Computer Modeling in Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.073039

ARTICLE

AI-Driven SDN and Blockchain-Based Routing Framework for Scalable and Trustworthy AIoT Networks

Mekhled Alharbi[1,*], Khalid Haseeb[2] and Mamoona Humayun[3,*]

[1]Department of Software Engineering, College of Computer and Information Sciences, Jouf University, Sakaka, 72388, Al-Jouf, Saudi Arabia

[2]Department of Computer Science, Islamia College Peshawar, Peshawar, 25120, Pakistan

[3]School of Computing, Engineering and the Built Environment, University of Roehampton, London, SW155PJ, UK

*Corresponding Authors: Mekhled Alharbi. Email: mn-alharbi@ju.edu.sa;
Mamoona Humayun. Email: mamoona.humayun@roehampton.ac.uk

Received: 09 September 2025; Accepted: 28 October 2025; Published: 26 November 2025

ABSTRACT: Emerging technologies and the Internet of Things (IoT) are integrating for the growth and development of heterogeneous networks. These systems are providing real-time devices to end users to deliver dynamic services and improve human lives. Most existing approaches have been proposed to improve energy efficiency and ensure reliable routing; however, trustworthiness and network scalability remain significant research challenges. In this research work, we introduce an AI-enabled Software-Defined Network (SDN)- driven framework to provide secure communication, trusted behavior, and effective route maintenance. By considering multiple parameters in the forwarder selection process, the proposed framework enhances network stability and optimizes decision-making. In addition, the involvement of the blockchain consensus algorithm and the intelligence of the SDN controller enables a proposed framework for robust authentication and a verifiable process of data blocks. Ultimately, only trusted devices are selected for routing, and malicious threats are prevented as data is forwarded to the cloud system. The extensive experimental analysis demonstrated that the proposed framework significantly improved energy consumption by 48%, packet loss by 49%, response time by 46%, and data transfer rate by 45% compared with existing techniques.

KEYWORDS: Blockchain; energy efficiency; Internet of Things; software-defined networking; trust management

1 Introduction

IoT integrated with smart technologies enables the development of real-time critical systems for the timely processing and automation across various domains, e.g., vehicle interaction, healthcare, and agriculture [1–3]. Artificial Intelligence of Things (AIoT) networks continuously collect observed data and maintain seamless connectivity among devices and physical objects [4,5]. The integration of such technologies drives growth in modern ecosystems and fosters smarter interactions among research communities and industries [6–8]. In recent decades, edge computing has enabled smart cities to access resources near source devices and to provide distributed computing with minimal overhead, while enabling effective resource management [9,10]. AI-driven techniques and edge computing support timely decision-making for autonomous services and enable timely detection of malicious activities, leveraging existing security policies [11,12]. Despite this, most proposed approaches still lack privacy-preserving, lightweight authentication mechanisms for adaptive environments, and thus are unable to address issues of fault tolerance and efficient bandwidth utilization [13–15]. In addition, due to the rapid involvement of malicious devices in the IoT system over

the insecure Internet, they are increasingly posing significant network threats, including involvement of untrusted devices, denial-of-service (DoS), and routing hole attacks [16–18]. In this research, we present a framework that integrates AI and blockchain technologies to increase intelligence at both the device and edge levels. It reduces additional computational costs in the constraint applications, and the involvement of the SDN controller helps optimize the decision-making system. It mitigates threats even in the presence of faulty IoT devices and enhances network-wide communication security through an authentic, authorized, and trusted system. The major contributions of our work are provided as follows.

i. A trust-aware routing mechanism integrating blockchain technology with SDN programmability is proposed to improve energy efficiency and enable real-time decision-making for AIoT networks.
ii. Dynamic trust computation using AI-driven behavioral analysis to continuously evaluate dynamic metrics, ensuring secure routing and minimizing route disruptions.
iii. It improves and enhances the privacy, and strengthens resilience of IoT systems using an AI-powered anomaly detection mechanism and mitigates network threats.

The paper is structured into the following sub-sections. Related work is discussed in Section 2. Section 3 explains the functionalities of the proposed framework. Performance analysis is done in Section 4, and Section 5 provides the conclusion of our work with future directions.

2 Related Work

Wireless devices and sensors are interconnected to develop real-time AIoT applications and generate large amounts of environmental data [19,20]. In smart cities, security against malicious attacks is a demanding requirement in most existing approaches that involve IoT systems and edge processing. It leads to compromised network integrity and unauthorized access during data transmission and decision-making [21–23]. Recent studies have explored blockchain for decentralized trust management [24,25], SDN for network programmability and centralized policy enforcement [26,27], and AI-driven approaches for threat detection and dynamic routing optimization [28,29]. However, most solutions often face scalability challenges, high computational costs, and limited end-to-end IoT security integration, motivating the need for a unified, lightweight framework. The proposed framework [30] integrates blockchain technology for decentralized, immutable data management, Artificial Intelligence for dynamic data analysis and threat detection, and advanced searchable encryption for secure, efficient queries. A patient-centered data access model that combines blockchain and trust chains enhances safety and efficiency, while also demonstrating a return on investment. The blockchain-based architecture ensures the integrity and immutability of medical data from IoMT devices, enabling decentralized, tamper-proof storage. In [31], the authors introduce a Free Node-based Routing Algorithm (FNRA) to provide efficient routing for the SIoT network. It compares the forwarding capabilities of relay and source nodes and distinguishes between in-community and out-of-community message forwarding. FNRA classifies devices into four structures and dynamically adopts forwarding strategies. The analysis of FNRA is evaluated through a range of experiments that demonstrate its superior performance compared to existing approaches. In [32], an Enhanced Energy Efficient Clustering and Routing protocol is proposed to address network issues. The protocol consists of three stages: selecting the best Cluster Head (CH) nodes using k-means clustering, designating a Super Cluster Head using an Adaptive Neuro Fuzzy Inference System, and determining the most energy-efficient multi-path routing strategy using the Black Widow Optimization algorithm. The proposed multi-level hierarchical secure and optimal routing (ML-HSOR) protocol [33] addresses network issues through four stages: registration, clustering, authentication, and optimal routing. Sensor nodes are registered with the base station using unique identities. A Markov model with adaptive weighting selects the optimal Cluster Head (CH) to improve network performance. Multi-level trust evaluation detects malicious nodes during authentication,

and data transmission is optimized using the polarity learning-based chimp optimization algorithm (PL-COA). Authors [34] proposed BlockDLO, an IoT security approach combining blockchain technology with deep learning. The architecture consists of five phases: (1) network localization using chaotic map-based identification, (2) page rank-based clustering for edge computing, (3) shared-chain technique with deep distributed file system and Ethereum smart contracts for block creation and data security, (4) communication route optimization via page rank centrality, and (5) deep learning integration to detect malicious data using authenticated received data, forming an efficient intrusion detection system. In [35], the authors proposed a MANET-IoT architecture using Hybrid K-Mode Clustering (HKMC) for cluster building and Spider Monkey Optimization (SMO) to identify the optimal Cluster Head (CH). An Energy-aware Multi-Attribute Trust (EMAT) model, based on Multi-Agent Reinforcement Learning (MA-RL), computes trust values and selects optimal routes using the Secure & Energy Score (SES) methodology. To enhance data security, a Multi-Attribute Cryptography (MAC) approach is introduced, improving energy efficiency and security in MANET-IoT environments. Authors of [36] present a novel multiobjective SDN-based framework for IoT sensors, ensuring end-to-end (E2E) QoS across multiple domains with heterogeneous traffic service classes (TSC). The framework employs a two-layer SDN architecture to manage QoS based on specific service demands. An optimal additive weighting module (OAWM) ranks TSCs and prioritizes service parameters such as delay, PLR, and jitter. At the same time, global controller statistics enable E2E QoS provisioning by mapping service requests from IoT sensors. Table 1 summarizes the significant contributions and limitations of existing approaches for IoT systems and for achieving data privacy and integrity.

Table 1: Comparison of existing schemes

Existing schemes	Limitations	Contributions
AI-driven Trust Management System (AI-DTMS) with blockchain	Challenges related to scalability when integrating AI with blockchain, especially in large-scale IoT deployments	Combines AI and blockchain to enhance the security of IoT networks by enabling dynamic trust management.
Free Node-based Routing Algorithm (FNRA)	Potential performance issues arise in highly dynamic networks, especially when nodes frequently join or leave.	Optimizes routing in IoT networks by utilizing community structures and selecting the optimal nodes for message forwarding.
Federated Deep Reinforcement Learning (FDRL) for IoT-enabled WSNs	Devices' efficient collaboration is limited due to the bounded resources and overhead.	Enables decentralized routing decision-making via federated deep reinforcement learning quality of servicet adapts to network conditions.
Enhanced Energy Efficient Clustering and Routing protocol	Multi phase routing increases complexity and network scalability.	Improves energy efficiency and routing performance by applying k-means clustering and Black Widow Optimization to select optimal paths.

(Continued)

Table 1 (continued)

Existing schemes	Limitations	Contributions
Multi-Level Hierarchical Secure and Optimal Routing (ML-HSOR) protocol	Potential delays in trust evaluation can impact the overall system performance, especially in real-time applications.	Utilizes a multi-stage approach that incorporates trust evaluation and optimizes data transmission paths for enhanced security and efficiency.
BlockDLO: Blockchain and Deep Learning for IoT security	The integration of deep learning for intrusion detection introduces high computational costs and energy consumption.	Combines blockchain technology and deep learning for secure data transmission, intrusion detection, and data integrity in IoT systems.
MANET-IoT architecture with Energy-aware Multi-Attribute Trust (EMAT) model	Excessive overhead incurs the complexity in trust evaluation and route-selection mechanisms.	Improves energy efficiency and communication security in IoT networks.
Reliable Routing based on Reinforcement Learning in SD-IoT Networks (RRSN)	Determining appropriate values for weight factors and managing delay caused by SDN controllers.	Optimized QoS-aware reliable routing is proposed for SD-IoT networks, integrating intelligent routing techniques with SDN and ML.
Multiobjective SDN-based Framework for IoT Sensors	the management of multiple QoS goals within diverse network traffic leads to additional overheads.	Rank traffic classes and provides the priority to QoS factors improves network metrics in terms of delays, lost rate and delivery performance.

3 Materials and Methods

The proposed framework models an IoT deployment with edge nodes and an SDN controller as a time-varying graph, where devices make routing decisions aided by blockchain-backed trust and AI-based anomaly detection. Let $V = \{v_1, \ldots, v_N\}$ denote IoT devices and edge nodes, and $E(t)$ the set of wireless links at time t. Each node v_i has coordinates (x_i, y_i), residual energy $E_i(t)$, transmit/receive electronics energy per bit E_{elec}, and amplification factor ϵ_{amp}; links have distance d_{ij} and one-hop latency $L_{ij}(t)$. The maximum radio range is $r_{\max}$, and packets have size s bits. Fig. 1 illustrates the architectural flow among the developed phases of the proposed framework.

To establish connectivity in physical space, the distance d_{ij} between two nodes, v_i and v_j, is defined as the Manhattan distance, expressed in Eq. (1).

$$d_{ij} = |x_i - x_j| + |y_i - y_j| \tag{1}$$

A link is considered available if the two nodes are within communication range of each other. The binary link indicator $a_{ij}(t)$ captures the condition, as defined in Eq. (2).

$$a_{ij}(t) = \begin{cases} 1, & d_{ij} \le r_{\max}, \\ 0, & \text{otherwise.} \end{cases} \tag{2}$$

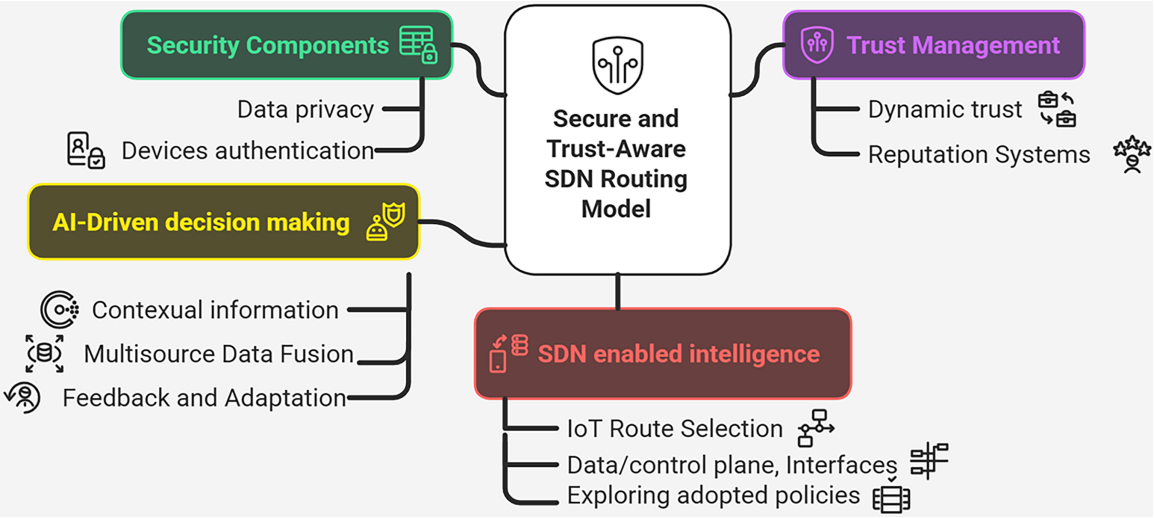

Figure 1: Phases of the proposed trust-aware SDN-driven AIoT model

The energy to transmit s bits over distance d_{ij} follows a standard radio model with path-loss exponent $\gamma \geq 2$. The per-transmission energy is defined in Eq. (3), while the reception consumes only electronic energy, and the per-reception energy at node v_j is given in Eq. (4).

$$E_{tx}(i \to j) = E_{\text{elec}} \cdot s + \epsilon_{\text{amp}} \cdot s \cdot d_{ij}^{\gamma} \tag{3}$$

$$E_{rx}(j) = E_{\text{elec}} \cdot s \tag{4}$$

The nodes' residual energy is updated after a single transmit-receive exchange to track their lifetimes using Eq. (5).

$$E_i(t+1) = E_i(t) - \mathbb{1}_{\{i\ \text{tx}\}} E_{tx}(i \to j) - \mathbb{1}_{\{i\ \text{rx}\}} E_{rx}(i) \tag{5}$$

where $\mathbb{1}\{\cdot\}$ is an indicator function that determines whether node i transmitted or received during the current time slot. Specifically, $\mathbb{1}_{\{i\ \text{tx}\}}$ subtracts the energy consumed by transmission $E_{tx}(i \to j)$, and $\mathbb{1}_{\{i\ \text{rx}\}}$ subtracts the energy consumed by reception $E_{rx}(i)$.

In the proposed framework, the link reliability over a sliding window of W packets is measured as the successful delivery ratio, capturing short-term wireless quality. The reliability $R_{ij}(t)$ is defined as the fraction of packets that were successfully received within the window and can be formulated using Eq. (6).

$$R_{ij}(t) = \frac{\sum_{\tau=t-W+1}^{t} \mathbb{1}\{\text{pkt}\ (i,\ j,\ \tau) \in \mathcal{S}\}}{W} \tag{6}$$

where $\mathbb{1}\{\cdot\}$ is an indicator function, and $\mathcal{S}$ is the set of successfully received packets during time slot τ. A node's local forwarding reliability aggregates its incident links to stabilize trust against fluctuations in the reliability of individual links. The neighborhood-averaged reliability is computed based on Eq. (7).

$$\overline{R}_i(t) = \frac{1}{|\mathcal{N}_i(t)|} \sum_{j \in \mathcal{N}_i(t)} R_{ij}(t) \tag{7}$$

where $\mathcal{N}_i(t) = \{j \,|\, a_{ij}(t) = 1\}$ is the neighbor set.

In addition, the proposed framework integrates blockchain to contribute an auditable record of behavior. Let $B_i(t)$ represent the blockchain-derived trust component for node i, which is updated using exponential smoothing based on the ratio of valid on-chain events. The trust update is given in Eq. (8).

$$B_i(t) = \alpha B_i(t-1) + (1-\alpha) \cdot \frac{V_i(t)}{T_i(t)}, \quad \alpha \in [0, 1] \tag{8}$$

where α is the smoothing factor, $V_i(t)$ is the number of valid events for node i at time t, and $T_i(t)$ is the total number of events for node i at time t. Each block k records the hashed state and transactions to ensure immutability. With the previous block's hash h_{k-1}, timestamp t_k, node set digest S_k, and transaction list Tx_k, the block hash is computed as given in Eq. (9).

$$h_k = H\left(h_{k-1} \parallel t_k \parallel S_k \parallel Tx_k \parallel \text{nonce}_k\right) \tag{9}$$

where $H(\cdot)$ is a cryptographic hash function, and $\parallel$ denotes concatenation.

The proposed framework explores Proof of Authority (PoA) as the consensus algorithm for establishing and maintaining the blockchain network. The following parameters are considered for blockchain operations:

i. A time needed to generate a new block is denoted by Block Time (T_{block}) and varies based on the network conditions and consensus algorithm. It is typically fixed for PoA, but can change with realistic, distributed loads.
ii. Block Size (S_{block}) is a dynamic parameter, and it contains collected data from IoT devices.
iii. Block Verification Time ($\tau_{\text{verify}}(t)$) is a dynamic parameter, and it represents the time while verifying a newly created block. Verification depends on network conditions, block size, and required computational power.
iv. Broadcast Time ($\tau_{\text{broadcast}}(t)$) denotes the time for flooding the blocks to all devices. Due to network conditions, latency, topology, etc., the value of this parameter varies.

Thus, the blockchain overhead $O_{\text{BC}}(t)$ is the sum of the block verification and broadcast times as given in Eqs. (10) to (12).

$$O_{\text{verify}}(t) = \tau_{\text{verify}}(t) \tag{10}$$

$$O_{\text{broadcast}}(t) = \tau_{\text{broadcast}}(t) \tag{11}$$

$$O_{\text{BC}}(t) = O_{\text{verify}}(t) + O_{\text{broadcast}}(t) \tag{12}$$

Edge-hosted AI assigns an anomaly score $A_i(t)$ using logistic regression [37] to each node based on its feature vector $\mathbf{f}_i(t)$, which can include metrics like inter-arrival variance, drop burst, and trust transition. The score is computed using a logistic regression head on an encoder function $g(\cdot)$ as given in Eq. (13).

$$A_i(t) = \sigma\left(w^{\top} g(f_i(t)) + b\right) \tag{13}$$

where $\sigma(z)$ is the sigmoid function, defined as given in Eq. (14).

$$\sigma(z) = \frac{1}{1+e^{-z}} \tag{14}$$

The trust score $T_i(t)$ of node i at time t is computed as a combination of node reliability $\overline{R}_i(t)$, blockchain-derived trust $B_i(t)$, and anomaly score $A_i(t)$, subject to $\beta_1 + \beta_2 + \beta_3 = 1$, as defined in Eq. (15).

$$T_i(t) \in \left\{\beta_1 \overline{R}_i(t) + \beta_2 B_i(t) + \beta_3 (1 - A_i(t)) \mid \beta_1 + \beta_2 + \beta_3 = 1\right\} \tag{15}$$

It represents the trust score $T_i(t)$ of node i at time t, where $\overline{R}_i(t)$ denotes the reliability or reputation of node i, $B_i(t)$ represents the blockchain-derived trust component for node i, and $A_i(t)$ is the anomaly score, indicating the likelihood of abnormal behavior, subject to the constraint $\beta_1 + \beta_2 + \beta_3 = 1$. The node reliability $\overline{R}_i(t)$, blockchain-derived trust $B_i(t)$, and anomaly score $A_i(t)$ are integrated to compute the trust score $T_i(t)$ of node i at time t, while $\beta_1 + \beta_2 + \beta_3 = 1$.

Also the proposed framework determines link-wise latency $L_{ij}(t)$, and it the combination of transmission ($T_{ij}^{\text{tx}}(t)$) that represents the associated with the link from device i to j at time t, propagation ($T_{ij}^{\text{prop}}(t)$) that measures the time taken in traveling the signal from device i to device j, queuing ($T_{ij}^{\text{queue}}(t)$) measures a time that a packet waits in the queue for for transmission, and processing delays ($T_{ij}^{\text{proc}}(t)$) indicates the time needed for the data to be processed, as shown in Eq. (16).

$$L_{ij}(t) = \begin{bmatrix} T_{ij}^{\text{tx}}(t) \\ T_{ij}^{\text{prop}}(t) \\ T_{ij}^{\text{queue}}(t) \\ T_{ij}^{\text{proc}}(t) \end{bmatrix} \tag{16}$$

In Eq. (17), a composite cost is computed by penalizing the factors such as delay, low energy, low trust, and blockchain overhead. The weighted parameters α, β, γ, and δ are combined with the parameters for balanced contribution such that (α, β, γ, $\delta \geq 0$).

$$w_{ij}(t) = \alpha \cdot L_{ij}(t) + \beta \cdot \frac{1}{E_j(t) + \varepsilon} + \gamma \cdot \frac{1}{T_j(t) + \varepsilon} + \delta \cdot O_{\text{BC}}(t) \tag{17}$$

Delay of the link between nodes i and j is denoted by $L_{ij}(t)$r, the energy depletion represents by $E_j(t)$, $T_j(t)$ is the trust score, and blockchain overhead is denoted by $O_{\text{BC}}(t)$. Also, to avoid undefined values in computations, a small constant ε is introduced. At the end, SDN determines the minimum-cost route under the current state as given in Eq. (18) for a path P.

$$P^{\star}(t) = \arg\min_{P \in \mathcal{P}} \; C(P, t), \qquad C(P, t) = \sum_{(i,j) \in P} w_{ij}(t) \tag{18}$$

To ensure end-to-end service guarantees, the data-plane delay of the selected route is monitored and sent back to the controller for reconfiguration, as given in Eq. (19).

$$D_{\text{e2e}}(P^{\star}, t) = \sum_{(i,j) \in P^{\star}} L_{ij}(t) \tag{19}$$

where $D_{\text{e2e}}(P^{\star}, t)$ is the total delay of the selected route $P^{\star}$ at time t, and $L_{ij}(t)$ is the delay on the link between nodes i and j. Table 2 summarizes the definitions and values of the key parameters used in the tests.

Algorithm 1 computes trust for IoT devices using blockchain technology to achieve more reliable, trustworthy communication. It enables distributed route establishment and lightweight computing while incurring the least overhead on the IoT system. $O(|V|)$ is used to evaluate the time complexity, where $|V|$ represents the number of nodes. Algorithm 2 governs the optimization of task distribution across network

edges and provides energy-efficient communication integrated blockchain technology. $O(|V| + |N|)$ is used for time complexity to validate the block, where $|N|$ is the number of edge nodes and $|V|$ is the number of trusted nodes.

Table 2: Definitions and values of parameters used in the tests

Parameter	Value/Range
Window size	200 samples
Smoothing factor (α)	0.5
Trust threshold (τ)	0.7
Coefficient for average reputation (β_1)	0.4
Coefficient for belief (β_2)	0.3
Coefficient for activity (β_3)	0.3
Error term (ε)	0.05

Algorithm 1: Trust-aware evaluation across edges

Input: Set of nodes V, Direct trust DT_i, Indirect trust IT_i, Decay factor α, Trust threshold τ
Output: Updated trust scores T_i

for *each node* $i \in V$ **do**
  Compute direct trust DT_i;
  Compute indirect trust IT_i;
  Calculate new trust T_i^{new} by combining T_i^{old}, DT_i, and IT_i with the decay factor α;
  if $T_i^{new} < \tau$ **then**
    Mark node i as untrusted;
  end
  Update T_i to T_i^{new};
end

Algorithm 2: Blockchain-assisted secure data transmission

Input: Sensor data D_i, Node trust scores T_i, Blockchain ledger BC, Hash function $H(\cdot)$
Output: Verified and securely transmitted data blocks

for *each trusted node i* **do**
  if $T_i \geq \tau$ **then**
    Block header: $B_{hdr} = H(D_i \| T_i \| timestamp)$;
    Generate block: $B_i = \{B_{hdr}, D_i, T_i\}$;
    Integration to blockchain: $BC \leftarrow BC \cup B_i$;
    Validation of block;
    if *block validated by majority consensus* **then**
      Transmit block to cloud;
    end
  end
end

4 Simulation Description

This section presents the experimental results of the proposed framework as compared to FNRA [31] and ML-HSOR [33], conducted using the NS-3 simulator. The deployed environment is composed of edge devices, IoT sensors, SDN controller, and sink nodes. IoT devices are resource-constrained, with static edges, limited processing power for intensive computing, and limited support for other resources. SDN controllers act as centralized managers, collecting global information about devices and optimizing decision-making. The dimension area is fixed to 2000 m × 2000 m, with 10–50 malicious devices, and 100–1000 sensors. The parameters considered for evaluating performance in a simulated environment are illustrated in Table 3.

Table 3: Simulation parameters

Parameter	Value
Simulation area	2000 m × 2000 m
Number of sensors	100 to 1000
Initial energy	5J per sensor
Malicious devices	10 to 50
Number of simulations	50 runs
Reputation weight (β)	0.3
Activity weight (γ)	0.2
Packet size	256 bits
Decay factor (α)	0.7
Edge devices	40
Analyzing scenarios	Varying network load and connection time
SDN controllers	2
Neighbor weight (δ)	0.5
Trust threshold (τ)	0.8

4.1 Analysis for Varying Connection Time

Fig. 2 demonstrates the performance evaluation of the proposed framework and existing approaches in terms of energy consumption over varying connection time. The results reveal an average improvement of 44% for the proposed framework. It is due to intelligent routing enabled by SDN, which reduces additional retransmissions among devices. Also, dynamic trust-aware evaluation increases confidence among devices and aligns communication more stably with the support of multiple parameters. Moreover, it dynamically updates trust scores to improve communication reliability upon fault detection in an IoT environment. The system's optimal decision-making enhances efficient resource management and ultimately results in the least energy consumption in crucial areas. The results of the data transfer rate analysis are depicted in Fig. 3 for the proposed framework and existing solutions. Based on the analysis, the proposed framework significantly improved data transfer rate by an average of 47%. It is because of considering dynamic attributes for detecting network threats while imposing the least communication overhead. In addition, the updation of established routes by reevaluating the quality of service factors decreases congestion on the forwarders and enhances the functionality of data forwarding. Trust computing also provides a more reliable process for route selection, which helps maintain a consistent communication system. Fig. 4 measures and evaluates the performance of the proposed framework for packet loss rate under varying connection times. Based on the statistical analysis, the proposed framework reduces packet loss relative to relevant approaches by an average of 49%. It is due

to the integration of artificial intelligence techniques and the SDN controller's controllability. Moreover, the edges are more robust at detecting malicious threats, with prompt trust evaluation and continuous reevaluation based on behavior and network conditions. In addition, the reliable detection of communication anomalies with trust penalties and block-wise authentication reduces the number of malicious packets in the network, thereby enabling only verified device participation and optimizing data flow with greater accuracy via fault-tolerant links. The performance of response time under varying connection counts is depicted in Fig. 5 for the proposed framework and existing approaches. The remarkable improvement of 42% on average has been observed for the proposed framework. It is due to the intelligent learning technique, which considers different device conditions and effective load distribution along the established routes. It maintains route stability for a more extended period and improves the timely response to requested nodes. Unlike other approaches, the SDN controller serves as a centralized hub for the proposed framework and continually monitors network behavior. In case any anomaly is detected, the routes are reformulated to improve the system's responsiveness.

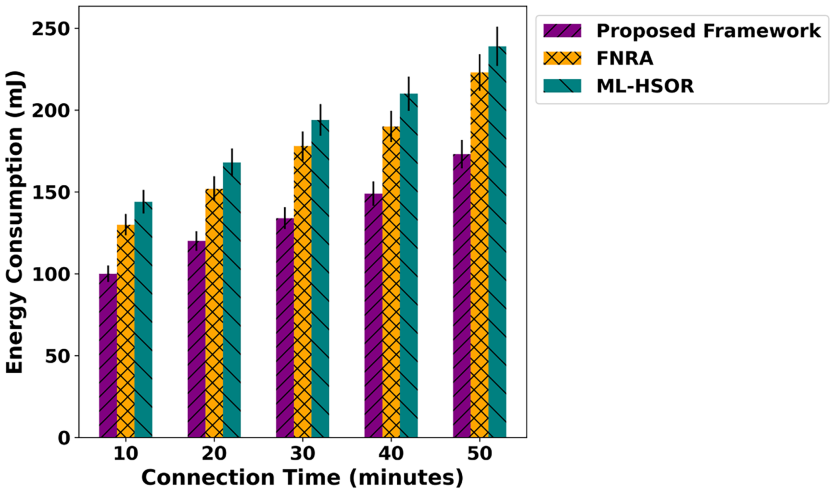

Figure 2: Impact of varying connection time on energy consumption

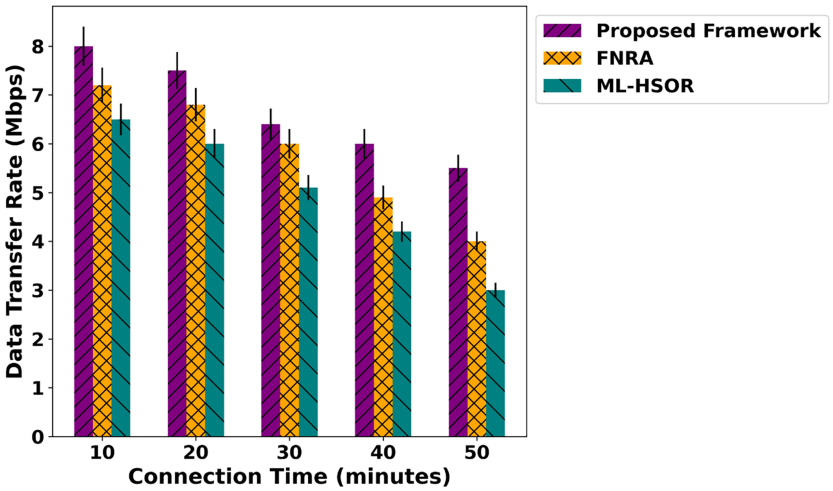

Figure 3: Impact of varying connection time on data transfer rate

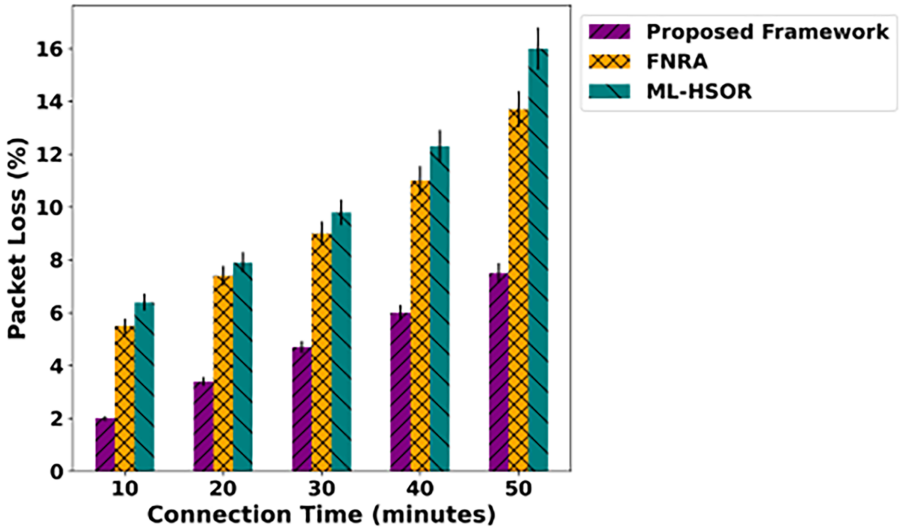

Figure 4: Impact of varying connection time on packet loss ratio

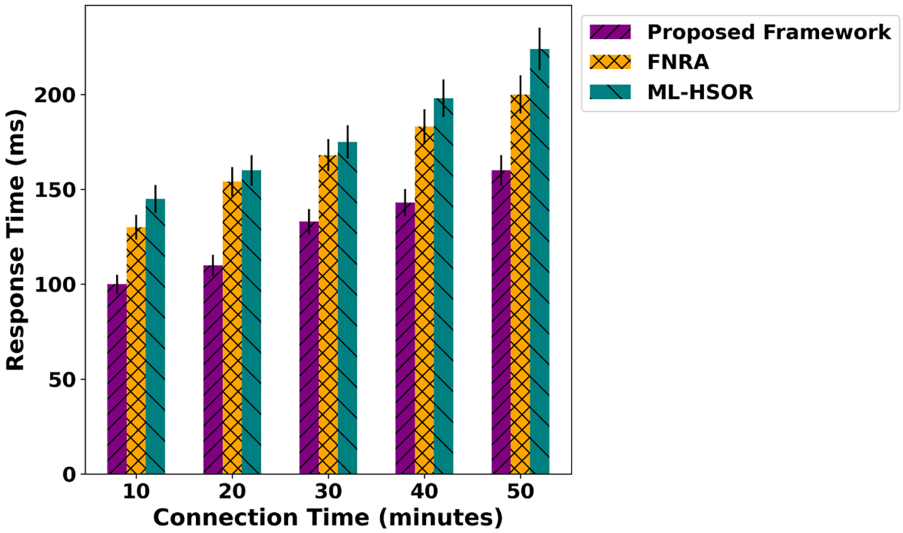

Figure 5: Impact of varying connection time on response time

4.2 Analysis for Varying Network Load

As shown in Fig. 6, the proposed framework exhibits a substantial improvement in energy efficiency across different network loads, achieving an average enhancement of 52% compared to existing solutions. This is made possible by the intelligent routing mechanism, which supports data-forwarding decisions based on trustworthy devices and integrates them via an authentic, blockchain-assisted scheme. During the prediction phase, the next hop is selected by exploring trusted edges while continuously monitoring network metrics, thereby balancing load across links. This ensures optimal decisions, improves route stability, and strengthens the resilience of the innovative system. By leveraging the robustness of the SDN controller and incorporating network feedback, the proposed framework enables lightweight operations. It ensures efficient communication services for resource optimization, ultimately improving energy utilization in the IoT network. In Fig. 7, the proposed framework is compared with existing approaches in terms of data transfer rate across varying network load. The results highlight notable improvements of 41% in the delivery

of data packets over the unpredictable environment. These improvements are attributed to the use of dynamic trust computation during route and channel selection, combined with authentic and secure blockchain validation. By optimizing learning patterns and establishing energy-aware, authenticated forwarding routes, the proposed framework achieves stronger, more reliable connectivity, even under the influence of malicious nodes. In addition, the routing costs are updated regularly based on dynamic conditions, providing more reliable paths for forwarding IoT data. The performance evaluation of the proposed framework and related studies is depicted in Fig. 8 over varying network load. Based on the results, the proposed framework significantly enables the timely detection of malicious activities through trust-aware computing. The trust scores are dynamically updated using network behavior and realistic conditions. In addition, the devices are mutually authentic based on the history and only authorize access to reliable connections. The SDN controller effectively manages resources and meets application demands on time. The reliable connections are frequently updated, and up-to-date information about the channels is maintained for further analysis. This continuous re-evaluation provides energy-efficient routes and long-term stable connections to increase the delivery ratio of data packets in real-time systems. In Fig. 9, the performance analysis of response time for the proposed framework and existing approaches is presented. Based on the results, the proposed framework improves the system's response time by an average of 50% with the support of network edges and trusted devices. It reduces the additional overhead on devices and the number of incoming requests for faulty devices to process data packets at the edges. The data routes are selected and maintained using dynamic network factors, which leads to lower processing power for the constraint devices and improves the overall efficacy of the communication system.

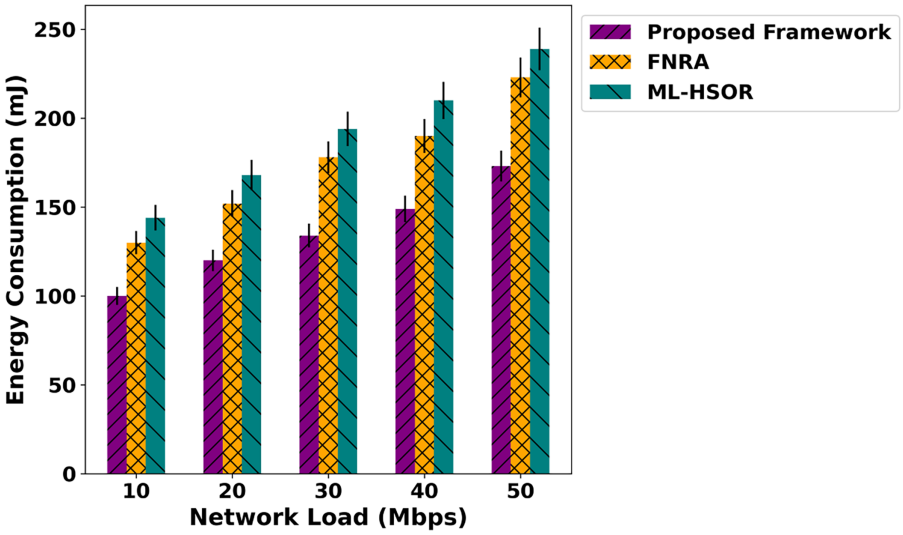

Figure 6: Impact of varying network load on energy consumption

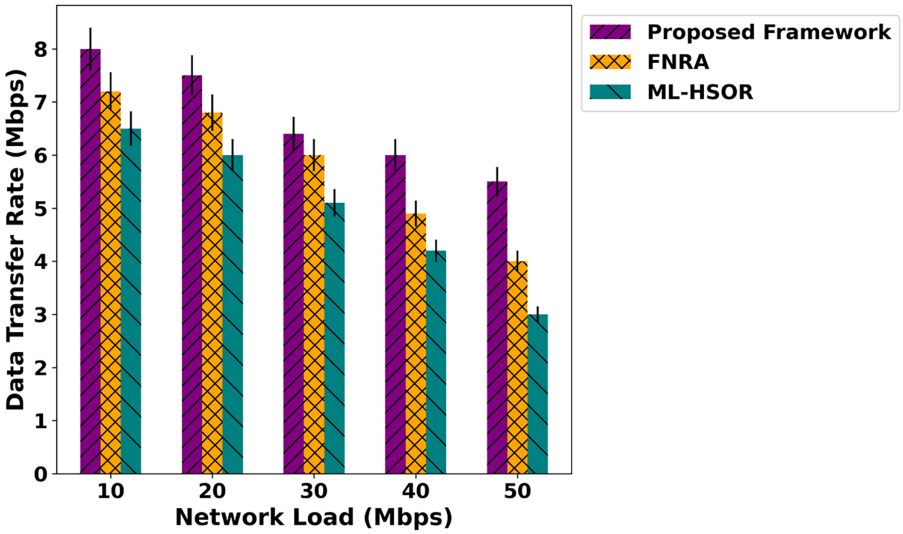

Figure 7: Impact of varying network load on data transfer rate

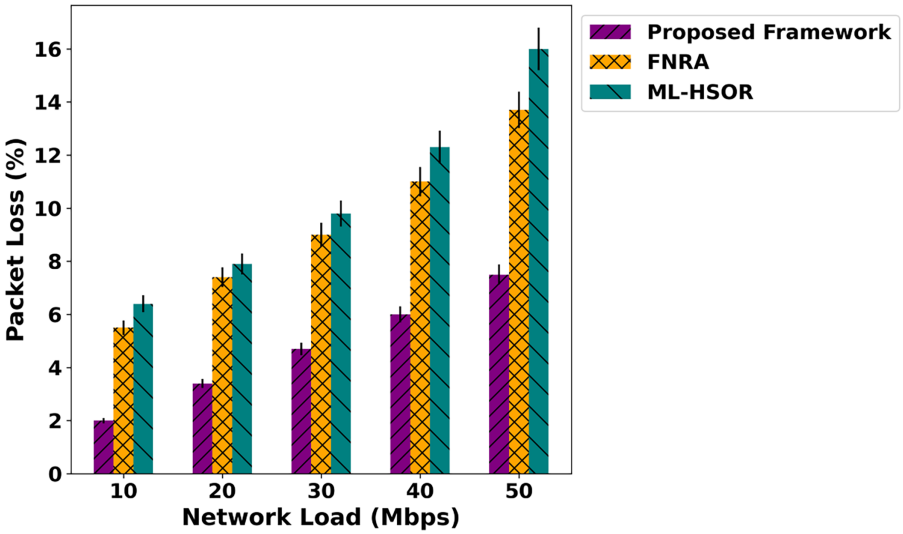

Figure 8: Impact of varying network load on packet loss ratio

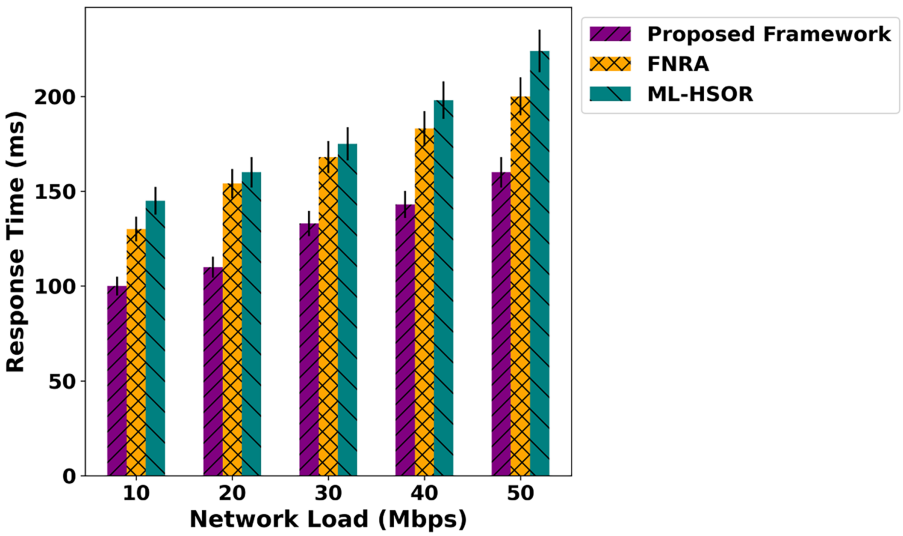

Figure 9: Impact of varying network load on response time

5 Conclusion

Real-time applications play a vital role in sensing and processing the collected data from the observed environment. IoT, along with emerging technologies, has led to the development and growth of smart cities. These systems are composed of sensors and many physical objects deployed in the sensing field to periodically gather data and forward it to the edge/cloud for further analysis in harsh environments. This research proposed a blockchain-assisted framework integrated with AI techniques to optimize network performance and security. In addition, intelligence is provided at the edges via lightweight computing to enhance decision-making and evenly distribute load across data forwarders and constraint devices. The network behavior and device conditions are frequently reevaluated for dynamic trust computation, thereby offering a more trustworthy system even in the presence of malicious threats. The consideration of multiple factors in route selection involves addressing energy holes across network boundaries by efficiently maintaining routes. In future work, we intend to incorporate a deep learning model to improve system stability under dynamic conditions and enhance distributed threat detection, thereby enhancing the security of the proposed framework in a large-scale IoT system.

Acknowledgement: The authors gratefully acknowledge the financial support from the Deanship of Graduate Studies and Scientific Research at Jouf University.

Funding Statement: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant No. DGSSR-2025-02-01669.

Author Contributions: Conceptualization, Mekhled Alharbi, Mamoona Humayun; Formal analysis, Mekhled Alharbi, Mamoona Humayun; Methodology, Mamoona Humayun, Khalid Haseeb; Supervision, Mamoona Humayun, Mekhled Alharbi; Validation, Mekhled Alharbi, Khalid Haseeb; Writing—original draft, Mekhled Alharbi, Khalid Haseeb; Writing—review & editing, Mekhled Alharbi, Mamoona Humayun. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data available on request from the authors.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Zeng F, Pang C, Tang H. Sensors on Internet of Things systems for the sustainable development of smart cities: a systematic literature review. Sensors. 2024;24(7):2074. doi:10.3390/s24072074.
2. Fadhel MA, Duhaim AM, Saihood A, Sewify A, Al-Hamadani MN, Albahri A, et al. Comprehensive systematic review of information fusion methods in smart cities and urban environments. Inf Fusion. 2024;107:102317. doi:10.1016/j.inffus.2024.102317.
3. Alshammeri M, Humayun M, Haseeb K, Alwakid GN. AI-driven sentiment-enhanced secure IoT communication model using resilience behavior analysis. Comput Mater Contin. 2025;84(1):433–46. doi:10.32604/cmc.2025.065660.
4. Yamini B, Pradeep G, Kalaiyarasi D, Jayaprakash M, Janani G, Uthayakumar G. Theoretical study and analysis of advanced wireless sensor network techniques in Internet of Things (IoT). Meas Sens. 2024;33:101098.
5. Magara T, Zhou Y. Internet of things (IoT) of smart homes: privacy and security. J Electr Comput Eng. 2024;2024(1):7716956. doi:10.1155/2024/7716956.
6. Kumar V, Yu J, Li F, Zhang J, Ye F, Karri S, et al. Seamless wireless communication platform for Internet of Things applications. IEEE Wireless Commun. 2022;30(6):102–10. doi:10.1109/mwc.006.2200097.
7. Albouq SS, Abi Sen AA, Almashf N, Yamin M, Alshanqiti A, Bahbouh NM. A survey of interoperability challenges and solutions for dealing with them in IoT environment. IEEE Access. 2022;10:36416–28. doi:10.1109/access.2022.3162219.
8. Alwakid GN, Humayun M, Haseeb K, Shafique A. Real-time e-health framework for efficient AI-driven disability monitoring using secured Internet of Medical Things. Computing. 2025;107(8):163. doi:10.1007/s00607-025-01519-7.
9. Sharma M, Tomar A, Hazra A. Edge computing for industry 5.0: fundamental, applications, and research challenges. IEEE Internet of Things J. 2024;11(11):19070–93. doi:10.1109/jiot.2024.3359297.
10. Oliveira F, Costa DG, Assis F, Silva I. Internet of Intelligent Things: a convergence of embedded systems, edge computing and machine learning. Internet Things. 2024;26:101153. doi:10.1016/j.iot.2024.101153.
11. Rong Y, Mao Y, Cui H, He X, Chen M. Edge computing enabled large-scale traffic flow prediction with GPT in intelligent autonomous transport system for 6G network. IEEE Trans Intell Transp Syst. 2024;26:17321–38. doi:10.1109/tits.2024.3456890.
12. 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.
13. Fouda MM, Fadlullah ZM, Ibrahem MI, Kato N. Privacy-preserving data-driven learning models for emerging communication networks: a comprehensive survey. IEEE Commun Surv Tutor. 2025;27(4):2505–42.
14. Feretzakis G, Papaspyridis K, Gkoulalas-Divanis A, Verykios VS. Privacy-preserving techniques in generative AI and large language models: a narrative review. Information. 2024;15(11):697. doi:10.3390/info15110697.
15. Menon UV, Kumaravelu VB, Kumar CV, Rammohan A, Chinnadurai S, Venkatesan R, et al. AI-powered IoT: a survey on integrating artificial intelligence with IoT for enhanced security, efficiency, and smart applications. IEEE Access. 2025;13:50296–339. doi:10.1109/access.2025.3551750.
16. Bergies S, Aljohani TM, Su SF, Elsisi M. An IoT-based deep-learning architecture to secure automated electric vehicles against cyberattacks and data loss. IEEE Trans Syst Man Cybern Syst. 2024;54(9):5717–32. doi:10.1109/tsmc.2024.3409314.
17. Abbas S, Bouazzi I, Ojo S, Al Hejaili A, Sampedro GA, Almadhor A, et al. Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks. PeerJ Comput Sci. 2024;10:e1793. doi:10.7717/peerj-cs.1793.
18. Kumar G, Alqahtani H. Machine learning techniques for intrusion detection systems in SDN-recent advances, challenges and future directions. Comput Model Eng Sci. 2023;134(1):89–119. doi:10.32604/cmes.2022.020724.
19. Bhatt K, Agrawal C, Bisen AM. A review on emerging applications of IoT and sensor technology for industry 4.0. Wireless Personal Commun. 2024;134(4):2371–89. doi:10.1007/s11277-024-11054-x.

20. Abdulhussain SH, Mahmmod BM, Alwhelat A, Shehada D, Shihab ZI, Mohammed HJ, et al. A comprehensive review of sensor technologies in IoT: technical aspects, challenges, and future directions. Computers. 2025;14(8):342. doi:10.3390/computers14080342.
21. Aouedi O, Vu TH, Sacco A, Nguyen DC, Piamrat K, Marchetto G, et al. A survey on intelligent Internet of Things: applications, security, privacy, and future directions. IEEE Commun Surv Tutor. 2025;27(2):1238–92.
22. 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 Trans Autonomous and Adaptive Syst. 2024;19(3):1–43. doi:10.1145/3664200.
23. Ahmed M, Soofi AA, Raza S, Li Y, Khan F, Khan WU, et al. A comprehensive survey on RIS-enhanced physical layer security in UAV-assisted networks. IEEE Internet of Things J. 2025;12(16):32538–62. doi:10.1109/jiot.2025.3569716.
24. Islam R, Bose R, Roy S, Khan AA, Sutradhar S, Das S, et al. Decentralized trust framework for smart cities: a blockchain-enabled cybersecurity and data integrity model. Sci Rep. 2025;15(1):23454. doi:10.1038/s41598-025-06405-y.
25. Shi L, Wang T, Xiong Z, Wang Z, Liu Y, Li J. Blockchain-aided decentralized trust management of edge computing: toward reliable off-chain and on-chain trust. IEEE Netw. 2024;38(5):182–8. doi:10.1109/mnet.2024.3399270.
26. Bringhenti D, Yusupov J, Zarca AM, Valenza F, Sisto R, Bernabe JB, et al. Automatic, verifiable and optimized policy-based security enforcement for SDN-aware IoT networks. Comput Netw. 2022;213:109123. doi:10.1016/j.comnet.2022.109123.
27. Priyadarsini M, Bera P, Das SK, Rahman MA. A security enforcement framework for SDN controller using game theoretic approach. IEEE Trans Dependable Secur Comput. 2022;20(2):1500–15. doi:10.1109/tdsc.2022.3158690.
28. Kavitha D, Thejas S. AI enabled threat detection: leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE Access. 2024;12:173127–36. doi:10.1109/access.2024.3493957.
29. Villegas-Ch W, Govea J, Gurierrez R, Mera-Navarrete A. Optimizing security in IoT ecosystems using hybrid artificial intelligence and blockchain models: a scalable and efficient approach for threat detection. IEEE Access. 2025;13:16933–58. doi:10.1109/access.2025.3532800.
30. Khan S, Khan M, Khan MA, Khan MA, Wang L, Wu K. A blockchain-enabled AI-driven secure searchable encryption framework for medical IoT systems. IEEE J Bio Health Inform. doi:10.1109/JBHI.2025.3538623.
31. Xu F, Lyu Y, Ahmed M, Xiong Z, Deng M, Wang W, et al. Improving routing performance in social internet of things with FNRA: the free node-based approach. Alexandria Eng J. 2024;88:68–79. doi:10.1016/j.aej.2024.01.010.
32. Senkumar M, Arafat IS, Nathiya R, Nishath SH. Enhanced energy efficient clustering and routing algorithm in wireless sensor network. Wireless Personal Commun. 2024;138(3):1531–58. doi:10.1007/s11277-024-11549-7.
33. 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.
34. Kokila M, Reddy KS. BlockDLO: blockchain computing with deep learning orchestration for secure data communication in IoT Environment. IEEE Access. 2024;12:134521–40. doi:10.1109/access.2024.3462735.
35. Aravindan S, Rajaram A. Energy-aware multi-attribute trust modal for secure MANET-IoT environment. Multimed Tools Appl. 2024;83(38):85637–62. doi:10.1007/s11042-024-20075-4.
36. Ali J, Song HH, Roh BH. An SDN-based framework for E2E QoS guarantee in Internet-of-Things devices. IEEE Internet Things J. 2025;12(1):605–22.
37. Solomon FAM, Sathianesan GW, Ramesh R. Logistic regression trust—a trust model for Internet-of-Things using regression analysis. Comput Syst Sci Eng. 2023;44(2):1125–42. doi:10.32604/csse.2023.024292.