



ARTICLE

Lightweight AI-Based Threat Detection and Surveillance Secure Edge-IoT Healthcare Systems

Menwa Alshammeri^{1,*}, Khalid Haseeb², Mamoon Humayun³ and Mona Saleh Alzahrani¹

¹Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka, Saudi Arabia

²Department of Computer Science, Islamia College Peshawar, Peshawar, Pakistan

³Department of Computer Science, Nottingham Trent University, Clifton Lane, Nottingham, UK

*Corresponding Author: Menwa Alshammeri. Email: mhalshammeri@ju.edu.sa

Received: 17 May 2026; Accepted: 04 September 2026; Published: 22 October 2026

ABSTRACT: Advances in emerging technologies, such as the Internet of Things (IoT) and artificial intelligence, provide a wide range of real-time applications to the development of smart cities. The physical objects, along with IoT systems, not only provide seamless connectivity to the remote environment but also continuously gather the required data through a sensor-based network. They provide timely information to connected devices, meet their needs, and enhance the flexibility of automated IoT-driven systems. Despite improvements in network maintenance and communication robustness, most existing healthcare systems still encounter challenges in addressing congestion and scalability as data traffic increases. Furthermore, as autonomous activities increase, communication trust among health devices decreases, thereby increasing computational overhead due to privacy concerns and potential attacks. This research proposes an intelligent, edge-enabled machine-learning model for an autonomous environment to identify proactive threats and enhance system trustworthiness by mitigating unauthorized and insecure activities in the healthcare network. The devices are controlled efficiently, with uniform load balancing, using edge computing and heuristic techniques to optimize resource allocation and energy efficiency. It intelligently controls network traffic and reduces on-device computational power by dynamically offloading to selected forwarders, without increasing network consumption or overhead. Moreover, the trusted schemes are designed to increase reliability within a bounded network system and to support the integrity of devices while processing health records at the network edges. Simulation results confirm that the proposed framework achieves improvements in energy overhead, latency, throughput, and response time compared to the RePUF-IoT and AIBS-IoTH schemes.

KEYWORDS: Internet of Things; security; edge networks; trust computing; smart system

1 Introduction

Modern IoT systems play a vital role in enhancing smart cities and developing crucial applications for society [1,2]. Many real-time systems, such as healthcare, vehicle automation, and surveillance, support connected devices for data gathering and processing, enabling interconnected electronic devices [3,4]. In recent decades, intelligent systems have been offering personalized approaches to monitor harsh environments and continuously inform remote users using IoT-based sensors and digital technologies [5,6]. It provides timely responses to network users for decision-making and facilitates efficient resource management while ensuring reliable service delivery in the IoT network. On the other hand, big data collects a massive amount of health records from multiple sources for patient care and operations optimization, and analyzes them using edge-level computing [7,8]. Recently, many approaches have adopted it to provide more intelligent

methods for data security and to prevent malicious traffic from being forwarded to cloud processing [9,10]. However, due to constrained system resources, particularly limited battery power in IoT sensors and lightweight wireless technologies, a security challenge arises when sensitive data must be processed and transmitted from edge devices to the cloud for storage or further analysis [11,12]. Moreover, the establishment of trust when forwarding IoT data from the connected independent network reveals threats, including unauthentic data processing, violations of user privacy, and compromise of the network's integrity [13,14]. The integration of trusted devices balances network operations and prevents unnecessary malicious traffic on healthcare devices, resulting in a more reliable and sustainable communication system. In recent decades, healthcare systems have been widely compromised due to cyber threats in heterogeneous and resource-limited communication [15,16]. Most proposed solutions rely on centralized mechanisms and cannot address scalability issues in rapidly growing IoT-enabled healthcare systems. Moreover, the lack of reliable methods for authenticating device associations during health record processing often compromises system integrity and reduces operational stability in edge-driven data transmission. The lack of intelligence in many existing approaches leads to inefficient resource utilization and degrades network optimization in complex real-time environments [17,18]. Therefore, the primary aim of our research is to address significant challenges in resource-constrained healthcare networks by focusing on security, data trust, and energy efficiency. It explores the K-Nearest Neighbors (KNN) approach [19] to provide trusted data processing on unpredictable devices and intelligently integrates edge-cloud interactions by introducing lightweight offloading computation, thereby optimizing network performance for the healthcare industry. Furthermore, threats are detected using IoT devices' learning patterns and conditions before they compromise communication and lead to data tampering. The lightweight mechanism of the proposed framework, supported by edge-driven decision-making, adaptively balances task offloading and ensures an energy-aware healthcare network. In addition, the trust-based methods facilitate reducing the number of suspicious devices and ultimately increase the network's resilience against potential threats. The following are the primary contributions of this research study.

- i. A dynamic trust-computing approach is developed for the Edge-IoT network using autonomous machine-learning-based fusion of multidimensional device behavior.
- ii. Intelligent decisions are made using task offloading with reinforcement learning, which decreases energy consumption by optimizing the performance of resource-constrained electronics.
- iii. Preventing network threats to enhance the reliability and trustworthiness in the healthcare system integrated with lightweight encryption and intelligent learning patterns.

The rest of the paper is structured as follows. Related work is explained in [Section 2](#). The discussion of the proposed framework, along with its components, is provided in [Section 3](#). In [Section 4](#), the performance results and discussion are provided. In the end, a conclusion is provided in [Section 5](#).

2 Related Work

The integration of IoT networks with industrial applications has significant potential for rapid, continuous monitoring of the target environment through interconnected devices [20,21]. It offers a data-collection service, enabling network providers to perform timely analyses of system issues and performance, thereby enabling the management of innovative IoT networks [22,23]. Cloud-integrated edge-level processing enhances IoT network functionality by enabling a more secure communication paradigm and improving scalability through effective network resource utilization [24,25]. In recent decades, many innovative IoT applications have been exploring decentralized approaches based on a cloud-edge architecture to ensure timely processing and storage of massive amounts of data for analytics and decision-making systems [26,27]. The study [28] enhances healthcare data processing by proposing a federated learning-based Edge-IoMT

model (FEEL) that provides secure, low-overhead communication. The proposed model effectively builds a decision-making system that balances energy resource use and protects data privacy against threats. The authors of [29] explore TinyJAMBU encryption with reconfigurable PUFs and hashing functions to propose the authentication protocol RePUF-IoT, which securely processes healthcare data and allows only authorized devices to access sensitive IoT data. The proposed approach employs machine learning models to enable secure interactions and protect network communication against threats, thereby improving data reliability. A Privacy Protection Scheme for Federated Learning under Edge Computing (PPFLEC) is proposed in [30] to provide a privacy-protection protocol with lightweight computation. The proposed scheme uses a shared secret and a weight mask. It provides more reliable and efficient methods than homomorphic encryption, authenticates devices, and maintains data integrity. However, it overlooks the need to adapt privacy-preserving methods to varying data distributions as more healthcare devices are deployed. A novel approach, delay-aware energy-efficient reliable routing (DA-EERR), is introduced in [31] for reliable routing with energy efficiency. It offers improved response time for time-constrained applications and distributes load uniformly across devices. Moreover, it increases the longevity of routing paths and, with effective selection of data forwarders, enhances the aggregation and delivery level of IoT data. In [32], the authors proposed a model based on optimized Tiny Machine Learning (TinyML) and Explainable AI (XAI) for binary classification. It offers an energy-aware healthcare system with trustworthy communication by exploiting fog computing. It balances device load and effectively reduces network latency, improving bandwidth utilization to support critical, real-time healthcare services. It improves response time for critical health alerts by leveraging the compression technique and provides a practical approach for time-constrained medical applications.

Authors in [33] proposed a unique blockchain-based artificial intelligence system for an IoT-based healthcare system (AIBS-IoTH), aiming to achieve energy efficiency and more reliable transmission of sensitive medical data. It captures patients' e-health records using wearable sensors and forwards them to processing devices. It uses a metaheuristic algorithm, specifically a modified sunflower-optimization-based clustering (MSFOC). Moreover, blockchain technology is adopted to secure both the intra-cluster and inter-cluster communication. Finally, the Classification Enhancement Generative Adversarial Networks (CEGAN) model is exploited for disease identification and conducts the diagnostic procedure on encrypted data. The study [34] exploits both Deep Reinforcement Learning (DRL) and Level of Autonomy (LOA) to propose a novel approach, DRL-LOA, that balances traffic data and optimizes network communication with an efficient structure. Moreover, to extract structural information and fuse it with traffic features to produce node vectors, DRL-LOA utilizes a Graph Convolutional Network (GCN). To efficiently categorize medical data on the fog device, the proposed approach used an FDNN classifier. The performance results significantly improved device latency and power consumption compared to existing solutions. Thus, emerging technologies for the formulation of smart cities have been rapidly explored alongside edge computing. It manages the flow of network data and uses services from emerging networks to support the communication paradigm with efficient, optimized performance. However, most existing solutions still lack trust management for distributed applications, leading to increased complexity in addressing network scalability [35,36]. Moreover, most approaches lack proactive threat-detection strategies to address significant research challenges and prevent malicious activity before it harms the healthcare network. Such malicious activities by devices not only disrupt communication but also compromise the integrity and authenticity of associated devices and ultimately pose threats to data privacy [37,38]. In [39], the authors proposed an Energy-Efficient Secure Routing Protocol (E2SRP) for a wireless sensor network that leverages edge computing to focus on both energy efficiency and data security. Unlike most existing approaches, E2SRP performs data aggregation and processing at the network edge. In addition, the GWO algorithm is used to select optimal routes and

achieve load balancing, leveraging fuzzy logic to enhance network stability. The study [40] introduces an Energy-Aware, low-latency, data-driven routing model for mobile edge computing (EALLR), aiming to reduce latency and efficiently utilize bandwidth by optimizing network performance through the integration of multiple parameters. The proposed model introduces the role of edge nodes in collecting and processing IoT data closer to the source, thereby improving response time in a critical environment. In addition, it reduces retransmissions and effectively controls congestion in a dynamic topology.

Research Statement

In recent decades, most approaches have focused on optimization and routing problems, especially in IoT-based applications such as healthcare, transportation, and surveillance. However, many of them are not fully reliable or trustworthy when devices are openly communicating across network boundaries in the presence of threats and unpredictable wireless conditions. This leads to degraded trust management and inefficient resource exploration when constrained devices are required to handle a large volume of gathered data. In addition, response time is a significant research challenge in time-constrained systems, particularly in healthcare, where remote users urgently require timely analysis of their data by medical experts. Such systems fail to deliver up-to-date, more accurate results from edge servers, thereby affecting the system's sustainability. Furthermore, the limited adaptability to varying IoT devices and dynamic network conditions prevents efficient task offloading and limits network scalability. Based on the highlighted issues, there is a need for a trust-aware, optimized routing framework that intelligently explores network resources while protecting IoT data from threats. In addition, the trust needs to be dynamically updated based on various factors to promptly detect potential attacks and improve the response time of the processing devices, thereby achieving system stability.

3 Proposed Methodology

This section discusses the proposed framework that integrates optimization and trustworthiness communication in edge-driven healthcare networks. It comprises two main stages aimed at proposing an energy-efficient, more reliable offloading approach with lightweight computations for constrained healthcare devices. In addition, the network's non-authentic and malicious behavior is continuously captured, maintaining trustworthiness across multiple layers of the proposed framework and ensuring uniform load balancing among IoT devices. Fig. 1 depicts the components and the associated stages of the proposed framework. It comprises trust evaluation, energy efficiency, continuous updating of device trust over time, and optimized offloading capabilities. Each component contributes to the development of an innovative Edge-IoT system by ensuring data security and effective load balancing in a resource-constrained network. It balances network traffic across forwarders using artificial intelligence and eliminates unnecessary route-discovery messages.

3.1 Trust Management Using Dynamic and Intelligent Prediction

The proposed framework evaluates the trustworthiness of health devices using a *KNN* approach based on each device's historical behavior and real-time performance. The trust value of each device is crucial in healthcare edge networks to ensure reliable and secure processing. The trust of device i at time t is computed using accuracy, previous task score (A_i), energy consumption (E_i), and abnormal behavior score, as shown in Eq. (1). Accordingly, trust improves with higher accuracy, while it decreases with higher energy consumption and abnormal device behavior detection.

$$T_i(t) = \Pi_{[0,1]} [(1 - \psi)T_i(t-1) + \psi(w_A A_i + w_E(1 - E_i) + w_M(1 - M_i))] \quad (1)$$

where both the normalized accuracy and energy consumption of the device i are denoted by A_i , and E_i . M_i presents the misbehavior or anomaly score. Also, the parameters w_A , w_E , and w_M are non-negative

weighting factors such that their summation must be equal to 1, and in the end, ψ denotes the updated trust rate. Whereas the projection operator $\Pi_{[0,1]}(\cdot)$ is used to restrict the updated trust value within the interval $[0, 1]$. To further enhance the trust evaluation, KNN is employed, where the trust value $T_i(t)$ of device N_i is determined by comparing its feature vector with its K nearest neighbors, based on the accuracy, energy efficiency, misbehavior score, and the previous trusted value $T_i(t-1)$, as denoted in Eq. (2).

$$f_i(t) = [A_i(t), 1 - E_i(t), 1 - M_i(t), T_i(t-1)] \quad (2)$$

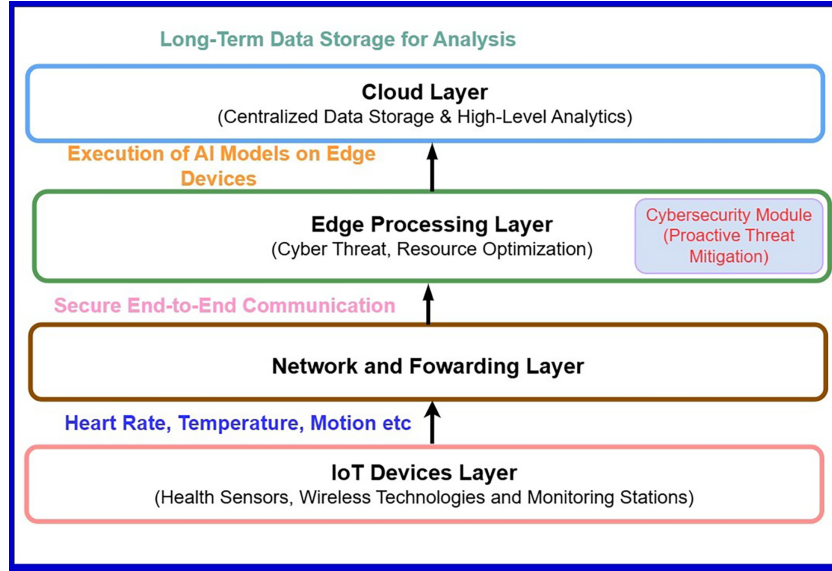


Figure 1: Key components of the proposed framework for Edge-IoT healthcare system.

Using the Euclidean distance d between behavioral feature vectors $\mathbf{f}_i(t), \mathbf{f}_j(t)$, the set of K nearest neighboring devices is selected as expressed in Eq. (3).

$$N_i^K(t) = \arg \min_{K, j \neq i} d(\mathbf{f}_i(t), \mathbf{f}_j(t)) \quad (3)$$

Afterward, K -nearest neighbors are updated based on the majority vote, ensuring that devices with similar characteristics are classified similarly in terms of trust, as expressed in Eq. (4).

$$\hat{z}_i(t) = \text{mode} \{z_j(t) \mid N_j \in N_i^K(t)\} \quad (4)$$

where predicted trust class of device N_i at time t is denoted by $\hat{z}_i(t)$. The operator mode denotes the majority-voting function, which selects the most frequent trust class $z_j(t)$ among the K nearest neighboring devices N_i^K at time t . In this way, the KNN results are used to determine device behavior and classify devices as malicious or reliable.

3.2 Secure Edge-Driven Routing and Optimized Offloading Decisions

In the task-offloading phase, the proposed framework leverages multi-agent-based Reinforcement Learning [41] to determine whether healthcare tasks should be processed locally at the network edge or offloaded to the cloud. The offloading decision is defined in Eq. (5), which is based on normalized processing time $\hat{T}(a)$, energy consumption $\hat{E}(a)$, communication distance $\hat{d}(a)$, and latency $\hat{L}(a)$.

$$\begin{aligned}
a^* &= \arg \min_{a \in \mathcal{A}} (w_1 \hat{T}(a) + w_2 \hat{E}(a) + w_3 \hat{d}(a) + w_4 \hat{L}(a)) \\
\text{s.t. } &T_i(t) \geq \tau_{\text{trust}}, \\
&C(i, j) \leq C_{\text{max}}, \\
&E_i \geq E_{\text{threshold}}
\end{aligned} \tag{5}$$

where trust value $T_i(t)$, communication cost $C(i, j)$, and E_i are constraints that are considered for a reliable and secure task offloading decision. The coefficients w_1, w_2, w_3 , and w_4 represent the relative contributions of the associated, such that $\sum_{m=1}^C w_m = 1$, where C is number of factors. Using Eq. (6), the agent's capabilities are improved, and a reward function is defined for the selection of resource-efficient and more secure offloading decisions.

$$R_{t+1} = T_{rt} \cdot T_i(t) - \varepsilon T_{\text{offload}} - \lambda I_{p,i} \tag{6}$$

where T_{offload} denotes the computed offloading cost, $T_i(t)$ is the trust score, T_{rt} is the trust rate, ε denotes the weighted factor for offloading cost, λ is the penalty coefficient, and $I_{p,i}$ denotes the imposed penalty when the resource constraint is avoided. Accordingly, an agent is assigned a higher reward for selecting more trusted devices with lower offloading costs. On the other hand, when any security constraint is avoided, the least reward is given to the agent.

In the proposed framework, the agent updates the Q-value based on energy consumption, latency, and processing time to determine whether to offload the task locally or to the cloud, as shown in Eq. (7).

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha [R_{t+1} + \gamma \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t)] \tag{7}$$

where α is the learning rate, R_{t+1} is the reward after taking action a_t in state s_t , and γ is the discount rate. The state space S represents the system's conditions, and the action space A consists of decisions such as offloading to the edge, cloud, or local processing. Through thorough exploration, the agent learns the optimal task offloading policy that balances energy efficiency, latency, and processing time. Eq. (8) defines the update rule for Q-learning, incorporating a decaying learning rate α_t that decreases over time to improve convergence and generate a more optimal policy for agents learning from the environment.

$$\alpha_t = \alpha \cdot (1 + \text{decay_factor} \cdot t)^{-1} \tag{8}$$

The proposed framework employs Identity-Based Encryption *IBE* to ensure data privacy and enhance security between health devices in healthcare IoT networks. *IBE* allows public keys to be generated directly from the device's identity, eliminating the need for certificates. Each device is assigned a unique identity ID_i , and the public key P_i is derived from it. This approach simplifies key management by directly linking a device's identity to its public key. In *IBE*, the private key for device N_i is generated by a Private Key Generator (PKG), which uses the device's identity ID_i to derive its private key. The device's public key P_i is generated from the identity ID_i without requiring certificates. The public key P_i is defined as in Eq. (9).

$$P_i = \text{IBE}_{\text{PKG}}(ID_i) \tag{9}$$

The private key k_i of device N_i is generated by the PKG using the identity ID_i and is shared securely between the PKG and device N_i . The private key k_i is used for decryption of messages in the system, and it is linked to a particular device. Moreover, the private key is generated by PKG only at the setup and initialization phase, and later encryption/decryption, signing, and verification operations are executed

locally by the participating devices. In the proposed framework, the *PKG* is considered a trusted third party to generate the private keys and distribute them securely to authorized devices. In addition, a distributed key splitting mechanism is explored to further protect the private keys from direct exposure to malicious attackers. In the proposed framework, the security overhead can be expressed as Eq. (10).

$$O_T = O_{IBE} + O_{SV} + O_{KS} \quad (10)$$

where O_T denotes overhead of whole system that is comprised of associated functionalities including data signing and its verification O_{SV} , key generation and data encryption O_{IBE} , and keys splitting with their distribution O_{KS} . However, the *PKG* only participates during the device initialization phase; thus, the recurring execution and computational overhead are limited while performing device communication. For secure communication, a device N_i uses its private key k_i to decrypt messages encrypted with the corresponding public key. The encryption and decryption processes are based on device identity, and the system remains certificate-free because it does not require a central certification authority. To ensure the security of the private key, a distributed key splitting mechanism is employed. It divides the private key k_i into n shares, which are securely distributed between the authentic devices. The private key share k_{ij} for the j -th participant is computed using Eq. (11), and the original private key is constructed when all the distributed shares are integrated.

$$k_i = \sum_{j=1}^n k_{ij} \quad (11)$$

In this system, k_i is the original private key, while k_{ij} denotes the j -th share of the particular split key into n shares. Thus, identity-based encryption (*IBE*) provides a certificate-free solution that simplifies key management while maintaining strong security in IoT networks. To authenticate the health record, device d_i signs σ of the message m using its private key k_i , which is reconstructed from the private keys of n devices. Upon receiving the message, the recipient uses the public key P_i to recover the original signature, as defined in Eq. (12).

$$\begin{aligned} \sigma_i &= \text{sign}(k_i, m) \\ \text{Verify}(\sigma_i, m, P_i) &= \begin{cases} \text{True} & \text{if valid} \\ \text{False} & \text{if invalid} \end{cases} \end{aligned} \quad (12)$$

Accordingly, health data d_i remains private and cannot be altered by malicious devices while being transmitted in an IoT-based system. Only authorized devices with the reconstructed private keys can recover the original messages, thereby preventing a man-in-the-middle attack. Moreover, timestamp and nonce are utilized by the proposed framework to prevent replay attacks and ensure that the message has not been retransmitted, as in Eq. (13).

$$\text{Reject}(d_i) = \begin{cases} \text{True,} & \text{if } T_{\text{timestamp}} < T_{\text{current}} - \Delta T \\ & \text{or invalid nonce} \\ \text{False,} & \text{otherwise} \end{cases} \quad (13)$$

Furthermore, the proposed framework mitigates potential attacks using Reputation-Based Systems. The health devices continuously compute and update the reputation score rs by exploiting the past behavior and feedback Fb of neighbor i , as in Eq. (14).

$$rs_i(t) = \beta_1 \cdot rs_i(t-1) + \beta_2 \cdot Fb(N_i) \quad (14)$$

where β_1 and β_2 are weighted coefficients. In addition, the proposed framework computes the cost function $c(i, j)$ for optimizing routing in a healthcare system by selecting the most dynamic next hop based on trust scores, task offloading decisions, and security factor measurements, as shown in Eq. (15). In the event of an invalid selection of forwarders, the proposed framework isolates them from normal devices.

$$\mathbf{x}_{ij} = \begin{bmatrix} x_1(i, j) \\ x_2(i, j) \\ \vdots \\ x_m(i, j) \end{bmatrix}, \quad \mathbf{w} = \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{bmatrix} \Rightarrow C(i, j) = \mathbf{w}^\top \mathbf{x}_{ij} \quad (15)$$

In Eq. (16), the optimal forwarder NF^* is selected by minimizing the cost function $C(i, j)$ across all available forwarders in the set N_i . If no valid forwarders are found, the system defaults to a fallback node.

$$\begin{aligned} NF^* &= \arg \min_{j \in N_i} C(i, j) \\ \text{subject to } T_i(t) &\geq \tau_{\text{trust}} \\ C(i, j) &< C_{\text{max}} \end{aligned} \quad (16)$$

Algorithm 1 outlines the dynamic selection of the optimal forwarders for the edge layer and provides an intelligent task Offloading decision process. It initiates the trust computation process using the devices' behavior and feedback history. The trust score is continuously updated based on network conditions and computes the probability of a device's trustworthiness. Such computations lead to the selection of a more dynamic forwarding route and the effective utilization of network resources. It also explores device evaluation based on trust, power efficiency, and latency, thereby enhancing reliability for intensive tasks. Accordingly, the proposed framework's intelligence-driven task-offloading decision-making improves resource conservation and ensures timely availability for processing incoming e-health data. Table 1 summarizes the main notations used in the proposed framework.

Algorithm 1: Trust-aware with secure task offloading IoT-based healthcare framework

- 1: **Input:** Feedback set, thresholds, previous trust value, decision parameters
 - 2: **Output:** Updated trust value $T_i(t)$ and offloading decision T_{offload}
 - 3: Initialize feedback set F_i , trust thresholds, system parameters, and network state
 - 4: Collect feedback $f_i \in F_i$ from device i
 - 5: Collect device and network-related information
 - 6: **for** each feedback instance $f_i \in F_i$ **do**
 - 7: Extract performance metrics for device behavior evaluation
 - 8: Evaluate the behavior status of device i as normal or malicious
 - 9: Record the feedback history of device i for long-term behavior monitoring
 - 10: **if** abnormal or malicious behavior is detected **then**
 - 11: Flag device i as unreliable for further analysis
 - 12: Restrict device i from direct edge offloading
 - 13: **else**
 - 14: Mark device i as reliable for secure health service access
 - 15: **end if**
-

(Continued)

Algorithm 1 (continued)

```

16: end for
17: Update the trust value  $T_i(t)$  using the previous trust value and feedback history
18: Normalize  $T_i(t)$ 
19: Compute the trust probability based on the normalized trust value
20: Apply a security mechanism for uncertain or low-trust IoT devices
21: Update security keys according to the latest trust status
22: Store the updated trust value, feedback record, and offloading decision for next-level computation
23: return  $T_i(t)$  and  $T_{\text{offload}}$ 

```

Table 1: Notation description.

Notation	Meaning
ψ	Updated trust
t	Time
N_i	Device
P_i	Public key
k_i	Private key
k_{ij}	j -th share of the private key of device N_i
α	Learning rate
T_{rt}	Trust rate
β_1, β_2	Weighted coefficients

4 Results Analysis

In this section, we present and analyze the performance outcomes of the proposed framework with existing algorithms: RePUF-IoT and AIBS-IoTH. The simulated environment is equipped with 10–1000 health sensors for continuous data sensing and transmission to the cloud platform through edge devices. The edges act as local decision-makers, performing processing to reduce the device's load and improve response times for medical experts. Edges have some mobility capabilities with more resources and processing power than ordinary sensors. Initially, the device's energy resource is set to 5000 mJ. The TensorFlow and PyTorch libraries were used for AI modeling and training, while NS-3 was used to create the network environment and simulate the reliable communication protocols. The generated trace files are used to evaluate performance metrics and to support security-related operations between devices. To simulate realistic sensor data, we generate a dataset from 50 simulations by designing predefined scenarios and parameters to capture device and network conditions. For each run x , the improvement I_m was computed from the metric values of the proposed framework, M_r^{prop} , and the corresponding baseline, M_r^{base} , and the final percentage was reported as the mean over all runs. Accordingly, we create a more controlled, dynamic environment to evaluate the performance of the proposed framework across a wide range of network metrics and learning algorithms. Moreover, the number of malicious devices remains fixed at 20; however, to evaluate the performance of the proposed framework over varying traffic intensities compared to existing approaches, the packet generation rate is varied from 2 to 20 packets/s per malicious device. We evaluate the performance of the proposed framework and existing schemes in terms of energy overhead, response time, throughput, and packet retransmission delay. The energy overhead is determined using the depletion amount of energy resources

in data processing, transmission, and security measurements. Network throughput is computed based on the number of successful data packets received over a particular time period from source to destination. Moreover, the system responsiveness is computed as the average time required by the IoT system to process and fulfill the demands of the requested devices. The packet retransmission time is measured as an end-to-end interaction while the packet is transmitted from source to destination, including all delays in processing, transmission, and queuing. Table 2 declares the simulation parameters used to conduct the experiments.

Table 2: Simulation parameters.

Parameter	Value
Initial energy	5000 mJ
Number of devices	10–1000
Sensing radius	5 m
Number of malicious nodes	20
Independent runs	50
Simulation scenarios	Varying time, devices, and malicious packet rate
Network simulator	NS-3
AI modeling libraries	TensorFlow and PyTorch
KNN parameter	$K = 5$
Trust update rate	0.1
Trust weights	$w_A = 0.4, w_E = 0.3, w_M = 0.3$
Weighted coefficients	$w_1 = 0.25, w_2 = 0.25, w_3 = 0.25, \text{ and } w_4 = 0.25$

Table 3 presents the schema of the generated dataset, detailing fields collected from simulation samples across network scenarios, including device, trust, security, and offloading-related attributes.

Table 3: Synthetic dataset schema for security-aware framework.

Field	Type	Values
Simulation_ID	Integer	1–50
Device_ID	Integer	1– N , where $N = 10$ –1000
Trust_Score $T_i(t)$	Float	0–1
Accuracy_Score A_i	Float	0–1
Feedback_Score F_i	Float	0–1
Misbehavior_Factor M_i	Float	0–1
Attack_Level	Integer	Low (1)/Medium (2)/High (3)
Ground_Truth_Label	Binary	0, 1
Predicted_Label	Binary	0, 1
Detection_Status	Binary	0, 1

4.1 Impact of Time Interval Variation

In Figs. 2 and 3, the proposed framework demonstrates its energy overhead and network throughput performance compared with existing approaches. The evaluation results demonstrate significant improvements in the proposed framework, with averages of 36% and 43% across varying time intervals. This is due to the integration of trust-driven and more secure computation, ensuring the selection of reliable devices

for transmitting health data over insecure channels. Moreover, trust values are frequently updated based on conditions and feedback from neighboring devices, enabling more adaptive decision-making and a more sustainable IoT communication system. The congested channels are intelligently analyzed to process incoming health traffic and select the optimal forwarders for transmitting IoT-based healthcare data. Figs. 4 and 5 reveal the improvement of the proposed framework by an average of 37% and 49% for response time and packet transmission delay over the existing schemes. The improvement of the proposed framework over related approaches is due to the integration of a multi-parameter selection mechanism that ensures the selection of more accurate, trustworthy, and reliable devices for aggregating and forwarding health records to the edges. In addition, intelligent decision-making facilitates the learning process to identify malicious traffic and compute trust scores with updated network parameters. As a result, it leads to reliable predictions, ensuring robustness and long-term performance for the health system.

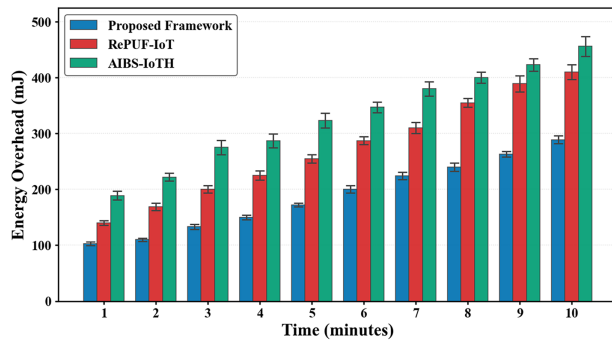


Figure 2: Energy overhead for proposed framework, RePUF-IoT and AIBS-IoTH under time intervals.

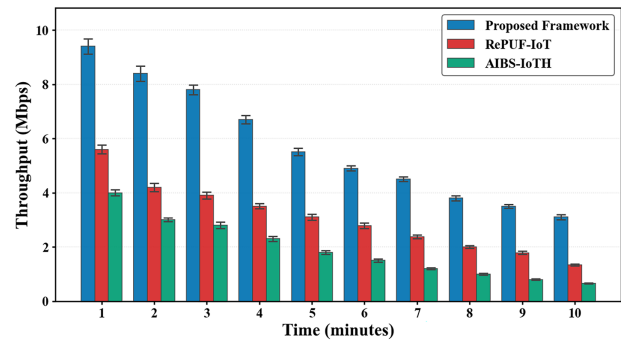


Figure 3: Throughput for proposed framework, RePUF-IoT and AIBS-IoTH under time intervals.

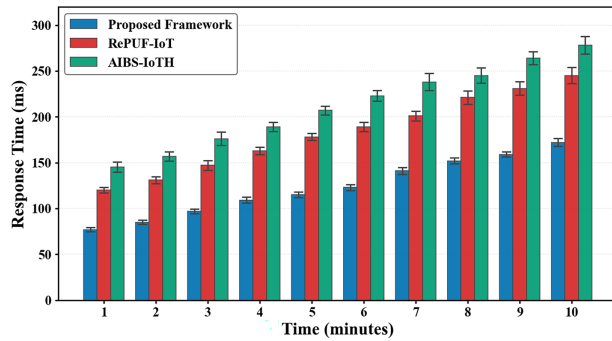


Figure 4: Response time for proposed framework, RePUF-IoT and AIBS-IoTH under time intervals.

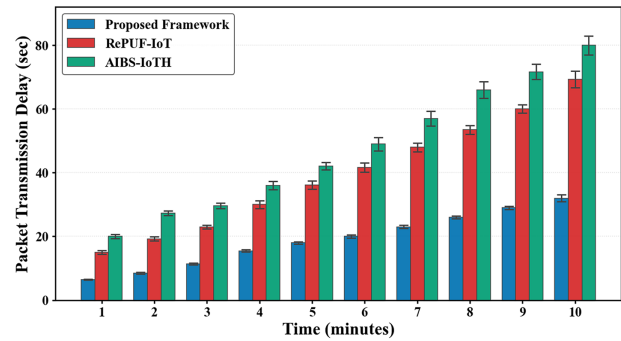


Figure 5: Packet transmission delay for proposed framework, RePUF-IoT and AIBS-IoTH under varying time intervals.

4.2 Impact of Device Density

Figs. 6 and 7 illustrate the performance analysis of energy overhead and throughput for the proposed framework, RePUF-IoT, and AIBS-IoTH across varying health devices. Based on the results analysis, the proposed framework improved performance by an average of 34% and 45%, respectively. The proposed framework intelligently prevents unreliable connections for forwarding health records and optimizes route selection using a computed cost function. By leveraging intelligent, lightweight cost computation, resources

in healthcare systems are dynamically allocated, thereby minimizing additional energy consumption while enhancing overall system performance. Moreover, the proposed framework provides an intelligent approach to reduce the distance between the source device and the cloud platform, enabling real-time data processing closer to the source and reducing additional energy utilization, with improved delivery of health data to destination devices.

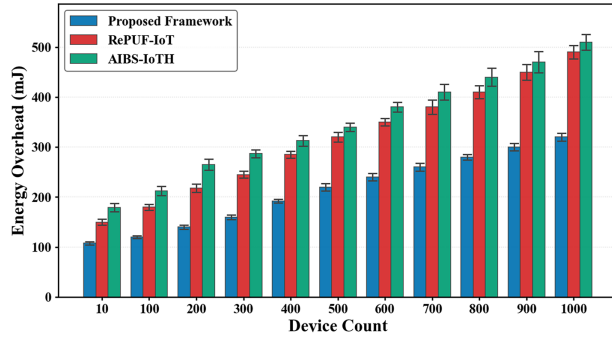


Figure 6: Energy overhead for proposed framework, RePUF-IoT and AIBS-IoTH under varying device counts.

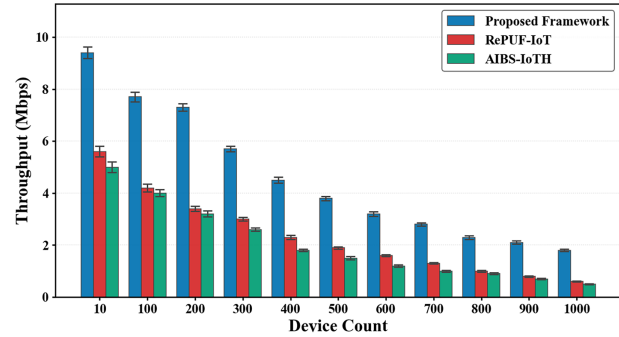


Figure 7: Throughput for proposed framework, RePUF-IoT and AIBS-IoTH under varying device counts.

Figs. 8 and 9 illustrate a significant improvement of the proposed framework by an average of 37% and 54%, respectively, as compared to RePUF-IoT and AIBS-IoTH. The combination of local decision-making in the proposed framework uses an artificial intelligence approach and dynamically manages response time while processing the device's request at the network edges. In addition, the decrease in transmission distance with effective security measures provides a more efficient approach to preventing malicious packets and also reduces the load on communication channels. As a result of distribution processing in the proposed framework, the network availability is enhanced even in the presence of faulty traffic, and the responsiveness of healthcare communication is improved.

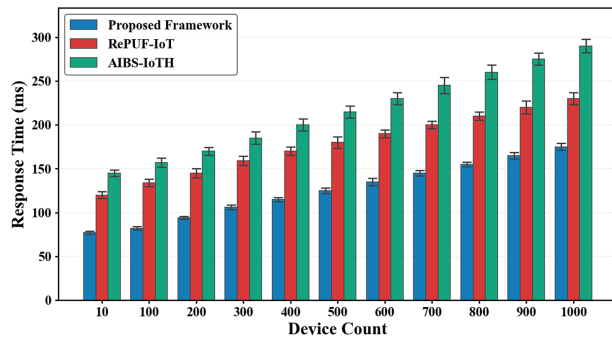


Figure 8: Response time for proposed framework, RePUF-IoT and AIBS-IoTH under varying device counts.

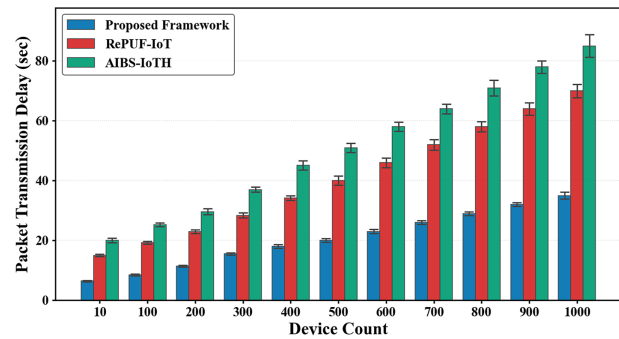


Figure 9: Packet transmission delay for the proposed framework, RePUF-IoT, and AIBS-IoTH under varying device counts.

4.3 Impact of Malicious Traffic Intensity

Figs. 10 and 11 illustrate the performance of the proposed framework in terms of energy overhead and throughput, compared with related approaches. The results demonstrate that the proposed framework

consistently outperforms existing solutions, such as RePUF-IoT and AIBS-IoTH, by an average of 38%, and 46%, respectively, across malicious packets. As the number of malicious activities increases, the proposed framework achieves significant improvements in data reception rate, particularly against potential threats, while reducing excessive energy consumption on constrained devices. It also achieves high trust, and its management enables timely, reliable device authentication. These findings demonstrate the robustness and effectiveness of the proposed framework in a real-world healthcare IoT environment. In addition, Figs. 12 and 13 depict the performance of the proposed framework for response time and packet transmission delay; the revealed analysis demonstrates the significant improvement of the proposed framework by an average of 35%, and 49% over existing approaches. This is due to computing trust based on the device's latest attributes and its neighbors' feedback. The trust is not only computed but also continuously updated to monitor the global schema of the IoT network at the network edges. If any malicious threat is detected, the proposed framework intelligently leverages cryptographic methods without imposing overhead on constrained devices. The selection of optimal routes ensures the timely delivery of critical health data to processing devices and improves the response time while forwarding the appropriate actions.

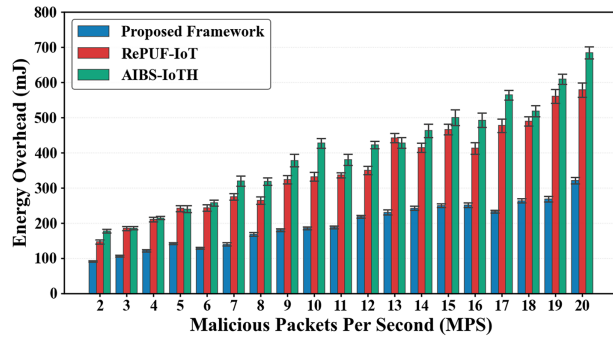


Figure 10: Energy overhead for proposed framework, RePUF-IoT and AIBS-IoTH under malicious packets.

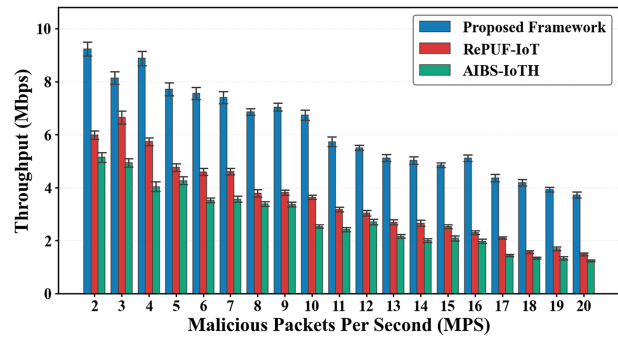


Figure 11: Throughput for proposed framework, RePUF-IoT and AIBS-IoTH under malicious packets.

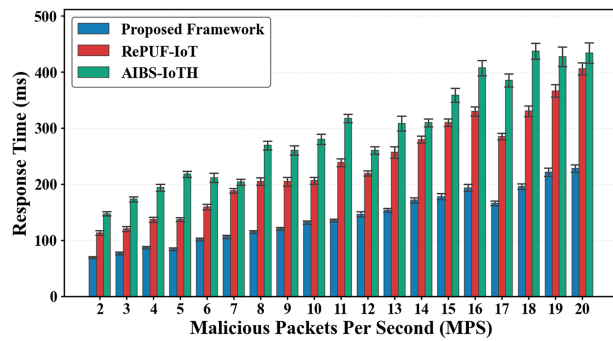


Figure 12: Response time for proposed framework, RePUF-IoT and AIBS-IoTH under malicious packets.

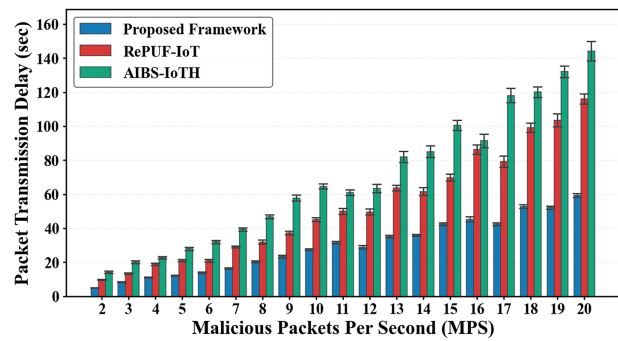


Figure 13: Packet transmission delay for the proposed framework, RePUF-IoT, and AIBS-IoTH under malicious packets.

In addition, Fig. 14 depicts the performance of the classification metrics, and the revealed results shown in Table 4, a remarkable improvement in terms of accuracy, precision, recall, and F1-score as compared with existing approaches.

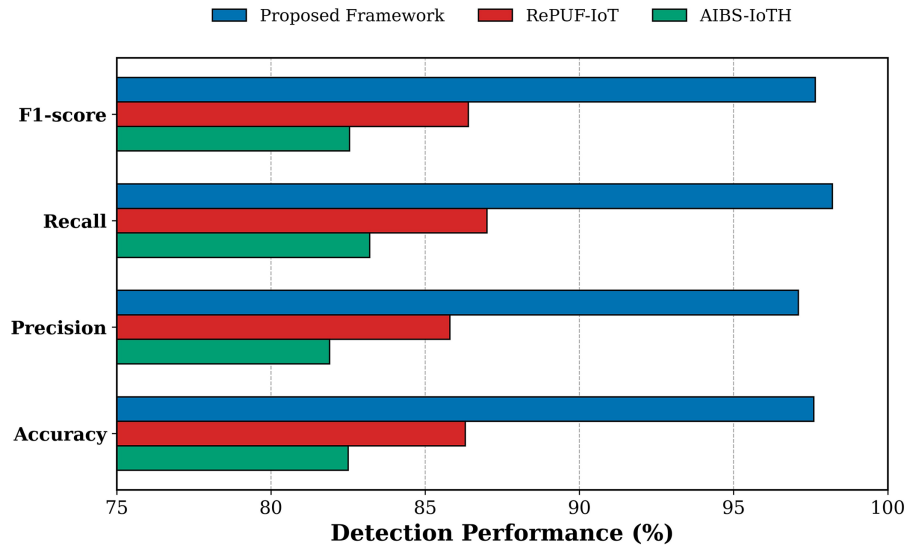


Figure 14: Classification performance comparison of the proposed framework, RePUF-IoT, and AIBS-IoTH.

Table 4: Performance metrics.

Metric	Proposed Framework	RePUF-IoT	AIBS-IoTH
Accuracy (%)	97.6	86.3	82.5
Precision (%)	97.1	85.8	81.9
Recall (%)	98.2	87.0	83.2
F1-score (%)	97.65	86.40	82.53

5 Conclusion

Wireless technologies enable the rapid development of IoT-based healthcare systems to process the collected data and report it to the requested devices. The medical server analyzes patients' data using robust processing capabilities and stores it in the cloud for remote users to access. It enhances decision-making by supporting critical tasks and improving the network system's reliability and responsiveness. Many solutions combine AI models to optimize resource use and ensure threat detection during IoT data transmission. However, most of them are unable to identify proactive attacks that threaten communication security, ultimately increasing device overhead. Furthermore, network conditions are not taken into account in trust evaluation, and the load is unequally distributed. In this research, an Edge-driven model is proposed using a machine-learning approach to enable autonomous communication in a more trusted, controlled manner. The decisions are generated using multiple parameters, and threats are identified with minimal network disruption and data breaches. The trust layer is responsible for maintaining reliable channels to establish robust, long-term routing paths that ensure authorized access to health data across unpredictable environments. In future work, we aim to integrate a software-defined network to enhance the processing power of the proposed framework, enabling rapid threat identification with lower computational cost on network devices. Moreover, we plan to conduct physical deployments and testbed evaluations to further assess the model's effectiveness and performance in real-world distributed environments.

Acknowledgement: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant No. (DGSSR-2025-02-01407).

Funding Statement: This work was supported under grant No. (DGSSR-2025-02-01407) by the Deanship of Graduate Studies and Scientific Research at Jouf University.

Author Contributions: Conceptualization, Menwa Alshammeri, Khalid Haseeb; Formal analysis, Khalid Haseeb and Mamoon Humayun; Methodology, Menwa Alshammeri, and Mona Saleh Alzahrani; Supervision, Mona Saleh Alzahrani and Mamoon Humayun; Validation, Mamoon Humayun and Khalid Haseeb; Writing—original draft, Menwa Alshammeri and Khalid Haseeb; Writing—review & editing, Mamoon Humayun and Mona Saleh Alzahrani. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: All data generated and analyzed in this study are included within the manuscript.

Ethics Approval: Not applicable.

Conflicts of Interest: Given her role as Guest Editor/Editorial Board Members of this journal, Mamoon Humayun had no involvement in the peer review of this article and had no access to information regarding its peer review. Full responsibility for the editorial process for this article was delegated to another journal editor. The authors declare no other conflicts of interest.

References

1. Houssein EH, Othman MA, Mohamed WM, Younan M. Internet of things in smart cities: comprehensive review, open issues and challenges. *IEEE Internet Things J.* 2024;11(21):34941–52.
2. Ullah A, Anwar SM, Li J, Nadeem L, Mahmood T, Rehman A, et al. Smart cities: the role of internet of things and machine learning in realizing a data-centric smart environment. *Complex Intell Syst.* 2024;10(1):1607–37.
3. Ferreira RJ, Ranaweera C, Lee K, Schneider J-G. Energy efficient resource management for real-time IoT applications. *Internet Things.* 2025;30(2):101515. doi:10.1016/j.iot.2025.101515.
4. Ficili I, Giacobbe M, Tricomi G, Puliafito A. From sensors to data intelligence: leveraging IoT, cloud, and edge computing with AI. *Sensors.* 2025;25(6):1763.
5. Kolhe RV, William P, Yawalkar PM, Paithankar DN, Pabale AR. Smart city implementation based on internet of things integrated with optimization technology. *Measur: Sensors.* 2023;27(13):100789. doi:10.1016/j.measen.2023.100789.
6. Syed AS, Sierra-Sosa D, Kumar A, Elmaghraby A. IoT in smart cities: a survey of technologies, practices and challenges. *Smart Cities.* 2021;4(2):429–75.
7. Kong L, Tan J, Huang J, Chen G, Wang S, Jin X, et al. Edge-computing-driven internet of things: a survey. *ACM Comput Surv.* 2022;55(8):1–41. doi:10.1145/3555308.
8. Hua H, Li Y, Wang T, Dong N, Li W, Cao J. Edge computing with artificial intelligence: a machine learning perspective. *ACM Comput Surv.* 2023;55(9):1–35.
9. Mughaid A, Obeidat I, Abualigah L, Alzubi S, Daoud MS, Migdady H. Intelligent cybersecurity approach for data protection in cloud computing based internet of things. *Int J Inf Secur.* 2024;23(3):2123–37. doi:10.1007/s10207-024-00832-0.
10. Aslan Ö, Ozkan-Okay M, Gupta D. Intelligent behavior-based malware detection system on cloud computing environment. *IEEE Access.* 2021;9:83252–71. doi:10.1109/access.2021.3087316.
11. Singh S, Sharma PK, Moon SY, Park JH. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *J Ambient Intell Humaniz Comput.* 2024;15(2):1625–42. doi:10.1007/s12652-017-0494-4.
12. Alzu'bi A, Alomar A, Alkhaza'leh S, Abuarqoub A, Ham-moudeh M. A review of privacy and security of edge computing in smart healthcare systems: issues, challenges, and research directions. *Tsinghua Sci Technol.* 2024;29(4):1152–80. doi:10.26599/tst.2023.9010080.
13. Ferraris D, Fernandez-Gago C, Roman R, Lopez J. A survey on IoT trust model frameworks. *J Supercomput.* 2024;80(6):8259–96. doi:10.1007/s11227-023-05765-4.

14. Nawshin F, Unal D, Hammoudeh M, Suganthan PN. AI-powered malware detection with differential privacy for zero trust security in internet of things networks. *Ad Hoc Netw.* 2024;161(3):103523. doi:10.1016/j.adhoc.2024.103523.
15. Mohammed B, Al-Shareeda M, Hamzah A, Alhasnawi B, Homod R, Alkhabra Y, et al. Security challenges and solutions in Internet of Medical Things (IoMT) communication: a review. *J King Saud Univ Comput Inf Sci.* 2026;38(5):254. doi:10.1007/s44443-026-00658-x.
16. Newaz AI, Sikder AK, Rahman MA, Uluagac AS. A survey on security and privacy issues in modern healthcare systems: attacks and defenses. *ACM Trans Comput Healthcare.* 2021;2(3):1–44. doi:10.1145/3453176.
17. Ahmad I, Shahabuddin S, Malik H, Harjula E, Leppänen T, Loven L, et al. Machine learning meets communication networks: current trends and future challenges. *IEEE Access.* 2020;8:223418–60.
18. Sallabi FM, Khater HM, Tariq A, Hayajneh M, Shuaib K, Barka ES. Smart healthcare network management: a comprehensive review. *Mathematics.* 2025;13(6):988.
19. Syriopoulos PK, Kalampalikis NG, Kotsiantis SB, Vrahatis MN. KNN classification: a review. *Ann Math Artif Intell.* 2025;93(1):43–75.
20. Villegas-Ch W, García-Ortiz J, Sánchez-Viteri S. Toward intelligent monitoring in IoT: AI applications for real-time analysis and prediction. *IEEE Access.* 2024;12:40368–86.
21. Bhatt K, Agrawal C, Bisen AM. A review on emerging applications of IoT and sensor technology for industry 4.0. *Wirel Pers Commun.* 2024;134(4):2371–89. doi:10.1007/s11277-024-11054-x.
22. Poorvi J, Kalita A, Gurusamy M. Reliable and efficient data collection in UAV based IoT networks. *IEEE Commun Surv Tutor.* 2025;28(3):2531–71. doi:10.1109/comst.2025.3550274.
23. Ali TE, Ali FI, Dakić P, Zoltan AD. Trends, prospects, challenges, and security in the healthcare internet of things. *Computing.* 2025;107(1):28. doi:10.1007/s00607-024-01352-4.
24. Alsalemi A, Amira A, Malekmohamadi H, Diao K. Energy data classification at the edge: a comparative study for energy efficiency applications. *Cluster Comput.* 2024;27(3):3259–75. doi:10.1007/s10586-023-04142-3.
25. Al-Quayed F. AI-powered anomaly detection and cybersecurity in healthcare IoT with fog-edge. *Comput Model Eng Sci.* 2026;146(1):45. doi:10.32604/cmes.2025.074799.
26. Maciá-Lillo A, Mora H, Jimeno-Morenilla A, García-D'Urso NE, Azorín-López J. AI edge cloud service provisioning for knowledge management smart applications. *Sci Rep.* 2025;15(1):32246. doi:10.1038/s41598-025-14429-7.
27. Boiko O, Komin A, Malekian R, Davidsson P. Edge-cloud architectures for hybrid energy management systems: a comprehensive review. *IEEE Sens J.* 2024;24(10):15748–72. doi:10.1109/jsen.2024.3382390.
28. Ghosh S, Ghosh SK. Feel: federated learning framework for elderly healthcare using Edge-IoMT. *IEEE Trans Comput Soc Syst.* 2023;10(4):1800–9.
29. Tanveer M, Alharbi AG, Aldossari SA. RePUF-IoT: reconfigurable puf-based authentication protocol for IoT-driven healthcare systems. *IEEE Internet Things J.* 2025;12(22):47575–87.
30. Wang R, Lai J, Zhang Z, Li X, Vijayakumar P, Karuppiah M. Privacy-preserving federated learning for internet of medical things under edge computing. *IEEE J Biomed Health Inform.* 2022;27(2):854–65. doi:10.1109/jbhi.2022.3157725.
31. Maurya S, Jain VK, Chowdhury DR. Delay aware energy efficient reliable routing for data transmission in heterogeneous mobile sink wireless sensor network. *J Netw Comput Appl.* 2019;144(8):118–37. doi:10.1016/j.jnca.2019.06.012.
32. Arthi R, Krishnaveni S. Optimized tiny machine learning and explainable AI for trustable and energy-efficient fog-enabled healthcare decision support system. *Int J Computat Intell Syst.* 2024;17(1):229. doi:10.1007/s44196-024-00631-4.
33. Escorcia-Gutierrez J, Mansour RF, Leal E, Villanueva J, Jimenez-Cabas J, Soto C, et al. Privacy preserving blockchain with energy aware clustering scheme for IoT healthcare systems. *Mobile Netw Appl.* 2024;29(1):1–12. doi:10.1007/s11036-023-02115-9.

34. Saranya S, Anusha P, Chandragandhi S, Kishore OK, Kumar NP, Srihari K. Enhanced decision-making in healthcare cloud-edge networks using deep reinforcement and lion optimization algorithm. *Biomed Signal Process Control*. 2024;92(8):105963. doi:10.1016/j.bspc.2024.105963.
35. Chen W, Wu W, Ouyang Z, Fu Y, Li M, Huang GQ. Event-based data authenticity analytics for IoT and blockchain-enabled ESG disclosure. *Comput Ind Eng*. 2024;190:109992. doi:10.2139/ssrn.4544036.
36. Hashem IA, Siddiq A, Alaba FA, Bilal M, Alhashmi SM. Distributed intelligence for IoT-based smart cities: a survey. *Neural Comput Appl*. 2024;36(27):16621–56. doi:10.1007/s00521-024-10136-y.
37. Villegas-Ch W, Gutierrez R, Sánchez-Salazar I, Mera-Navarrete A. Adaptive security framework for the internet of things: improving threat detection and energy optimization in distributed environments. *IEEE Access*. 2024;12:157924–44.
38. Sarfraz M, Sumra IA, Khalid B, Fatima E. AI-driven predictive threat detection and cyber risk mitigation: a survey. *J Comput Biomed Inform*. 2025;8(2):852.
39. Prabhu TN, Kumar CR, Sabeena B, Fatima H. E2SRP: energy efficient secure routing protocol for edge-assisted wireless sensor networks. *Sustain Comput: Inform Syst*. 2025;49:101287.
40. Zhang X, Hou D, Xiong Z, Liu Y, Wang S, Li Y. EALLR: energy-aware low-latency routing data driven model in mobile edge computing. *IEEE Trans Consum Electron*. 2024;71(2):6612–26.
41. Liang J, Miao H, Li K, Tan J, Wang X, Luo R, et al. A review of multiagent reinforcement learning algorithms. *Electronics*. 2025;14(4):820. doi:10.3390/electronics14040820.