Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.069102

ARTICLE

Lightweight Multi-Agent Edge Framework for Cybersecurity and Resource Optimization in Mobile Sensor Networks

Fatima Al-Quayed*

Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka, 72388, Al Jouf, Saudi Arabia

*Corresponding Author: Fatima Al-Quayed. Email: ffalquayed@ju.edu.sa

Received: 15 June 2025; Accepted: 20 August 2025; Published: 10 November 2025

ABSTRACT: Due to the growth of smart cities, many real-time systems have been developed to support smart cities using Internet of Things (IoT) and emerging technologies. They are formulated to collect the data for environment monitoring and automate the communication process. In recent decades, researchers have made many efforts to propose autonomous systems for manipulating network data and providing on-time responses in critical operations. However, the widespread use of IoT devices in resource-constrained applications and mobile sensor networks introduces significant research challenges for cybersecurity. These systems are vulnerable to a variety of cyberattacks, including unauthorized access, denial-of-service attacks, and data leakage, which compromise the network's security. Additionally, uneven load balancing between mobile IoT devices, which frequently experience link interferences, compromises the trustworthiness of the system. This paper introduces a Multi-Agent secured framework using lightweight edge computing to enhance cybersecurity for sensor networks, aiming to leverage artificial intelligence for adaptive routing and multi-metric trust evaluation to achieve data privacy and mitigate potential threats. Moreover, it enhances the efficiency of distributed sensors for energy consumption through intelligent data analytics techniques, resulting in highly consistent and low-latency network communication. Using simulations, the proposed framework reveals its significant performance compared to state-of-the-art approaches for energy consumption by 43%, latency by 46%, network throughput by 51%, packet loss rate by 40%, and denial of service attacks by 42%.

KEYWORDS: Artificial intelligence; cybersecurity; edge computing; Internet of Things; threat detection

1 Introduction

Edge computing and smart devices, combined with the collaborative support of future technologies, drive growth in IoT ecosystems [1,2]. They maintain the information system and enhance communication among connected devices, providing rapid response times and developing real-time applications [3,4]. Future sensing technologies, leveraging 5G/6G, observe targeted areas and ease end-users with rapid data analysis and processing [5–7]. In recent decades, cloud-centric data processing models have struggled to meet the dynamic and real-time requirements of these applications, especially when balancing scalability with sustainability [6,8]. Due to centralized processing and data storage, intelligent systems are vulnerable to data breaches and security threats, including the single path of data transmission, which can facilitate malicious activities and degrade the performance of IoT networks [9,10]. It decreases the scalability of connected devices and provides a lack of resilience in processing network services. Such systems demand a distributed and low-cost communication process with the integration of intelligence [11,12]. Moreover, establishing trust and achieving long-term connectivity among limited-resource devices plays a crucial role in optimizing resources and enhancing network efficiency [13,14]. The enhancement in security for innovative ecosystems provides the most authorized systems for handling intrusion detection against unauthorized access and data integrity [15–17]. These vulnerabilities increase the potential risks of disrupting critical information and lead to retransmission with additional overhead on IoT devices. Adapting robust security measures promotes a fault-tolerant and resilient system against network attacks, guaranteeing a highly protected and trustworthy environment [18,19]. This research aims to develop a Multi-Agent System (MAS)-based secure framework utilizing edge Computing for mobile sensor networks, exploring the application of artificial intelligence. The framework enhances security against cyber attacks, anomaly detection, and adaptive resource management by integrating trust evaluation, dynamic routing, and blockchain-based validation. This approach aims to improve network resilience, scalability, and energy efficiency while ensuring low latency in IoT environments. The main contributions of the proposed framework are as follows.

i. It developed an adaptive IoT routing system and evaluates trust scores using a Multi-Agent System (MAS) to ensure low-latency, secure data transmission against cyber threats in mobile sensor networks.
ii. It designs a trust-aware, lightweight routing protocol to enhance security and optimize routes with efficient energy management in the IoT-edge network. In addition, the trustworthiness of the proposed framework ensures protection against vulnerabilities and mitigates the risks of cyber attacks through a lightweight sensor-driven decision-making system.
iii. A trust model is designed to emphasize anomaly detection by evaluating multiple metrics, thereby maintaining the integrity and enhancing the reliability of the mobile sensor network in the presence of malicious threats.

The remaining sections are organized as follows. Related work is explained in Section 2. Section 3 provides details of the proposed framework. Section 4 describes the analysis of the performance results. Ultimately, Section 5 concludes the research work.

2 Related Work

The IoT network enables the seamless collection of sensor data through the integration of wireless systems, allowing for real-time monitoring in unpredictable environments [20,21]. It enhances the development functionalities for a bounded network with efficient infrastructure in terms of cost, leading to the timely delivery of crucial data to connected devices [22,23]. The concept of edge computing, on the other hand, processes the collected data locally, decreasing latency through effective bandwidth utilization in smart cities. They establish a scalable and modern network ecosystem to meet the requirements of applications, leveraging emerging technologies for support [24,25]. An autonomous IoT network with an edge-driven approach not only provides a decision-making system in dynamic conditions but also offers timely data analysis under unsustainable situations. In [26], the authors proposed a connection-quality-based Energy-Efficient routing (LQEER) protocol. It incorporates the energy, link quality, and distance parameters to compute the weight for efficient packet transmission. Moreover, it improved the energy efficiency of the network by decreasing unnecessary updates among devices. The performance results demonstrate superior results to existing solutions for dynamic network factors.

For information-centric wireless sensor networks (ICWSN), Vaiyapuri et al. [27] proposed an IoT-enabled cluster-based routing (CBR) protocol, named CBR-ICWSN. It explored a black widow optimization (BWO)-based clustering approach to select optimal cluster heads with a stable network lifetime. Moreover, the CBR-ICWSN based solution also utilized an oppositional artificial bee colony (OABC) enabled routing process, and enhanced the stability of routing paths. A series of simulations was performed to evaluate the performance of the proposed protocol, and its results demonstrated a significant improvement over existing approaches in several network and communication aspects. To implement Distributed Artificial Intelligence

(DAI) using neural networks, authors [28] proposed a novel method that achieves energy efficiency alongside rapid response for intra-cluster communication. The proposed solution offers a novel implementation approach by combining the DAI and Self-Organizing Map (SOM) techniques. The performance results revealed improved solutions for network parameters and computational challenges. Authors [29] introduced a cloud-based SDN solution to improve energy-efficient routing and load balancing in IoT networks. The AI-enabled technique optimizes the clustering of heterogeneous nodes and reduces the additional energy consumption of devices. The high intelligence power of SDN is utilized for the formulation of clusters and effectively manages computational costs. The performance of the proposed approach is validated using simulations that demonstrate its efficacy over existing methods in terms of load balancing and optimization. In [30], the authors proposed a destination-sequenced distance vector (DSDV) framework by exploring deep-Q-learning (DQL). It first modifies the routing information of connected nodes, and later, the next hop count is computed by the DQL method. The Q-values are determined as the distance between linked nodes while accounting for traffic flow. The performance evaluation indicates that DQL-DSDV offers better Quality of Service (QoS) while minimizing packet loss, delay, congestion, and communication costs. From the context of the discussion, it is observed that smart cities face critical research challenges for real-time applications in terms of optimizing and scaling IoT systems with nominal overhead. Moreover, ensuring data trust between constrained devices and adaptive wireless technologies is also demanded for sustainable development with effective cost management. Moreover, scalable and adaptive routing systems are necessary to distribute network traffic evenly among routes and minimize network emissions. Ultimately, it is also evident that reliable solutions are insufficient without effective security policies and edge intelligence to ensure secure data sharing, promoting resilient, fault-tolerant, and sustainable development.

3 Proposed Multi-Agent Based Trust-Aware Framework Using Edge Intelligence

In this section, we present our proposed framework, which introduces a lightweight Blockchain security using multi-agent-enabled collaborative edge intelligence for mobile IoT networks. It enhances resource optimization and trustworthiness in real-time data sharing using reliable network edges. The following subsections explain the details of the proposed framework.

3.1 Modeling and Discussion

In the proposed framework, IoT or edge nodes are designated as agents that independently monitor network conditions, perform trust computing, and intelligently collaborate to balance resource and load distribution. The devices are interconnected in the form the graph $G = (N, L)$ to determine the network behavior by initialing the resource consumptions in terms of energy and latency, where $N = \{n_1, n_2, \ldots, n_m\}$ denotes the set of IoT and edge devices, and $L = \{l_{ij} | i, j \in N\}$ presents the communication links between connected devices. The proposed framework maintains a time-aware record of device neighbors using a dynamic set of edges E in the local table, as defined by the connectivity metric $C_n(i, j)$ in Eq. (1).

$$C_n(i, j, t) = \begin{cases} 1, & \text{if } (i, j) \in E(t) \\ 0, & \text{if } (i, j) \notin E(t) \end{cases} \tag{1}$$

As edge-IoT networks are constrained in terms of resources, energy efficiency plays a crucial role in optimizing the performance for data gathering and transmission. Eq. (2) computes the overall energy consumed for nodes N by exploring computation energy E_{comp_i}, communication E_{comm_i}, and blockchain-based security $E^{\mathrm{BC}}_{\mathrm{sec}_i}$ operation.

$$E_{\mathrm{total}} = \sum_{i=1}^{N} \left(E_{\mathrm{comp}_i} + E_{\mathrm{comm}_i} + E^{\mathrm{BC}}_{\mathrm{sec}_i} \right) \tag{2}$$

Computational Energy $comp_i$ at node i for processing task can be computed as given in Eq. (3).

$$E^i_{comp} = P_{cpu} \cdot T^i_{comp} \tag{3}$$

where P_{cpu} is the power consumption per CPU cycle, and T^i_{comp} is the computation time. Communication Energy $comm_i$ at node i denotes transmission energy consumed from its transmit power P_{tx} and the duration of communication T^i_{comm}, as computed in Eq. (4).

$$E^i_{comm} = P_{tx} \cdot T^i_{comm} \tag{4}$$

Eq. (5) computes the energy overhead $E^{i,\mathrm{BC}}_{\mathrm{sec}}$ at node i using blockchain-based tasks.

$$E^{i,\mathrm{BC}}_{\mathrm{sec}} = \begin{bmatrix} P_{\mathrm{enc}} & P_{\mathrm{dec}} & P_{\mathrm{auth}} & P_{\mathrm{key}} & P_{\mathrm{val}} \end{bmatrix} \cdot \begin{bmatrix} T^i_{\mathrm{enc}} \\ T^i_{\mathrm{dec}} \\ T^i_{\mathrm{auth}} \\ T^i_{\mathrm{key}} \\ T^i_{\mathrm{val}} \end{bmatrix} \tag{5}$$

where P_{enc}, P_{dec}, P_{auth}, P_{key}, and P_{val} are the power consumption values, while T^i_{enc}, T^i_{dec}, T^i_{auth}, T^i_{key}, and T^i_{val} are the corresponding execution times for device i during encryption, decryption, authentication, key management, and validation, respectively. The variable P_{key} represents the power consumption associated with the key management process, which is critical for securing blockchain tasks at node i. Latency is another critical metric for the significant performance of real-time IoT applications, especially when demanded for quality-aware communication services. Thus, the proposed framework is modelled using Eq. (6).

$$D_{\mathrm{total}} = \sum_{i=1}^{m} \left(D_{\mathrm{comp}_i} + D_{\mathrm{comm}_i} + D^{\mathrm{BC}}_{\mathrm{sec}_i} \right) \tag{6}$$

where D_{comp_i} denotes processing delay, with C_i as computational workload and F_i as processing speed, as formulated by Eq. (7)

$$D_{\mathrm{comp}_i} = \frac{C_i}{F_i} \tag{7}$$

D_{comm_i} is the communication delay, where S is data size and B is bandwidth, as given in Eq. (8). Lastly, Eq. (9) determines time overhead $D^{\mathrm{BC}}_{\mathrm{sec}_i}$ introduced by blockchain based security methods.

$$D_{\mathrm{comm}_i} = \frac{S}{B} \tag{8}$$

$$D^{\mathrm{BC}}_{\mathrm{sec}_i} = T^i_{\mathrm{enc}} + T^i_{\mathrm{auth}} + T^i_{\mathrm{cons}} + T^i_{\mathrm{val}} \tag{9}$$

In Algorithm 1, the execution of different logical stages for ensuring multi-agent based routing is depicted.

Algorithm 1: Trust-aware optimized routing using MAS and genetic algorithm

```
Input: Sensor node set $D = \{D_1, D_2, \ldots, D_n\}$;
Communication graph $G = (V, E)$;
Behavioral metrics for each neighbor $j \in N_i$;
Trust-related parameters $(\alpha_{ij}, \bar{S}_j, \Delta t_j, \sigma_j)$
Output: Updated trust scores $T_{\text{new}}(i)$ for each $i \in D$;
Trust-optimized routing paths $P^*$
foreach node $i \in D$ do
    Assign a Multi-Agent System (MAS) agent to node $i$;
    Initialize local trust score $T_i$ using historical metrics;
end
Generate initial population of routing paths using random sampling;
Set Genetic Algorithm parameters: population size $P$, mutation rate $\mu$, crossover rate $c$, number of
 generations $G$;
foreach agent $i$ do
    Compute updated trust score;
    Exchange new trust score with neighboring agents $N_i$;
end
for generation $g = 1$ to $G$ do
    foreach routing solution $s$ in the population do
        Evaluate fitness based on trust-aware cost model;
    end
    Select optimal solutions using selection operator;
    Apply crossover and mutation to generate new population;
    if no improvement in best fitness for $\theta$ consecutive generations then
        convergence achieved;
        break;
    end
end
Select optimal routing path $P^*$ with highest fitness and minimal cost;
Deploy $P^*$ across the edge-IoT network;
```

3.2 Trusted IoT-Edge Resource Optimization and Cybersecurity Using Genetic Algorithm

In this section, the proposed framework utilizes a Genetic Algorithm to optimize the balancing of traffic load in IoT-edge networks, along with effective resource allocation and the inclusion of cybersecurity measures against potential threats. The minimization of network congestion across edge nodes, GA dynamically allocates communication tasks among devices, thereby increasing network intelligence and improving latency and response time. The MAS computes the traffic load at each node i using Eq. (10) based on the link L and transmission rate R between nodes i and j. Moreover, it incorporated the Denial of Service (DoS) resilience factor $\alpha_{i,j}$ to mitigate network attacks, thereby minimizing the impact of DoS attacks on the trustworthiness of IoT flows across the network.

$$T_i = \sum_{j \in N} L_{ij} R_{ij} \cdot (1 - \alpha_{ij}) \tag{10}$$

The optimization function for ensuring efficient resource allocation with minimizing communication cost is computed using Eq. (11).

$$\begin{aligned} &\min \sum_{i=1}^{m} C_i T_i \\ &\text{subject to: } T_i \geq 0, \\ &\qquad\qquad\quad C_i > 0 \end{aligned} \tag{11}$$

Eq. (12) formulates the optimization criteria for network efficiency by incorporating the communication cost C_i and the traffic load T_i at each node. By incorporating the dynamic trust penalty, where trust is computed as a weighted sum of n behavioral metrics between IoT devices.

$$Fit = \sum_{i=1}^{m} (C_i T_i) \cdot \left(1 - \sum_{k=1}^{n} \omega_k \tau_{i,j}^{k}\right) \tag{12}$$

Ultimately, the proposed framework ensures secure IoT routing through the combination of trust computing, dynamic route selection, and its maintenance. It reduces the likelihood of selecting an untrusted node as a forwarder by utilizing realistic network conditions and maintains the selected route in the IoT-edge environment. The agents compute the updated trust score of device i using Eq. (13).

$$T_{\text{new}}(i) = \sum_{j \in N} \beta_{ij} \cdot \left(\gamma \cdot \bar{S}_j \cdot e^{-\lambda \Delta t_j}\right) \cdot (1 - \alpha_{ij}) \cdot \left(1 - \frac{\sigma_j}{\sigma_{\max}}\right) \tag{13}$$

where $T_{\text{new}}(i)$ aggregates trust contributions from all neighboring devices $j \in N$. The term $\bar{S}_j$ denotes the average service success rate of device j. This value is modulated by an exponential decay factor $e^{-\lambda \Delta t_j}$, where Δt_j represents the response delay, giving higher weight to more recent interactions. The parameter γ is a scaling factor to control the intensity of trust contributions, and each contribution is weighted by β_{ij}. The penalty term $(1 - \alpha_{ij})$ reduces the trust score for devices suspected of DoS behavior. Finally, the factor $\left(1 - \frac{\sigma_j}{\sigma_{\max}}\right)$ penalizes trust scores based on the behavioral variance σ_j of device j, where higher variance results in a greater reduction of trust. The node with a low trust score is not permitted to be included in the routing path; accordingly, the proposed framework increases the security level of the IoT-edge network. The cost function Ct_i of node i is computed for the selection of a trusted route based on transmission distance $Dist_{trans}$, energy consumption En_{Comm} and trust of route $T(i, j)$, as given in Eq. (14). Also, DoS penalty φ_{ij} is included to guarantee unreliable routes cost function to ensure that DoS-affected routes with higher $\alpha_{i,j}$ are penalized in the node selection process.

$$C_{t,i}(i, j) = w_1 \cdot \text{Dist}_{trans} + w_2 \cdot \text{En}_{comm} + w_3 \cdot T(i, j) + w_4 \cdot (1 - \alpha_{ij}) \cdot \varphi_{ij} \tag{14}$$

where the weight vector W is represented as $\mathbf{w} = [w_1, w_2, w_3, w_4]$ and each factor has a uniform contribution shown in Eq. (15).

$$w_k = \frac{1}{n}, \quad \forall k \in \{1, 2, 3, 4\} \tag{15}$$

To maintain the routes, MAS agent compute a anomaly score A_i of node i using an average reputation rank R_{avg} of all nodes, the existing reputation rank of a specific node R_i, and the standard deviation D_R, which supports for identify the misbehaving communication of node i, as given in Eq. (16). When DOS attacks are detected then anomaly scores increases the indicating the effecting IoT device on the network routes.

$$A_{\text{score}}(i) = \frac{|R_i - R_{\text{avg}}|}{D_R} \cdot (1 + \alpha_{ij}) \tag{16}$$

Algorithm 2 governs the stages of attaining security and routes maintenance in IoT-edge network.

Algorithm 2: MAS-based trust-aware anomaly detection and routing

```
Input: Reputation scores $R_i$, average $R_{\text{avg}}$, deviation range $D_R$;
       DoS resilience factor $\alpha_{ij}$, anomaly threshold $\theta$;
       Trust parameters: $T_{\text{init}}$, $\lambda$, $\mu$, $\delta$
Output: Anomaly-free graph $G'$, updated routing paths
foreach node $i \in D$ do
    Assign MAS agent;
    if first round then
        $T_i \leftarrow T_{\text{init}}$
    end
    else if active then
        $T_i \leftarrow \lambda T_i + (1 - \lambda) T_{\text{obs}}(i)$
    end
    else if inactive $\delta$ time then
        $T_i \leftarrow T_i \cdot e^{-\mu\delta}$
    end
    Compute anomaly score from $R_i$, $R_{\text{avg}}$, $D_R$, $\alpha_{ij}$;
    if score > $\theta$ then
        blacklist node $i$
    end
end
if $\mathcal{B} \neq \emptyset$ then
    foreach path $P$ do
        if $P$ contains node $i \in \mathcal{B}$ then
            Recompute $P^*$ avoiding $\mathcal{B}$; update routing table
        end
    end
    Update network: $G' = G \backslash \mathcal{B}$;
end
```

Fig. 1 depicts the architecture design of the proposed agent-based trusted routing framework. It is composed of three main layers. First, IoT devices, edge devices, and gateways are connected to a communication system using a wireless standard to sense and collect the environmental field. The data is initially processed at the device level and then forwarded to the second layer for decision-making using artificial intelligence-driven techniques to determine optimized routes. The forwarders on the selected routes are energy efficient and reliable in terms of bandwidth allocation and congestion management. Their roles are shifted when transmitting data in the IoT-edge network and maintaining the devices' connectivity for a more extended period. Ultimately, the trust score is computed to enhance system security, and faulty devices are removed from the routing tables. The trust score is recomputed rapidly, making the system more trustworthy and increasing the likelihood of anomaly detection against threats in IoT-edge networks.

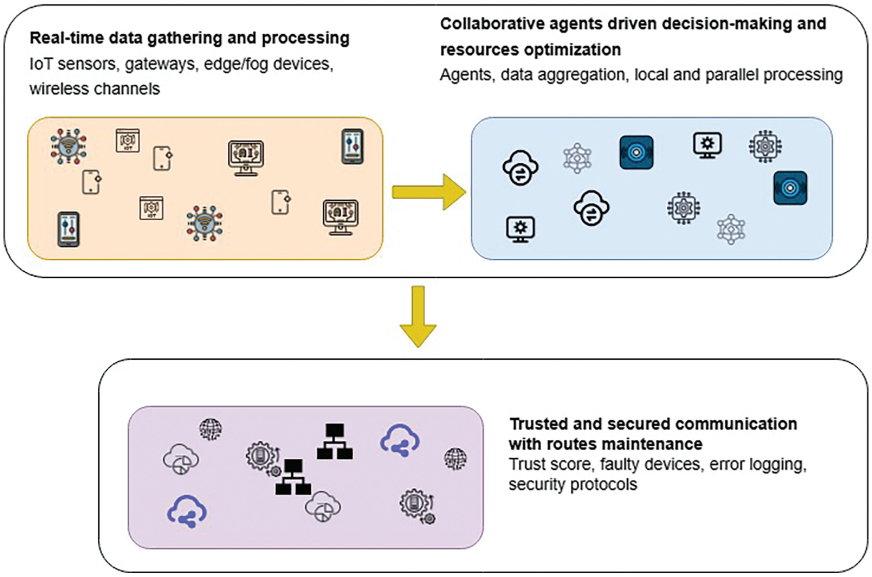

Real-time data gathering and processing
IoT sensors, gateways, edge/fog devices, wireless channels
Collaborative agents driven decision-making and resources optimization
Agents, data aggregation, local and parallel processing
Trusted and secured communication with routes maintenance
Trust score, faulty devices, error logging, security protocols

Figure 1: Architecture design of the proposed agent based IoT-edge trusted framework

Fig. 2 illustrates the flowchart of the proposed framework, which includes agent-based optimization for routing with trust computing. Its main procedures are network modeling to initiate the communication structure, trust computing, and route selection. The samples of selected routes undergo genetic operations, and if the trust value is less than the threshold, the selected route is removed from the forwarding channels. The new cost values are recomputed using a multi-factor technique with a genetic algorithm, and an alternative route is selected for data transmission. Table 1 outlines a range of security threats considered in our proposed framework and highlights the proposed detection and mitigation mechanisms for the edge-IoT environment.

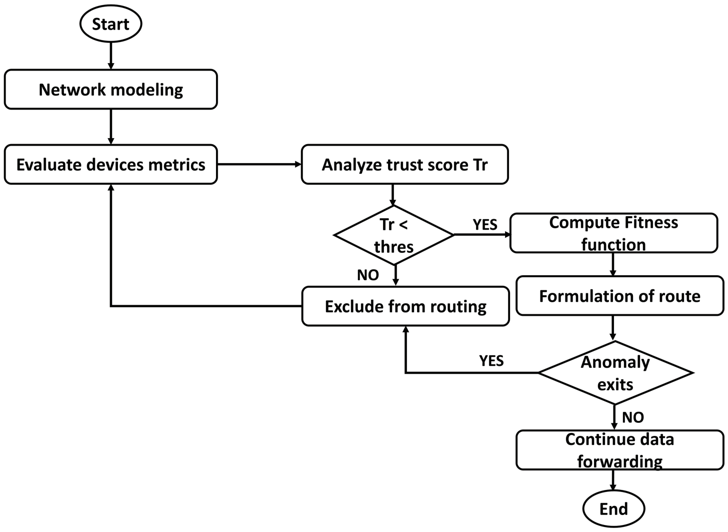


Figure 2: Working flow of proposed agent-based trust-aware optimized IoT-edge routing framework

Table 1: Security threats and detection mechanisms

Attack type	Detection and handling mechanism
DoS	Traffic thresholding based on packet rate and latency
Data tampering	TrustAgent detects anomalies via behavioral deviations (α_{ij})
Routing misbehavior	Trust-aware MAS routing excludes low-trust nodes
Blackhole/Sinkhole	Packet drop patterns and reputation decay trigger isolation
Malware injection	Unusual energy consumption or transmission spikes trigger alerts
Replay attack	Timestamp-based message freshness verification by agents

4 Simulation Description

In this section, we evaluate the proposed Multi-Agent based trusted routing framework against existing work using simulation in an IoT-edge environment, and compare it against related work. The simulations are performed in the NS-3 simulator, and trace files are maintained to store the statistical records. The network field is fixed at 1000 m × 1000 m, populated by 200 to 800 mobile IoT devices, with an initial energy level of 5 J. Sensors are equipped with GPS and have a 4 m transmission radius. Twenty edge devices are distributed in the field, each with sufficient power to collect and process incoming data. The agents in the system communicated using the Message Queuing Telemetry Transport (MQTT) protocol, a lightweight messaging protocol designed for constrained devices. MQTT is particularly well-suited for IoT environments with limited resources, as it enables efficient communication even in low-bandwidth and low-power scenarios. The deployed agents exchanged information about network states, security levels, and trust metrics through MQTT messages, ensuring timely and reliable updates across the IoT network. Smart contracts were implemented and deployed within the NS3 simulation environment to evaluate their performance in a blockchain-based IoT security system. These contracts automate key management, transaction validation, and authentication, essential for secure IoT communication. A custom blockchain module was integrated into NS3 to simulate Ethereum-like contract functionality. The smart contracts were tested on a local NS3 network, where each node represented an IoT device. Key management processes, including encryption key generation and validation, were automated, while transaction validation ensured secure data exchanges. Performance tests evaluated execution time, energy consumption, and transaction throughput under various configurations. Results showed that smart contracts reduced the energy overhead compared to traditional security methods, demonstrating their efficiency in blockchain-secured IoT networks. To evaluate the behavior of the proposed framework, the publicly available IoT-23 dataset [31] is utilized. It comprises network traffic data from 23 distinct IoT devices, including both benign and malicious devices, with approximately 80% benign traffic and 20% malicious traffic. The benign traffic is collected from normal IoT devices, while the malicious traffic simulates various attack scenarios using malicious devices. The imbalance between benign and malicious traffic can influence detection performance. The higher proportion of benign traffic may lead to false positives, where benign traffic is misclassified as malicious. Conversely, the smaller proportion of malicious traffic may increase the likelihood of false negatives, where attacks are not detected. The dataset provides valuable insights into typical IoT traffic and includes features such as connection metadata, packet sizes, and other relevant behavioral statistics. The proposed framework leverages this data to assess security levels and network metrics, and to perform anomaly detection under realistic IoT traffic conditions.

The simulation parameters are depicted in Table 2.

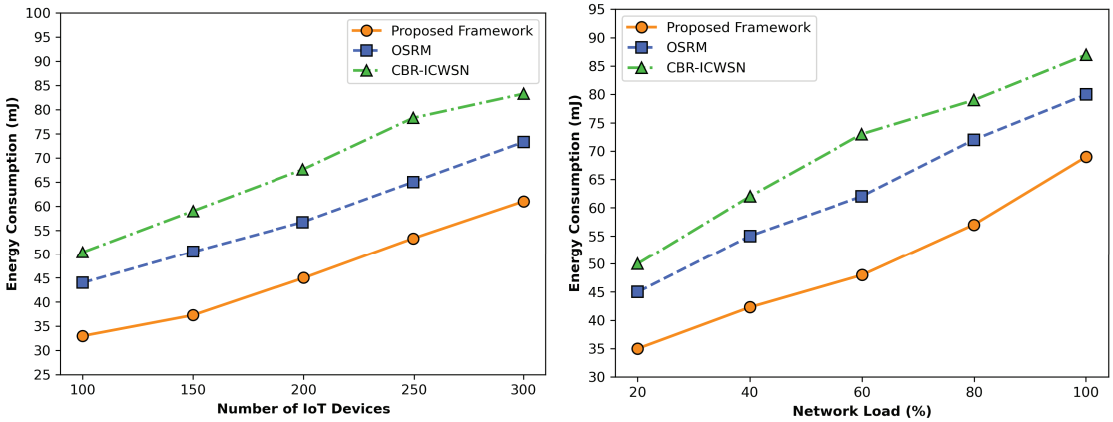
Table 2: Simulation parameters

Parameter	Value
Simulation area	1000 m × 1000 m
Mobile IoT devices	200 to 800
Number of edges	20
Malicious devices	10
Initial energy	5 J
Bandwidth	1 Mbps
Simulations run	60
Mobility model	Random Waypoint
DoS attack model	Flooding-based attack using high-rate CBR traffic from malicious nodes
Trust evaluation	MAS-based scoring via behavioral analysis
Intrusion detection	Threshold-based anomaly detection from traffic stats
Energy model	Radio dissipation model
Trust modules	MAS-trust module
DoS resilience range	0 to 1
GA and trust tuning	Sensitivity analysis on GA parameters and trusted weights (w_1, w_2, w_3, w_4)

Results

Fig. 3a exhibits that the proposed framework improved energy consumption against varying IoT devices as compared to existing solutions by an average of 45.3% and 58%. This is because it utilizes intelligent methods to determine data routing with the assistance of an authentic and trusted scheme. In the prediction phase, the next hop is selected by exploring the optimal edges while also keeping track of link measurements regarding congestion and load balancing. Such an outcome offers an optimal decision and improves the stability of the smart system. Furthermore, the proposed framework's distributed processing, combined with the identification of network past behavior, supports a more lightweight mechanism and efficient communication services for resource optimization. Moreover, the timely capture of malicious nodes prevents the transmission of false and flooded data on the network channels, thereby reducing the ratio of overloaded nodes and enhancing the system's performance, which in turn improves energy efficiency. Fig. 3b depicts the analysis of the proposed framework and existing studies for energy consumption under varying network load. The experimental results revealed that the proposed framework outperforms related studies by 35% and 40.3%. The improvement is attributed to the more effective allocation of resources through the optimization of the Genetic algorithm's learning pattern and a reduction in the forward load on the devices. The trustworthiness, combined with artificial intelligence-driven intelligence, enhances the security performance of the proposed framework and ensures a tamper-proof IoT-edge communication system. Moreover, despite the flooding of malicious packets, trust computing minimizes data disruption and provides seamless connectivity for real-time network applications.

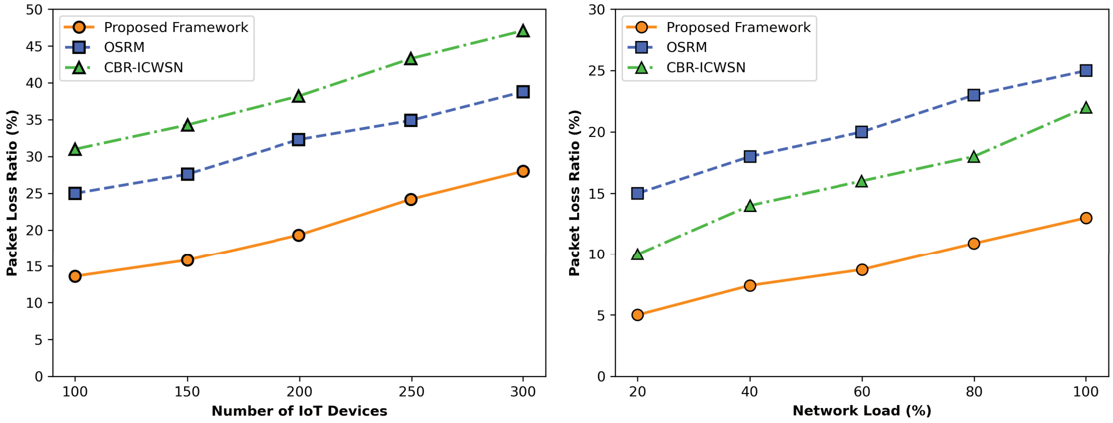
The experimental results of the proposed framework in comparison to the existing solution for packet loss ratio are illustrated in Fig. 4a. Across various IoT devices, it was observed that the proposed framework reduced the packet loss rate by 42.5% and 49.2%. The analysis of multiple criteria, combined with a genetic algorithm, enables the proposed framework to deliver optimal performance from IoT sensors and manage resources effectively, with intelligently controlled network congestion. In addition, selecting several key parameters based on network conditions provides reliable communication links for managing IoT data. Accordingly, the next-hop is more consistent, offers long-run connectivity for continuous data routing, and offers a high-performance maintenance system. In Fig. 4b, the performance analysis depicted improved outcomes of the proposed framework compared to existing studies by 44.5% and 53%. This occurs because routing paths are continuously updated by identifying nearby trustworthy neighbors and extending the lifetime of routes while reducing the traffic load on network-wide devices. The optimizing algorithm not only balances the load on the peer data connection links but also increases the confidence for establishing device trust. Furthermore, routes that are busy in data dissemination are marked as invalid for a particular time, and the source node is informed to formulate an alternative route. The proposed framework ensured fault tolerance while improving the utilization of network resources under dynamic network conditions. As a result, adopting the strategies proposed in the framework enhances the performance of critical IoT deployments in terms of scalability, with uniform traffic distribution, and improves data reception on uncertain IoT wireless channels.



(*a*) Energy consumption vs. number of IoT devices.

(*b*) Energy consumption vs. network load.

Figure 3: Performance impact of Proposed Framework, OSRM, CBR-ICWSN for energy consumption (**a**) varying IoT devices (200–800) and (**b**) varying network load (20%–100%)

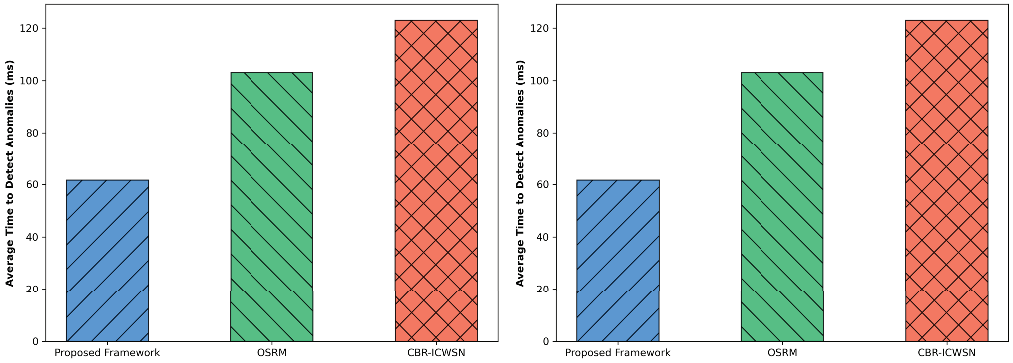


(*a*) Packet loss ratio vs. number of IoT devices.

(*b*) Packet loss ratio vs. network load.

Figure 4: Performance impact of Proposed Framework, OSRM, CBR-ICWSN for packet loss ratio (**a**) varying IoT devices (200–800) and (**b**) varying network load (20%–100%)

Fig. 5a illustrates the performance of the proposed framework in comparison to existing solutions, specifically in terms of anomaly detection ratio for varying numbers of IoT devices. It is a process of identifying malicious patterns in the IoT traffic due to the occurrence of communication faults or system failures. The results analysis has shown that the proposed framework improved the anomaly detection by 30.5% and 39.4%, which is due to both the sensors and intermediate devices being involved in maintaining the trust and reliability of the IoT ecosystem. The intelligence of the proposed framework also supports rerouting crucial IoT data to alternative routes by utilizing crossover and mutation operations of the genetic algorithm. Additionally, agents play a vital role in identifying faulty channels based on the multi-factor trust computation. The trust scores are updated at regular intervals. Thus, it is hard for unauthentic devices and brute-force attacks to resend the fake route requests. Fig. 5b shows the performance analysis of the proposed framework for anomaly detection over varying network load. The statistical analysis revealed that the proposed framework improved the anomaly detection ratio by 35% and 46% compared to existing approaches. This is made possible by the integration of artificial intelligence-driven multi-factor analysis, which optimizes decision-making through collaboration with edge devices. In this process, the routing flags in tables are updated rapidly, and the proposed framework effectively manages transmission costs with latency-aware data forwarding. It enables the timely mitigation of potential network vulnerabilities and ensures the privacy of critical data with lightweight computation. Furthermore, the proposed framework's proactive and reliable routing approach ensures that the IoT-edge system is more suited for real-time applications.

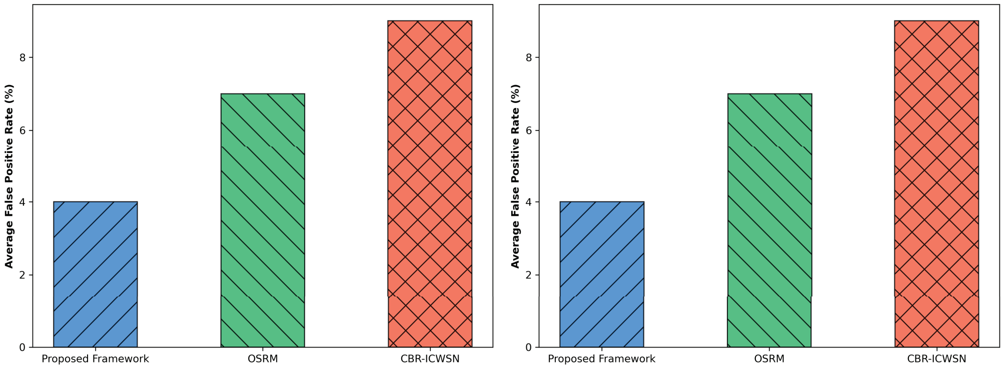


(*a*) Anomaly detection time vs. number of IoT devices.

(*b*) anomaly detection time vs. network load.

Figure 5: Performance impact of Proposed Framework, OSRM, CBR-ICWSN for Anomaly detection time (**a**) varying IoT devices (200–800) and (**b**) varying network load (20%–100%)

Fig. 6a shows the analysis of the proposed framework and existing approaches under varying IoT devices for the false positive rate. It is defined as the number of negative classified samples incorrectly labeled as positive. The performance of the proposed framework was improved for varying IoT devices by 30% and 37% by utilizing a more reliable anomaly detection mechanism. The proposed framework reduces the likelihood of misclassifying regular network traffic as threats by computing trust scores, an adaptive threshold, and pattern analysis in the devices' communication. In addition, the agents play a vital role in identifying authentic devices while sending real-time data to cloud stations; only verified devices are permitted to be part of the IoT system. It reduces false traffic on communication links and increases the trustworthiness level for innovative and unpredictable technologies. Fig. 6b illustrates the performance analysis of the proposed framework compared to existing studies in terms of false positive rate under varying network load. The proposed framework significantly improved the false positive rate by 37% and 44%, respectively. The intelligent behavior of the proposed framework efficiently classified the network traffic as either malicious or usual. The proposed system ensures that device resources are not misused in false positives and provides reliable decisions for identifying network threats. Due to consistency in coping with inauthentic devices, the proposed framework decreases the ratio of false notifications, thus providing a more robust security mechanism. By exploring the proposed security and alarm mechanism, the framework optimizes decision-making through the allocation of resources and a combination of trust. Fig. 7 depicts the impact of the Proposed Framework with OSRM, and CBR-ICWSN in terms of various security metrics under DoS attacks. The results show that the proposed framework improves the trust recovery rate by approximately 45%, isolation efficiency by 55%, mitigation success by 49%, and reduces attack impact by 43% compared to existing methods. These enhancements result from integrating trust evaluation and intelligent anomaly detection, which enable proactive identification and isolation of malicious nodes. Lightweight MAS agents authenticate each IoT device before edge processing, thereby reducing network congestion and mitigating the effects of malicious traffic. Consequently, compromised routes are effectively penalized, significantly boosting network resilience and cybersecurity in dynamic IoT-edge environments.



(*a*) False positive rate vs. number of IoT devices.

(*b*) False positive rate vs. network load.

Figure 6: Performance impact of Proposed Framework, OSRM, CBR-ICWSN for False positive rate (**a**) varying IoT devices (200–800) and (**b**) varying network load (20%–100%)

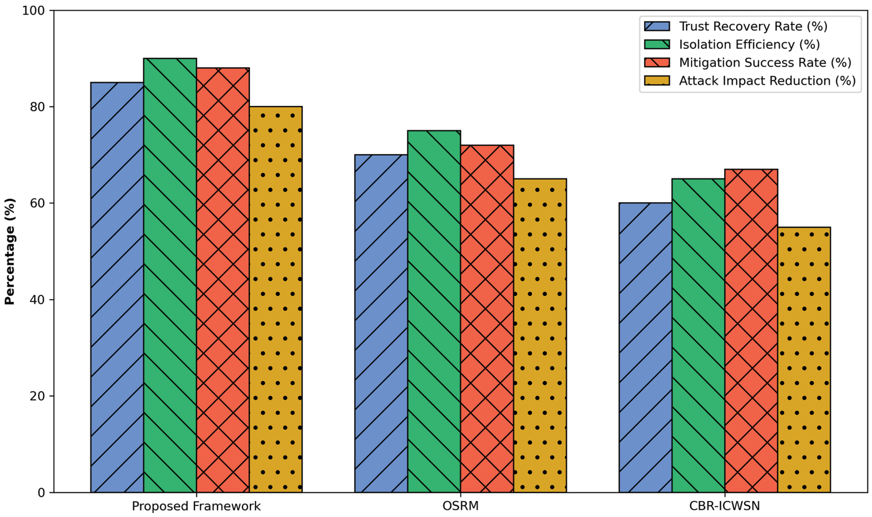


Figure 7: Performance impact of Proposed Framework, OSRM, and CBR-ICWSN under DoS attack for key security metrics

5 Conclusion

The development of sustainable networks has enabled the growth of sensing the real world and processing the demands of connected devices using sensor-driven networks. With the integration of future and advanced technologies, the unpredictable environment is analyzed, and big data is processed through cloud systems. Edge computing provides numerous parallel processing capabilities to enhance scalability and foster growth in automated systems within IoT networks. However, due to the bounded limitations of sensor applications, many existing approaches are insufficient to provide an early response in critical circumstances, posing significant challenges for security and cyber threats. Moreover, deploying in real-world scenarios also presents challenges, such as interoperability among heterogeneous devices, secure data exchange, and dynamic trust management across diverse environments. This work presents an agent-based trusted framework by incorporating multi-metric trust computation and explores artificial intelligence for decision-making. It ensures secure data sharing through lightweight computation between sensors, reducing the likelihood of network anomalies. Additionally, the edge devices perform various local processing services and manage IoT resources by utilizing learning patterns of genetic algorithms. The proposed framework enables efficient energy consumption and reduces latency, facilitating on-time data analysis and effective cybersecurity. However, we aim to implement dynamic strategies for bandwidth allocation to reduce further the computational power required by constrained devices under higher network loads. Such efforts will guarantee more reliable performance in the presence of distributed network threats. In future work, a mobile cloud-based platform can be integrated into the proposed framework to handle on-demand high-power requests for resource management and ensure scalability for the IoT-edge network.

Acknowledgement: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant No. (DGSSR-2025-02-01278).

Funding Statement: This research was supported by the Deanship of Graduate Studies and Scientific Research at Jouf University.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The author declares no conflicts of interest to report regarding the present study.

References

1. Alahi MEE, Sukkuea A, Tina FW, Nag A, Kurdthongmee W, Suwannarat K, et al. Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. Sensors. 2023;23(11):5206. doi:10.3390/s23115206.
2. Hussain I, Elomri A, Kerbache L, El Omri A. Smart city solutions: comparative analysis of waste management models in IoT-enabled environments using multiagent simulation. Sustain Cities Soc. 2024;103(6):105247. doi:10.1016/j.scs.2024.105247.
3. Sneha, Malik P, Sharma R, Ghosh U, Alnumay WS. Internet of Things and long-range antenna's; challenges, solutions and comparison in next generation systems. Microprocess Microsyst. 2023;103(7):104934. doi:10.1016/j.micpro.2023.104934.
4. Ahmad R, Hämäläinen M, Wazirali R, Abu-Ain T. Digital-care in next generation networks: requirements and future directions. Comput Netw. 2023;224(3):109599. doi:10.1016/j.comnet.2023.109599.
5. Alotaibi A, Barnawi A. Securing massive IoT in 6G: recent solutions, architectures, future directions. Internet Things. 2023;22(1):100715. doi:10.1016/j.iot.2023.100715.

6. Ishteyaq I, Muzaffar K, Shafi N, Alathbah MA. Unleashing the power of tomorrow: exploration of next frontier with 6G networks and cutting edge technologies. IEEE Access. 2024;12(254):29445–63. doi:10.1109/access.2024.3367976.
7. Shayea I, El-Saleh AA, Ergen M, Saoud B, Hartani R, Turan D, et al. Integration of 5G, 6G and IoT with Low Earth Orbit (LEO) networks: opportunity, challenges and future trends. Res Eng. 2024;23(3):102409. doi:10.1016/j.rineng.2024.102409.
8. Hazra A, Rana P, Adhikari M, Amgoth T. Fog computing for next-generation internet of things: fundamental, state-of-the-art and research challenges. Comput Sci Rev. 2023;48(5):100549. doi:10.1016/j.cosrev.2023.100549.
9. Poojara SR, Dehury CK, Jakovits P, Srirama SN. Serverless data pipeline approaches for IoT data in fog and cloud computing. Future Generat Comput Syst. 2022;130(8):91–105. doi:10.1016/j.future.2021.12.012.
10. Abbas G, Mehmood A, Carsten M, Epiphaniou G, Lloret J. Safety, security and privacy in machine learning based internet of things. J Sens Actuator Netw. 2022;11(3):38. doi:10.3390/jsan11030038.
11. Golpayegani F, Chen N, Afraz N, Gyamfi E, Malekjafarian A, Schäfer D, et al. Adaptation in edge computing: a review on design principles and research challenges. ACM Transact Autonom Adapt Syst. 2024;19(3):1–43. doi:10.1145/3664200.
12. Bharany S, Badotra S, Sharma S, Rani S, Alazab M, Jhaveri RH, et al. Energy efficient fault tolerance techniques in green cloud computing: a systematic survey and taxonomy. Sustain Energy Technol Assess. 2022;53(2):102613. doi:10.1016/j.seta.2022.102613.
13. Sharma V, Beniwal R, Kumar V. Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications. J Supercomput. 2024;80(8):11338–81. doi:10.1007/s11227-023-05875-z.
14. Manogaran N, Nandagopal M, Abi NE, Seerangan K, Balusamy B, Selvarajan S. Integrating meta-heuristic with named data networking for secure edge computing in IoT enabled healthcare monitoring system. Sci Rep. 2024;14(1):21532. doi:10.1038/s41598-024-71506-z.
15. Haque AB, Bhushan B, Dhiman G. Conceptualizing smart city applications: requirements, architecture, security issues, and emerging trends. Expert Syst. 2022;39(5):e12753. doi:10.1111/exsy.12753.
16. Bradbury M, Jhumka A, Watson T. Information management for trust computation on resource-constrained IoT devices. Future Generat Comput Syst. 2022;135(2):348–63. doi:10.1016/j.future.2022.05.004.
17. Wang B, Dabbaghjamanesh M, Kavousi-Fard A, Yue Y. AI-enhanced multi-stage learning-to-learning approach for secure smart cities load management in IoT networks. Ad Hoc Netw. 2024;164(2):103628. doi:10.1016/j.adhoc.2024.103628.
18. Batista AdS, Dos Santos AL. A survey on resilience in information sharing on networks: taxonomy and applied techniques. ACM Comput Surv. 2024;56(12):1–36. doi:10.1145/3659944.
19. Alshudukhi KS, Ashfaq F, Jhanjhi N, Humayun M. Blockchain-enabled federated learning for longitudinal emergency care. IEEE Access. 2024;12(5):137284–94. doi:10.1109/access.2024.3449550.
20. Trigka M, Dritsas E. Wireless sensor networks: from fundamentals and applications to innovations and future trends. IEEE Access. 2025;13(1):96365–99. doi:10.1109/access.2025.3572328.
21. 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. doi:10.3390/s25061763.
22. Anitha P, Vimala H, Shreyas J. Comprehensive review on congestion detection, alleviation, and control for IoT networks. J Netw Comput Appl. 2024;221(2):103749. doi:10.1016/j.jnca.2023.103749.
23. Nilima SI, Bhuyan MK, Kamruzzaman M, Akter J, Hasan R, Johora FT. Optimizing resource management for IoT devices in constrained environments. J Comput Commun. 2024;12(8):81–98. doi:10.4236/jcc.2024.128005.
24. Alshudukhi KS, Humayun M, Alwakid GN. Integrating edge intelligence with blockchain-driven secured IoT healthcare optimization model. Comput Mater Contin. 2025;83(2):1973–86. doi:10.32604/cmc.2025.063077.
25. 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.
26. Shahid M, Tariq M, Iqbal Z, Albarakati HM, Fatima N, Khan MA, et al. Link-quality-based energy-efficient routing protocol for WSN in IoT. IEEE Trans Consum Electron. 2024;70(1):4645–53. doi:10.1109/tce.2024.3356195.

27. Vaiyapuri T, Parvathy VS, Manikandan V, Krishnaraj N, Gupta D, Shankar K. A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing. Wirel Pers Commun. 2022;127(1):39–62. doi:10.1007/s11277-021-08088-w.
28. Goswami P, Mukherjee A, Hazra R, Yang L, Ghosh U, Qi Y, et al. AI based energy efficient routing protocol for intelligent transportation system. IEEE trans Intell Transp Syst. 2021;23(2):1670–9. doi:10.1109/tits.2021.3107527.
29. Udayaprasad P, Shreyas J, Srinidhi N, Kumar SD, Dayananda P, Askar SS, et al. Energy efficient optimized routing technique with distributed SDN-AI to large scale I-IoT networks. IEEE Access. 2024;12:2742–59. doi:10.1109/access.2023.3346679.
30. Adil M, Usman M, Jan MA, Abulkasim H, Farouk A, Jin Z. An improved congestion-controlled routing protocol for IoT applications in extreme environments. IEEE Internet Things J. 2024;11(3):3757–67. doi:10.1109/jiot.2023.3310927.
31. Stoian NA. Machine learning for anomaly detection in IoT networks: Malware analysis on the IoT-23 data set [master's thesis]. Enschede, the Netherland: University of Twente; 2020.