRef]
21. Alketbi, K.S.; Mehmood, A. A Comprehensive Survey of Explainable Artificial Intelligence Techniques for Malicious In-sider Threat Detection. *IEEE Access* **2025**, *13*, 121772–121798. [CrossRef]
22. Shafiq, M.; Choi, J.G.; Cheikhrouhou, O.; Hamam, H. Advances in IoMT for healthcare systems. *Sensors* **2023**, *24*, 10. [CrossRef]
23. Pradyumna, G.R.; Hegde, R.B.; Bommegowda, K.B.; Jan, T.; Naik, G.R. Empowering healthcare with IoMT: Evolution, machine learning integration, security, and interoperability challenges. *IEEE Access* **2024**, *12*, 20603–20623. [CrossRef]
24. Ibrahim, M.; Al-Wadi, A.; Elhafiz, R. Security analysis for smart healthcare systems. *Sensors* **2024**, *24*, 3375. [CrossRef] [PubMed]
25. Awotunde, J.B.; Imoize, A.L.; Jimoh, R.G.; Adeniyi, E.A.; Abdulraheem, M.; Oladipo, I.D.; Falola, P.B. AIoMT enabling real-time monitoring of healthcare systems: Security and privacy considerations. In *Handbook of Security and Privacy of AI-Enabled Healthcare Systems and Internet of Medical Things*; CRC Press: Boca Raton, FL, USA, 2023; pp. 97–133.
26. Rajavel, R.; Ravichandran, S.K.; Harimoorthy, K.; Nagappan, P.; Gobichettipalayam, K.R. IoT-based smart healthcare video surveillance system using edge computing. *J. Ambient Intell. Humaniz. Comput.* **2022**, *13*, 3195–3207. [CrossRef]
27. Alshuhail, A.; Alshahrani, A.; Mahgoub, H.; Ghaleb, M.; Darem, A.A.; Aljehane, N.O.; Alotaibi, M.; Alzahrani, F. Ma-chine edge-aware IoT framework for real-time health monitoring: Sensor fusion and AI-driven emergency response in decentralized networks. *Alex. Eng. J.* **2025**, *129*, 1349–1361. [CrossRef]
28. Al-Sadoon, M.E.; Jedidi, A.; Al-Raweshidy, H. Dual-tier cluster-based routing in mobile wireless sensor network for IoT application. *IEEE Access* **2023**, *11*, 4079–4094. [CrossRef]
29. Arpitha, T.; Chouhan, D.; Shreyas, J. A hybrid optimization approach to enhance source location privacy for iot healthcare. *IEEE Access* **2024**, *12*, 132801–132816. [CrossRef]
30. Karunkuzhali, D.; Meenakshi, B.; Lingam, K. A QoS-aware routing approach for Internet of Things-enabled wireless sensor networks in smart cities. *Multimed. Tools Appl.* **2025**, *84*, 17951–17977. [CrossRef]
31. Sharma, S.; Mishra, V.M.; Tripathi, M.M.; Verma, S.; Kaur, S. SEEDI: Sink-Mobility-Based Energy-Efficient Data Dissemi-nation in the Internet of Medical Things. *IEEE Sens. J.* **2024**, *24*, 35367–35373. [CrossRef]
32. Berguiga, A.; Harchay, A.; Massaoudi, A. HIDS-IoMT: A deep Learning-Based intelligent intrusion detection system for the internet of medical things. *IEEE Access* **2025**, *13*, 32863–32882. [CrossRef]
33. Gupta, S.; Chithaluru, P.; Stephan, T.; Nafisa, S.; Kumar, S. HSPBCI: A robust framework for secure healthcare data management in blockchain-based IoT systems. *Multimed. Tools Appl.* **2025**, *84*, 27695–27719. [CrossRef]