Computer Modeling in Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.072326

ARTICLE

Trust-Aware AI-Enabled Edge Framework for Intelligent Traffic Control in Cyber-Physical Systems

Khalid Haseeb[1], Imran Qureshi[2,*], Naveed Abbas[1], Muhammad Ali[3], Muhammad Arif Shah[4] and Qaisar Abbas[2]

[1]Department of Computer Science, Islamia College Peshawar, Peshawar, 25120, Pakistan
[2]College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, 11432, Saudi Arabia
[3]School of Computer Science & IT, Institute of Management Sciences (IMSciences), Peshawar, 25100, Pakistan
[4]City University of Science and Information Technology (CUSIT), Peshawar, 25000, Pakistan

*Corresponding Author: Imran Qureshi. Email: iqureshi@imamu.edu.sa

Received: 24 August 2025; Accepted: 01 December 2025; Published: 23 December 2025

ABSTRACT: The rapid evolution of smart cities has led to the deployment of Cyber-Physical IoT Systems (CPS-IoT) for real-time monitoring, intelligent decision-making, and efficient resource management, particularly in intelligent transportation and vehicular networks. Edge intelligence plays a crucial role in these systems by enabling low-latency processing and localized optimization for dynamic, data-intensive, and vehicular environments. However, challenges such as high computational overhead, uneven load distribution, and inefficient utilization of communication resources significantly hinder scalability and responsiveness. Our research presents a robust framework that integrates artificial intelligence and edge-level traffic prediction for CPS-IoT systems. Distributed computing for selecting forwarders and analyzing threats across the IoT system enhances stability while improving energy efficiency. In addition, to achieve efficient routing decision-making, the Artificial Bee Colony algorithm is explored to enhance the effective utilization of network resources across IoT systems. Based on the simulation results, the proposed framework achieves remarkable performance in terms of throughput by 38%–41%, packet loss ratio by 30%–33%, security risk mitigation by 35%–37%, and trust level by 41%–44% as compared to existing work.

KEYWORDS: Adaptive learning; cyber-physical applications; communication threats; edge intelligence; trust computing

1 Introduction

IoT networks and edge computing enable rapid development in the automation process, facilitating data collection and processing [1,2]. The real-world system utilizing future-generation technologies not only maintains the observing field but also reduces human efforts in monitoring and controlling the remote environment [3,4]. Recently, many existing systems require consistent and distributed services to achieve reliable and load-balanced approaches integrated with CPS-IoT, enabling timely responses from the requested devices and support for intelligence in smart cities [5,6]. Moreover, due to the dynamic infrastructure, incorporating security and threat analysis is also a significant research challenge [7,8], as well as controlling the massive data traffic generated by interconnected devices [9,10]. Moreover, such issues degrade the performance of sensor-driven applications in terms of scalability and effective load distribution across heterogeneous infrastructure [11,12]. Furthermore, due to the increasing use of battery-powered IoT

devices, optimizing energy consumption is a critical research problem for physical systems. Thus, smart cities require an efficient solution for energy scheduling and allocation of network resources [13,14]. Due to the dynamic and inconsistent structure of IoT systems, they are more suspicious in the presence of malicious threats, and are vulnerable to distributed attacks to compromise the data with unauthorized access [15,16]. Most existing approaches cope with network threats, but at the cost of additional overhead and rapidly degrading energy resources. Thus, recently, many researchers have focused on developing reliable and fault-tolerant network solutions to address privacy and trustworthiness issues [17,18]. Such a system should be able to tackle faulty requests for connections and provide robust authentication and verifiable strategies to permit only authorized devices to access resources and sensitive data. Moreover, lightweight encryption/decryption must be designed to prevent against potential threats and mitigate multifaceted communication holes [19,20]. It has been observed that most IoT-CPS systems require resource optimization and trustworthiness approaches, necessitating the development of energy efficiency and threat analysis solutions. Therefore, our research aims to provide a framework with traffic-based analysis for route selection, considering edge-level local processing with realistic parameters and environmental conditions. In this research, we introduce a framework for a T-CPS environment by integrating trusted and load-balanced devices with the collaboration of edge-level intelligence. The trust computation enhances consistency among vehicles and reduces network traffic by effectively managing threats and malicious behavior.

i. Firstly, by exploring the Artificial Bee Colony algorithm, a distributed computing approach is employed to optimize resource usage while transmitting transportation data in smart cities.
ii. Secondly, the proposed framework is trained to analyze device behavior and identify abnormal traffic resulting from malicious activities.
iii. Lastly, only authentic data can be analyzed and processed by the trusted edges for issuing connected requests to devices.

The article is organized as follows: Related work is explained in Section 2, Section 3 explains the functionalities of the proposed framework, the experimental setup and results analysis are discussed in Section 4, and at the end, this research study is concluded in Section 5.

2 Related Work

IoT networks enable many smart communication systems for Cyber-Physical communication, advancing automation and real-time data management [21,22]. Unlike cloud networks, edge computing provides access to resources near the source device, enabling rapid data processing for real-time analysis. It improves response time and increases device performance in critical applications by reducing latency and overhead [23,24]. These systems enhance task computation effectiveness by distributing the load across intermediate devices, improving system resilience in critical infrastructure against communication failures [25,26]. In [27], the authors propose an adaptive routing protocol to control energy usage in end-user devices. It utilizes a link quality prediction method to cluster network objects and route data based on the movement of these objects. The protocol introduced the NHARSO algorithm [28] to determine optimal paths between cluster heads and base stations in IoT-enabled Wireless Sensor Networks (IWSNs), addressing issues related to sensing, residual energy, and communication. The selection of optimal cluster heads not only increases the network lifetime but also efficiently utilizes the energy consumption of the devices.

In [29], authors have proposed an energy-efficient multilevel secure routing (EEMSR) protocol, which aims to cluster the network for efficient resource management and energy efficiency. It also decreases the overhead on the devices and supports the communication system with a prolonged network lifetime. Moreover, multiple factors are explored for trust, including data perception, fusion, and communication

trust, to provide security and protect the system against threats. An Artificial Intelligence-based Energy-aware Intrusion Detection and Secure Routing model is proposed in [30] for Industrial Wireless Sensor Networks. Its aim is to establish a secure IoT network with minimal additional energy consumption in the network structure. In addition, the proposed model integrates intrusion detection with a game strategy-based decision mechanism to provide an energy-aware ad hoc on-demand distance vector algorithm with authentic and reliable routing.

Authors in [31] integrate software-defined networking (SDN) and blockchain technology to address the challenges of energy efficiency and security research. Consequently, a novel energy protocol combined with a cluster structure was proposed to develop a secure and blockchain-enabled SDN controller architecture for IoT networks. Because it uses public and private blockchains for peer-to-peer (P2P) communication between IoT devices and SDN controllers, eliminating Proof-of-Work, the distributed trust architecture is suitable for resource-constrained IoT devices. The study [32] introduces a modified AntHocNet in the FANET routing protocol, aiming to provide optimal data forwarders for route establishment using ant colony optimization (ACO). The data forwarders are rotated to maintain the constructed paths and enhance the system's efficacy. The result analysis significantly enhanced the energy efficiency of the network, resulting in a long-run stable period. Table 1 outlines the existing research challenges in most related work, along with the inclusion of major functionalities of the proposed framework.

Table 1: Key limitations in existing solutions and corresponding improvements in the proposed framework

Problem in existing solutions	Proposed framework solution
Limited trust and security mechanisms, leading to unreliable communication	Introduces a trust-aware mechanism that ensures only reliable nodes participate, enhancing authenticity and security
High latency in traffic management decisions	AI-enabled edge computing performs local processing and intelligent decision-making, reducing response time
Single-factor decision-making ignores multiple performance metrics	Employs multi-factor decision-making that considers latency, trust, reliability, and resource efficiency for robust operation
Poor adaptability to dynamic IoT and CPS environments	Adaptive control mechanisms adjust to changing network conditions, device mobility, and workload variations
Resource constraints of IoT and edge devices are not efficiently handled	Optimizes computational and energy resources at the edge while maintaining high performance and trust levels

3 Materials and Methods

In this section, we present the details of our proposed framework along with its algorithms.

3.1 Overview

Graph initialization, communication optimization, and trust integration are the three main phases of the proposed framework, as depicted in Fig. 1. Such an environment consists of IoT sensors that sense objects and send the collected data to the edges for local processing. The integration of intelligence is another key feature of the proposed framework, supported by a trust-driven approach. It not only identifies malicious devices but also enhances security for T-CPS through mutual authentication. The proposed framework assumes the following assumptions for realistic Cyber-Physical IoT Systems.

- Network devices in T-CPS are resource-constrained in terms of energy, transmission power, and memory, requiring efficient communication mechanisms.
- CPS-IoT environments are dynamic and may experience unreliable connectivity, mobility, and varying communication reliability.
- Edge devices possess sufficient computational resources for distributed processing and task offloading from constrained nodes.
- Source and destination devices are initially trusted, while intermediate nodes may be malicious; hence, trust-based mechanisms are employed for secure communication.

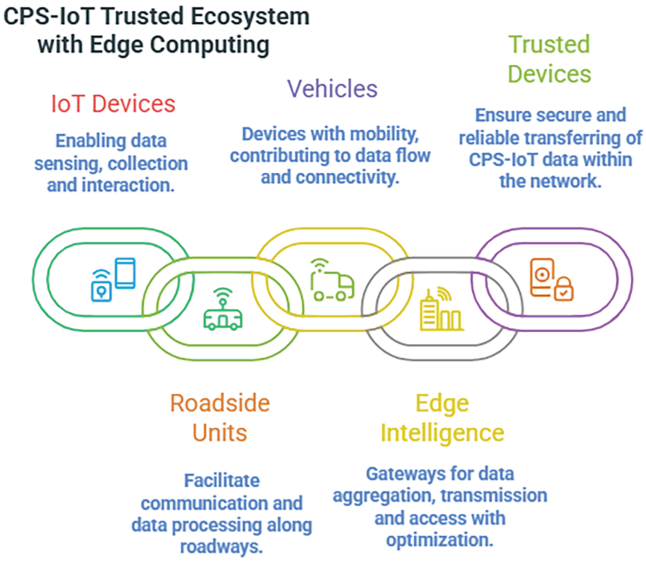

Figure 1: T-CPS enabled communication architecture for IoT-based Trusted systems

3.2 Discussion

Initially, a connected graph G is formed using nodes V and edges E. Edges denote the communication links. In the proposed framework, we explore the Artificial Bee Colony [33] based optimization to cope with the transmission of transportation data among vehicles. Moreover, edges are not selected based on cost and are randomly selected to construct initial routes for disseminating data in the Transportation Cyber-Physical System (T-CPS). Such a mechanism manages the traffic load in a balanced order and reduces device congestion. Node i computes its weight we using cost c, reliability r, and trust tr factors as given in Eq. (1).

$$we(i) = c(i) + w_1.r(i) + w_2.T(i) \tag{1}$$

where $c(i)$ depends on the bandwidth bn and latency li metrics, its computation is defined in Eq. (2).

$$c(i) = \frac{\lambda \cdot b_n(i) \cdot l(i)}{l(i)} + \frac{\mu \cdot l_{\text{thres}}}{l(i)} \tag{2}$$

where l_{thres} shows the maximum level of latency over the communication channel from vehicle i to j. The reliability of the channel between node i and j represents the stability of communication, and it must be higher to attain high-performance T-CPS communication, as shown in Eq. (3).

$$r(i) = w_1 \cdot \left(\frac{P_T}{B + \alpha}\right) + w_2 \cdot \left(\frac{T_R}{B_w + \beta}\right) \tag{3}$$

where P_T is signal strength, B denotes probability of Bit Error Rate (BER), T_R denotes transmission rate, B_w is bandwidth, α, and β are adjusting factors. In the proposed framework, the bees act as agents and explore the nearby nodes $\{i, i+1, \ldots, n\}$ along with their associated edges to compute the effectiveness and quality of various routing paths by examining the weighted value $we(i)$. Accordingly, the proposed framework ensures load balancing by selecting the edges with the lowest weights while considering randomness in their routing decisions. Later, we introduced the multi-factor-enabled trust computation in dual stages. In the first stage, node-to-node trust is established to achieve the maximum success rate. Subsequently, border-to-edge trust is established to ensure consistent communication with the edges. In the proposed framework, the packet drop ratio Pdr, latency L, and node reliability R_n are the three primary parameters of trust that aim to achieve a more reliable transmission paradigm in T-CPS. The trust value based on Pdr for node i to j is defined in Eq. (4).

$$T_{Pdr}(i,j) = \frac{P_{sent}(i,j)}{P_{del}(i,j)} \tag{4}$$

Eq. (5) defines the latency metric to compute the communication delay in vehicles and enhances the trust level in a crucial environment with rapid response.

$$T_L(i,j) = 1 - \frac{L(i,j)}{Thres_L} \tag{5}$$

$Thres_L$ shows the threshold limit and latency among vehicle i and j is denoted by $L(i,j)$.

Eq. (6) computes the node reliability based on the behavior and consistency of vehicles. In such a case, the trust in vehicle i increases when reliability improves. The reliability trust component is defined as $T_{N_r}(i) = \frac{N_r(i)}{N_{r_{max}}}$, where $N_r(i)$ represents the device's reliability level. The cumulative weighted trust score $T_r(i,j)$ is determined as a balanced linear combination of packet delivery rate (Pdr), latency (L), and node reliability (N_r), that are weighted by empirically derived factors w_1, w_2, w_3.

$$T_r(i,j) = w_1\, T_{Pdr}(i,j) + w_2\, T_L(i,j) + w_3\, T_{N_r}(i) \tag{6}$$

where:

- $T_r(i,j)$: Overall weighted trust score between nodes i and j
- $T_{Pdr}(i,j)$: Trust component based on packet delivery rate
- $T_L(i,j)$: Trust component derived from latency performance
- $T_{N_r}(i)$: Node reliability trust component
- w_1, w_2, w_3: Weighting coefficients satisfying $w_1 + w_2 + w_3 = 1$

Eq. (7) defines the edge selection process by integrating a trust evaluation mechanism.

$$TS(b_i, e_d) = (\alpha \cdot T(b_i) + \beta \cdot T(e_d)) \cdot (1 - \delta \cdot t) \tag{7}$$

$T(b_i)$ and $T(e_d)$ denote the trust levels of the border device and edge node, respectively. The time-based trust decay factor, $(1 - \delta \cdot t)$, where δ is heuristically tuned, is used to compute a cumulative trust score by aggregating historical trust observations using Eq. (8).

$$CTS(b_i, e_d) = \frac{\sum_{k=1}^{n} \omega_k \cdot TS_k(b_i, e_d)}{\sum_{k=1}^{n} \omega_k} \tag{8}$$

where ω_k is the weight assigned to the k-th observation, emphasizing recent trust evaluations while maintaining historical awareness. For fair comparison between heterogeneous devices, trust values are normalized to a bounded index, as given in Eq. (9).

$$NTI(b_i) = \frac{T(b_i) - T_{\min}}{T_{\max} - T_{\min}} \tag{9}$$

where:

- $T(b_i)$: Computed trust value of the border device
- $T_{\min}$, $T_{\max}$: Minimum and maximum trust levels observed in the network
- $NTI(b_i)$: Normalized trust index used for ranking devices during edge selection

Fig. 2 shows the working flow of the proposed framework using IoT architecture for the T-CPS environment. It evaluates real-time capture data and generates an optimal decision-making system using the Artificial Bee Colony algorithm. Weighted methods are explored to incorporate multiple parameters, such as communication cost, link dependability, and trust, allowing agents to select the most reliable forwarders with the highest reliability and trust levels. Such decisions are less likely to be erroneous. Thus, our proposed framework optimizes and controls IoT traffic while ensuring efficient resource management and secure computations across associated devices. The generated decision is also adaptively updated based on traffic and network conditions. To achieve secure, more authentic IoT-based communication, the proposed trustworthy techniques are depicted in Fig. 3. In the proposed framework, the trust score plays a crucial role in promptly identifying malicious devices. The deployed edges are treated as agents and select communication routes with higher trusted scores, thereby introducing a more stable T-CPS communication system that efficiently utilizes network resources. If any lower-rated devices are selected as forwarders, they are marked as invalid for further data transmission. All devices are assigned a trust score based on their behavior, which changes dynamically over time. Moreover, the lightweight security methods make it able to attain the integrity and less congested the bounded constraint devices. Our layer-based trust management offers more reliable and resilient communication channels over the CPS environment.

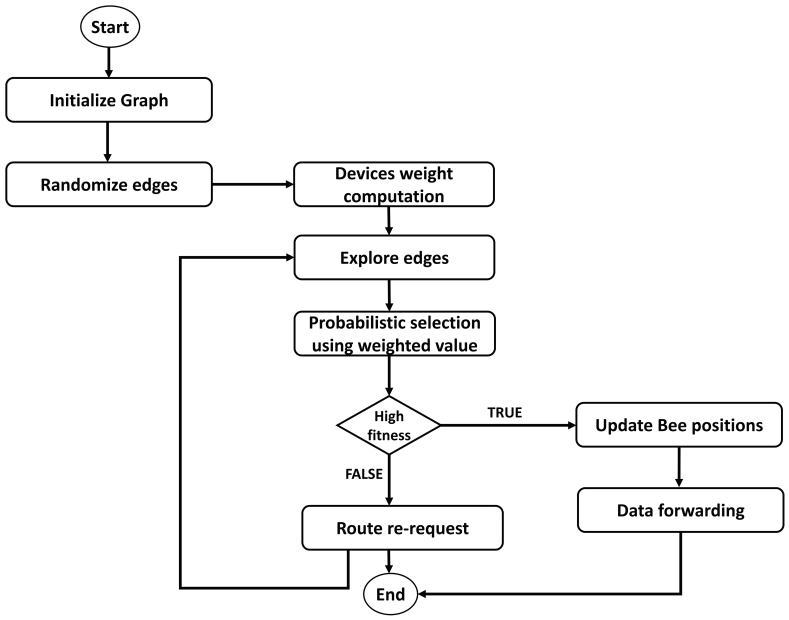

Figure 2: Flowchart for real-time data dissemination using network edges in CPS system

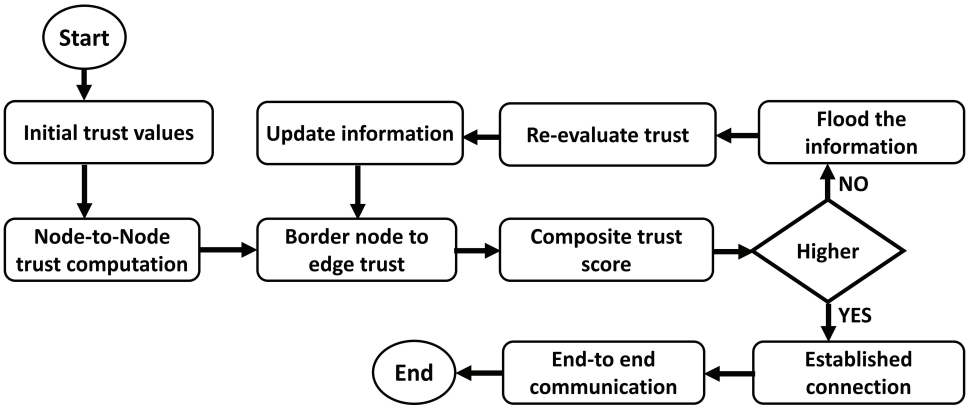

Figure 3: Flowchart for trust-aware communication and adaptive routing in T-CPS

Algorithm 1 illustrates the developed procedures for optimized decision-making, trust computation, and route maintenance using edge-level processing.

Algorithm 1: Graph initialization, trust calculation, and route exploration

Input: Graph *G (V, E)*, nodes *V*, edges *E*, historical trust scores *H (i)*, performance metrics *P (i)*, time factor *t*

Output: Updated trust scores and optimal routes

for *each node* $i \in V$ **do**
  Compute weight: $we(i) = c(i) + r(i) + T(i)$;
  Update trust: $T(i) = T(i) \cdot (1 - \delta \cdot t)$;
  for *each edge (i, j) in G(V, E)* **do**
    Compute edge trust:
    $T(i,j) = T(i,j) + \lambda \cdot \frac{P(i,j)}{T(i)+T(j)}$
    Apply time decay:
    $T(i,j) = T(i,j) \cdot (1 - \delta \cdot t)$
    if $T(i,j) < threshold$ **then**
      Reduce selection probability for low trust edges;
    end
  end
end
While *Unexplored routes* **do**
  Randomly select new routes;
  Recompute trust and evaluate performance;
  if *Trust meets criteria* **then**
    Store route as optimal;
  end
  else
    Reject the route;
  end
end
return updated trust scores and optimal routes;

Table 2 describes the proposed security methods while addressing potential attacks in IoT networks to guarantee a reliable T-CPS environment with trustworthiness.

Table 2: Security analysis and mitigation strategies

Potential risk	Proposed mitigation
Malicious nodes	Detected via continuous trust updates $T(v_i)$; Artificial Bee Colony algorithm ensures routing through nodes with $T(v_i) \geq \theta$.
Denial of Service (DoS)	Traffic re-routed through high-trust paths; Artificial Bee Colony optimization minimizes attack impact.
Data manipulation	End-to-end encryption ensure confidentiality; secure routing reduces tampering.
Replay attacks	Session keys K_{session} and timestamps prevent reuse of intercepted messages.
Key management	Periodic key rotation K_{key} and Artificial Bee Colony-based routing restrict exposure.
Edge-cloud security	Secure key rotation K_{rot} and trusted Artificial Bee Colony paths limit breach risks.
Blockchain limitations	Device authentication Auth(v_i) preserves confidentiality $D_{\text{confidential}}$.
Access control	Strict A_{control} and Audit(v_i) ensure accountability and prevent unauthorized access.

4 Simulation Description

This section presents the performance evaluation of the proposed framework with related studies in terms of varying sensors and transmission data. The deployed environment consists of sensors, edge nodes, and sink nodes, all of which are connected to the cloud system. Simulation parameters with their default values are declared in Table 3.

Table 3: Simulation parameters

Parameter	Value
Nodes placement	Random
Simulation area	5000 m × 5000 m
Transmission speed	100–500 packets/sec (step = 100)
Traffic model	Constant Bit Rate (CBR)
Number of sensors	400 to 2000 (step = 400)
Number of edge devices	20
Mobile malicious devices	10 to 30 (step = 5)
Initial energy	5 J
Simulations	60
Propagation loss model	Two-ray Ground
Mobility model	Random Waypoint
Weighted factors	w_1, w_2, w_3
Evaluation Scenarios	Varying number of sensors and varying transmissions
Performance metrics	Packet loss ratio, network throughput, security risk, and trust level

We compared the performance of the packet drop ratio of the proposed framework with existing approaches, as depicted in Figs. 4 and 5. The proposed framework reduced the packet drop ratio by an average of 32% and 37% under varying numbers of sensors and transmission data. This is due to integrating the Artificial Bee Colony algorithm, which is used to select more reliable communication links and efficiently manage network resources. Moreover, the proposed framework provides stable paths by computing link interference parameters, thereby enhancing data reception and reducing the probability of network congestion. The proposed trusted mechanisms mitigated malicious traffic and prevented false requests from devices, thus improving the overall management of transportation traffic and stabilizing the real-time environment of CPS.

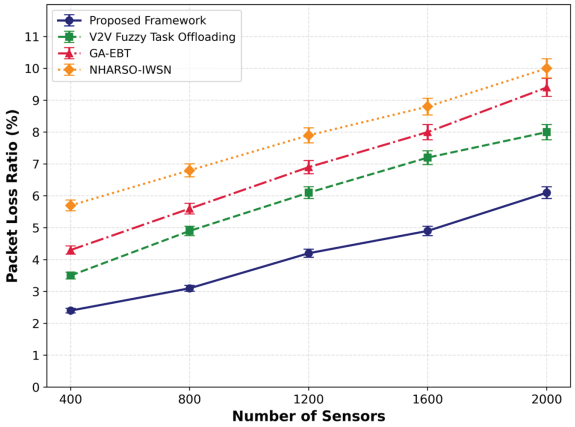

Figure 4: Performance of proposed framework with V2V fuzzy task offloading, GA-EBT, and NHARSO-IWSN for packet loss rate under varying number of sensors

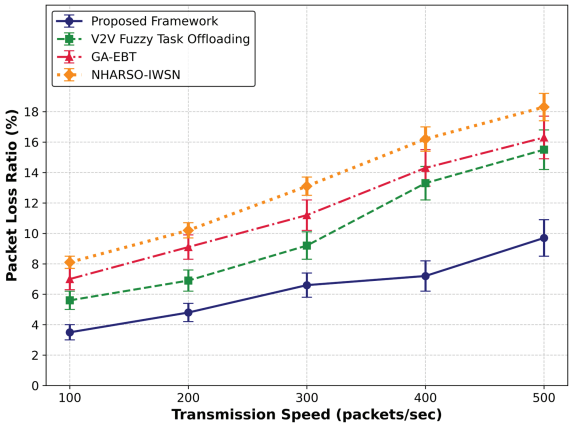

Figure 5: Performance of proposed framework with V2V fuzzy task offloading, GA-EBT, and NHARSO-IWSN for packet loss rate under varying transmissions

The network throughput of the proposed framework is evaluated against existing approaches, as shown in Figs. 6 and 7. The experimental results indicate that our framework improves average network throughput by 40% and 45% under varying numbers of sensors and data transmission scenarios, respectively. The initial route selection leverages a weighted objective function that incorporates device history, performance metrics, and decayed trust values, thus providing uniform contribution for each parameter. It also reduces the load on the selected forwarders through balancing strategies. In addition, the dual-level trust enables T-CPS not to send sensor data for further processing via wireless links that are compromised or inauthentic.

The security risk performance of the proposed framework, compared with existing approaches, is illustrated in Figs. 8 and 9 under varying sensors and transmission data. Upon comparison, it was discovered that the proposed framework effectively improved the protection of T-CPS against threats by an average of 34% and 39%, respectively, by identifying malicious devices and routing traffic only over the more trusted links. This is due to the combination of multiple parameters that enable secure data forwarders to maintain a reliable history in terms of data computation and association with neighboring nodes. The edges continuously monitor the border nodes, and if any malicious activity is detected based on communication behavior, the edges mark the transmission as compromised and record the information in log files. Furthermore, the resilient and incoming transportation data is verified using historical information, which is later sent to the cloud system. The proposed framework offers lightweight computing and minimizes unnecessary resource consumption by imposing a minimal overhead on transportation devices.

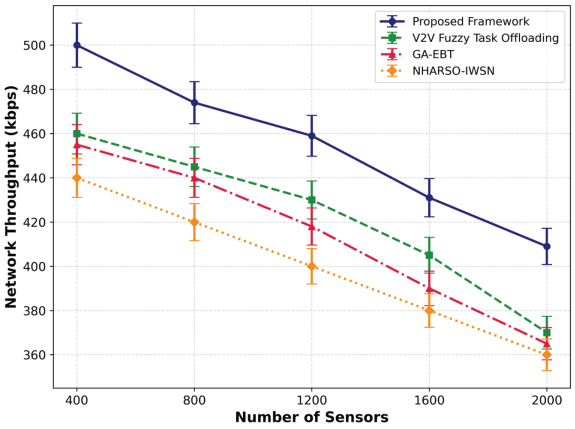

Figure 6: Performance of proposed framework with V2V fuzzy task offloading and GA-EBT for network throughput under varying number of sensors

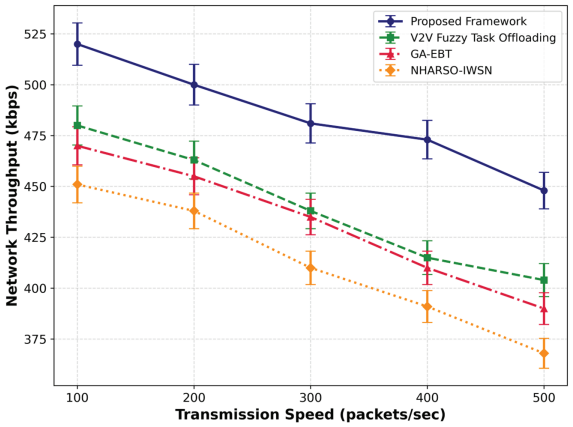

Figure 7: Performance of proposed framework with V2V fuzzy task offloading, GA-EBT, and NHARSO-IWSN for network throughput under varying transmissions

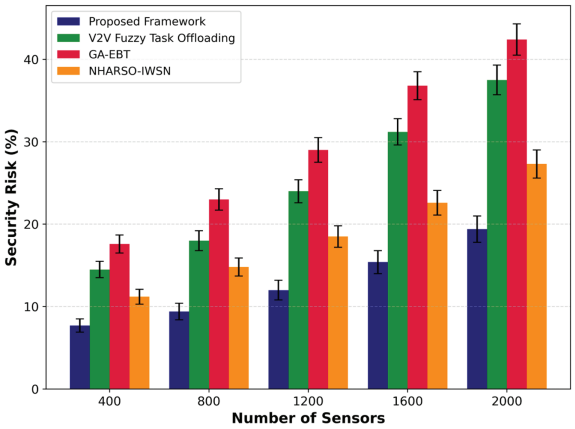

Figure 8: Performance of proposed framework with V2V fuzzy task offloading, GA-EBT, and NHARSO-IWSN for security risk under varying number of sensors

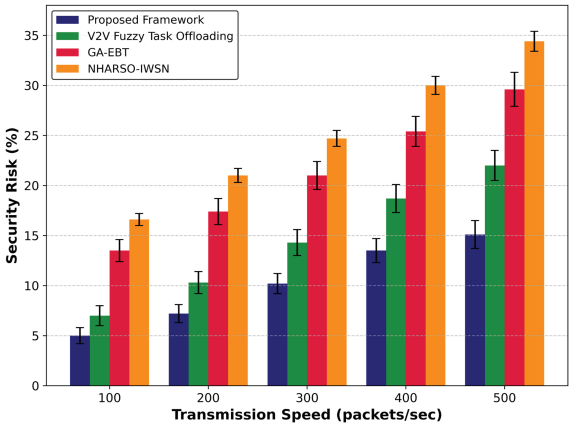

Figure 9: Performance of proposed framework with V2V fuzzy task offloading, GA-EBT, and NHARSO-IWSN for security risk under varying transmissions

In Figs. 10 and 11, the performance of the proposed framework and existing approaches is compared to evaluate trust levels under varying sensor and transmission data. Based on the results analysis, it was found that the proposed framework improved the performance by an average of 43% and 48% for prediction trust levels. By leveraging intelligence in decision-making, the proposed framework reduces device overhead and actively identifies threats through a multi-level trusted mechanism. Moreover, the Artificial Bee Colony algorithm provides more reliable, long-term communication paths for data routing, avoiding communication holes while accounting for multiple factors and environmental conditions.

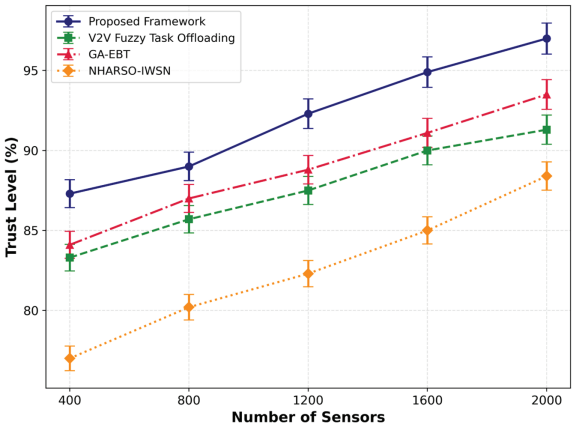

Figure 10: Performance of proposed framework with V2V fuzzy task offloading, GA-EBT, and NHARSO-IWSN for trust level under varying number of sensors

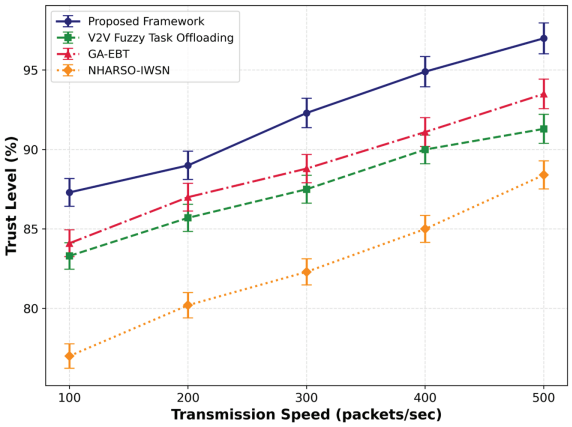

Figure 11: Performance of proposed framework with V2V fuzzy task offloading, GA-EBT, and NHARSO-IWSN for trust level varying transmissionss

5 Conclusion

In recent decades, emerging technologies with IoT systems have enabled real-time data processing and management for the formulation of smart cities. On the other hand, edge computing provides local processing and enables real-time traffic analysis for transportation networks. However, some solutions still lack intelligent decision-making, leading to additional energy consumption in the communication system. Moreover, threat analysis is another crucial component that is often overlooked in most existing approaches. Our proposed framework optimizes the decision-making strategies using the Artificial Bee Colony algorithm and integrates the multi-level trust detection against threats. Additionally, the distributed computing in the proposed framework reduces communication gaps through its load-balancing approach, thereby enhancing the vehicles' efficacy. However, based on the results, it was noted that our proposed framework lacks scalability as the vehicle increases in size, resulting in additional computational cost. Thus, in future work, we plan to introduce SDN controllers to enhance flexibility and minimize the connection disturbance in heterogeneous CPS-IoT systems.

Acknowledgement: The authors would like to acknowledge the support by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-DDRSP2504).

Funding Statement: This work was supported and funded by the Deanship of Scientific Research at Imam Mohammad Ibn Saud Islamic University (IMSIU) (grant number IMSIU-DDRSP2504).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Khalid Haseeb, Imran Qureshi; data collection: Naveed Abbas, Muhammad Ali, Muhammad Arif Shah; analysis and interpretation of results: Muhammad Ali, Muhammad Arif Shah, Qaisar Abbas; draft manuscript preparation: Khalid Haseeb, Imran Qureshi, Naveed Abass. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All data generated or analyzed during this study are included in this published article.

Ethics Approval: Not applicable.

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

References

1. Abkenar FS, Ramezani P, Iranmanesh S, Murali S, Chulerttiyawong D, Wan X, et al. A survey on mobility of edge computing networks in IoT: state-of-the-art, architectures, and challenges. IEEE Commun Survs Tutor. 2022;24(4):2329–65.
2. Andriulo FC, Fiore M, Mongiello M, Traversa E, Zizzo V. Edge computing and cloud computing for internet of things: a review. Informatics. 2024;11:71.
3. Ahmed SF, Alam MSB, Hoque M, Lameesa A, Afrin S, Farah T, et al. Industrial Internet of Things enabled technologies, challenges, and future directions. Comput Electr Eng. 2023;110:108847. doi:10.1016/j.compeleceng.2023.108847.
4. 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.
5. Ullah I, Noor A, Nazir S, Ali F, Ghadi YY, Aslam N. Protecting IoT devices from security attacks using effective decision-making strategy of appropriate features. J Supercomput. 2024;80(5):5870–99. doi:10.1007/s11227-023-05685-3.
6. Kato T, Fukumoto N, Sasaki C, Tagami A, Nakao A. Challenges of CPS/IoT network architecture in 6G era. IEEE Access. 2024;12(1):62804–17. doi:10.1109/access.2024.3395363.
7. Mei Q, Xiong H, Chen YC, Chen CM. Blockchain-enabled privacy-preserving authentication mechanism for transportation CPS with cloud-edge computing. IEEE Trans Eng Manag. 2022;71(37):12463–74. doi:10.1109/tem.2022.3159311.
8. Bhansali A, Patra RK, Divakarachari PB, Falkowski-Gilski P, Shivakanth G, Patil SN. CNN-CLFFA: support mobile edge computing in transportation cyber physical system. IEEE Access. 2024;12:21026–37. doi:10.1109/access.2024.3361837.
9. Mohammed A. Cybersecurity in Smart Cities: as cities become smarter, new vulnerabilities arise. Research can focus on securing IoT devices, smart infrastructure, and privacy concerns associated with smart city data. Pioneer Res J Comput Sci. 2024;1(1):75–82. doi:10.4018/979-8-3373-3326-7.ch003.
10. Escolar AM, Wang Q, Calero JMA. Enhancing honeynet-based protection with network slicing for massive Pre-6G IoT Smart Cities deployments. J Netw Comput Appl. 2024;229(8):103918. doi:10.1016/j.jnca.2024.103918.
11. Trigka M, Dritsas E. Edge and cloud computing in smart cities. Future Internet. 2025;17(3):118. doi:10.3390/fi17030118.
12. Babar M, Khan MS, Din A, Ali F, Habib U, Kwak KS. Intelligent computation offloading for IoT applications in scalable edge computing using artificial bee colony optimization. Complexity. 2021;2021(1):5563531. doi:10.1155/2021/5563531.
13. Reddy KHK, Luhach AK, Kumar VV, Pratihar S, Kumar D, Roy DS. Towards energy efficient Smart city services: a software defined resource management scheme for data centers. Sustain Comput Inform Syst. 2022;35(2):100776. doi:10.1016/j.suscom.2022.100776.
14. Sun Z, Yang H, Li C, Yao Q, Teng Y, Zhang J, et al. A resource allocation scheme for edge computing network in smart city based on attention mechanism. ACM Trans Sens Netw. 2024;4(2):22. doi:10.1145/3650031.
15. Alzaabi FR, Mehmood A. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access. 2024;12:30907–27. doi:10.1109/access.2024.3519957.
16. Siwakoti YR, Bhurtel M, Rawat DB, Oest A, Johnson R. Advances in IoT security: vulnerabilities, enabled criminal services, attacks, and countermeasures. IEEE Internet Things J. 2023;10(13):11224–39. doi:10.1109/jiot.2023.3252594.
17. Chunduri V, Alsaadi M, Gupta S, Ahanger TA, Gopi A, Alghayadh FY, et al. Blockchain-based secure trust management scheme for internet of vehicles over cyber-physical system. IEEE Trans Intell Transp Syst. 2024;26(9):14067–76. doi:10.1109/tits.2024.3485481.
18. Rehman A, Haseeb K, Alruwaili FF, Ara A, Saba T. Autonomous and intelligent mobile multimedia cyber-physical system with secured heterogeneous IoT network. Mobile Netw Appl. 2024;29(3):876–85. doi:10.1007/s11036-024-02329-5.

19. Ozaif M, Mustajab S, Alam M. Exploration of secured data transmission in internet of things: a survey. In: 2024 IEEE international conference on computing, power and communication technologies (IC2PCT); 2024 Feb 9–10; Greater Noida, India. p. 106–12. doi:10.1109/ic2pct60090.2024.10486716.
20. Jha AV, Appasani B, Khan MS, Zeadally S, Katib I. 6G for intelligent transportation systems: standards, technologies, and challenges. Telecommun Syst. 2024;86(2):241–68. doi:10.1007/s11235-024-01126-5.
21. Ryalat M, ElMoaqet H, AlFaouri M. Design of a smart factory based on cyber-physical systems and Internet of Things towards Industry 4.0. Appl Sci. 2023;13(4):2156. doi:10.3390/app13042156.
22. Zhang K, Shi Y, Karnouskos S, Sauter T, Fang H, Colombo AW. Advancements in industrial cyber-physical systems: an overview and perspectives. IEEE Trans Ind Inform. 2022;19(1):716–29. doi:10.1109/tii.2022.3199481.
23. Rodrigues TK, Suto K, Nishiyama H, Liu J, Kato N. Machine learning meets computation and communication control in evolving edge and cloud: challenges and future perspective. IEEE Commun Surv Tutor. 2019;22(1):38–67.
24. Firouzi F, Jiang S, Chakrabarty K, Farahani B, Daneshmand M, Song J, et al. Fusion of IoT, AI, edge-fog–cloud, and blockchain: challenges, solutions, and a case study in healthcare and medicine. IEEE Internet Things J. 2022;10(5):3686–705. doi:10.36227/techrxiv.20369043.v1.
25. Luo Q, Hu S, Li C, Li G, Shi W. Resource scheduling in edge computing: a survey. IEEE Commun Surv Tutor. 2021;23(4):2131–65.
26. Avan A, Azim A, Mahmoud QH. A state-of-the-art review of task scheduling for edge computing: a delay-sensitive application perspective. Electronics. 2023;12(12):2599. doi:10.3390/electronics12122599.
27. Foko Sindjoung ML, Velempini M, Kengne Tchendji V. ARPMEC: an adaptive mobile edge computing-based routing protocol for IoT networks. Cluster Comput. 2024;27(7):9435–50. doi:10.1007/s10586-024-04450-2.
28. Sharma P, Sharma M, Singh R, Kumar V, Agarwal R, Malik PK. NHARSO-IWSN: a Novel hybridized adaptive-network-based fuzzy inference system with reptile search optimization algorithm-based routing protocol for internet of things-enabled wireless sensor networks. IEEE Trans Consumer Electron. 2024;70(3):6293–302. doi:10.1109/tce.2024.3418845.
29. Zhang Y, Ren Q, Song K, Liu Y, Zhang T, Qian Y. An energy-efficient multilevel secure routing protocol in IoT networks. IEEE Internet Things J. 2021;9(13):10539–53. doi:10.1109/jiot.2021.3121529.
30. Aruchamy P, Gnanaselvi S, Sowndarya D, Naveenkumar P. An artificial intelligence approach for energy-aware intrusion detection and secure routing in internet of things-enabled wireless sensor networks. Concurr Comput. 2023;35(23):e7818. doi:10.1002/cpe.7818.
31. Yazdinejad A, Parizi RM, Dehghantanha A, Zhang Q, Choo KKR. An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. IEEE Trans Services Comput. 2020;13(4):625–38. doi:10.1109/tsc.2020.2966970.
32. Khan IU, Qureshi IM, Aziz MA, Cheema TA, Shah SBH. Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET). IEEE Access. 2020;8:56371–8. doi:10.1109/access.2020.2981531.
33. Kaya E, Gorkemli B, Akay B, Karaboga D. A review on the studies employing artificial bee colony algorithm to solve combinatorial optimization problems. Eng Appl Artif Intell. 2022;115(3):105311. doi:10.1016/j.engappai.2022.105311.