Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.073832

ARTICLE

Blockchain-Enabled AI Recommendation Systems Using IoT-Asisted Trusted 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, 72341, 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, SW15 5PU, UK

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

Received: 26 September 2025; Accepted: 11 December 2025; Published: 12 March 2026

ABSTRACT: The Internet of Things (IoT) and cloud computing have significantly contributed to the development of smart cities, enabling real-time monitoring, intelligent decision-making, and efficient resource management. These systems, particularly in IoT networks, rely on numerous interconnected devices that handle time-sensitive data for critical applications. In related approaches, trusted communication and reliable device interaction have been overlooked, thereby lowering security when sharing sensitive IoT data. Moreover, it incurs additional energy consumption and overhead while addressing potential threats in the dynamic environment. In this research, an Artificial Intelligence (AI) recommended fault-tolerant framework is proposed that leverages blockchain technology, aiming to enhance device trustworthiness and ensure data privacy. In addition, the intelligence of the proposed framework enables more authentic and authorized device involvement in data routing, thereby enabling seamless transmission in smart cities integrated with lightweight computing. To evaluate dynamic network conditions, the proposed framework offers a timely decision-making system to ensure robust delivery of IoT-assisted services. Using simulations, the efficacy of the proposed framework is validated by comparing it with existing approaches across various network metrics, demonstrating remarkable performance while achieving energy efficiency and optimizing network resources.

KEYWORDS: Artificial intelligence; blockchain; data security; IoT; recommendation systems

1 Introduction

IoT has introduced a significant innovation paradigm for communication among smart devices and interaction with physical environments [1,2]. In smart cities, the quality of service is directly impacted by constrained resources and computing limitations of Wireless Sensor Network (WSN) [3–5]. Sensing technologies enable the observation and collection of data from dynamic, inconsistent environments. Unlike traditional networks, intelligent systems require load-balancing and consistent forwarding paths to retain reliable data transfer in critical and unpredictable environments [6,7]. In recent decades, real-time applications have integrated artificial intelligence and IoT systems to aggregate and process data from external sources, thereby enhancing the prediction and responsiveness of heterogeneous services [8,9]. The deployed devices at lower layers sense the communication infrastructure and analyze the desired parameters for the monitoring of network communication [10,11]. These systems require a significant contribution to establish trust in relaying services and offer the most robust multi-paths to enhance system performance

in terms of resource management [12,13]. On the other hand, edge computing is also used in many innovative applications to process requested data at the edge, rather than by devices or local servers [14,15]. However, many approaches have been proposed that combine edge computing with reduced computing power on constrained devices. Nonetheless, it remains a challenging research issue for effective load distribution in mobile networks, particularly in coping with energy holes near the proximity of edges [16,17]. Furthermore, as smart devices interact with cloud systems via intermediate, insecure relay nodes, ensuring secure management of data confidentiality and integrity is another significant research challenge for IoT systems [18–20]. It has been observed that most existing approaches still suffer from suboptimal, untrusted data forwarding decisions, leading to additional energy consumption due to malicious devices. Moreover, limited approaches have been proposed using an AI-integrated blockchain solution to ensure a dynamic, authentic, and verifiable routing recommendation engine. To address these research challenges, our research proposed a framework that explores artificial intelligence strategies for managing industrial IoT networks and optimization algorithms to identify load-balanced, energy-efficient data forwarders with distributed decision-making criteria. Furthermore, a cooperative edge technique is designed to achieve security and trustworthiness. The main contributions of our proposed framework are outlined below.

i. It proposes an AI-driven framework for adaptive trust management in IoT networks, enhancing system reliability by dynamically assessing device trustworthiness and ensuring consistent performance.
ii. A routing recommendation engine is integrated to process the devices' requests and analyze timely network conditions with more effective data forwarding decisions in IoT environments.
iii. To secure data transmission and achieve privacy in the innovative system, a blockchain and trust computation are utilized to mitigate communication risks.

The remaining sections are structured as follows: Section 2 explains Related work. Section 3 discusses the proposed methodology along with its development components. The simulation environment and performance results are discussed in Section 4. Finally, Section 5 concluded this work.

2 Related Work

Smart cities provide seamless connectivity among IoT devices and act as a backbone for the interconnection of physical objects and real-time applications [21,22]. These systems are developed for continuous data collection in harsh environments and reduce human effort in managing and controlling unpredictable circumstances [23,24]. Such a dynamic network enhances the functionality of constrained resources by more efficiently utilizing network infrastructure, enabling sustainable development and autonomous decision-making models [25,26]. Edge computing, in collaboration with wireless technologies, enables timely data processing at affordable computational cost for constrained applications, thereby improving system responsiveness under dynamic network conditions [27,28]. The study [29] proposes a Graph-Based Trust-Enabled Routing (GBTR) scheme for vehicular networks, aiming to provide trustworthy communication for devices by computing direct, indirect, and contextual trust. Communication success, delay, and mobility factors are explored for the direct trust, while device feedback and link reliability are used to compute the indirect trust. Factors such as location, time, weather, and traffic conditions are used to determine contextual trust. Using the proposed scheme, the routes are more reliable, less congested, and strengthen the communication system with the integration of rewards and penalties on trust computation. Authors of [30] proposed a lightweight blockchain-based authentication mechanism for IoT network, aims to improve the energy consumption while storing only a few credentials of devices. It introduced on-demand routing by optimizing energy usage through a genetic algorithm-based Software Defined Networking (SDN) controller. With robust threats detection mechanism, malicious devices are identified and maintain a blacklist on the blockchain. The study [31] proposed a Lightweight Secure Routing (LSR) algorithm by introducing a multiobjective

WSN optimization. It enhances the security and connectivity for devices in Wireless Sensor Network by integrating Ant Colony Optimization (ACO), adaptive trust, QoS and adaptive connectivity models. The performance results significantly improve resource optimization without additional energy depletion in the network. Authors of [32] propose a secure routing protocol for IoT-enabled healthcare by combining a fuzzy logic system and the Whale Optimization Algorithm (WOA). The approach consists of a fuzzy trust strategy to evaluate device trustworthiness and a WOA-based clustering framework to select optimal cluster heads based on centrality, communication range, hop count, energy, and trust. The method enhances the efficiency and security of IoT networks. Authors of [33] propose the Attribute Trust-based Security (ATST) algorithm to preserve data privacy and grant access control for sensitive information. To develop a trust measurement model and an authentic access control structure, ATST used user attributes. Moreover, encryption techniques are explored to secure data transfer, and a dual-trust model is proposed to mitigate malicious threats and enhance network reliability. Using an authentic scheme, authorized devices can join the network and access encrypted data using secret information. In [34], the authors propose a three-layered IoT security architecture integrated with AI and blockchain for real-time threat mitigation. The architecture includes a novel legitimacy score assessment and an Ethereum-based data repositioning framework to enhance privacy. A simplified consensus module generates a conclusive evidence matrix, and an AI-based security optimization, enhanced by metaheuristic algorithms, ensures faster and more efficient security measures. Table 1 highlights the significant contributions and limitations of the existing approaches.

3 Proposed Methodology

This section discusses the phases and components of the proposed framework. The system model comprises sensors, sink nodes, and edges that gather environmental data and forward it to processing servers to fulfill device requests. Sensors are homogeneous and static, while the sink node is mobile. They are rotated with a predefined speed. Each node uses its transmission power to create local files that store initial parameters and routing path information, and all tables are continuously updated to optimize forwarding in the IoT network. The local information is recorded in the tables to identify the observing neighbors. We modeled the network as a directed graph and explored a traversal mechanism to identify all possible routes from source to sink. The records of all routes are stored in routing tables and are frequently updated whenever a suitable candidate is found to forward network traffic. The first phase is an AI-based routing recommendation system that predicts efficient routing paths by optimizing network resources. It also ensures quality-aware communication and imposes nominal computational overheads on IoT devices. On the other hand, blockchain is integrated into the proposed framework to ensure data integrity and maintain the authenticity of associated devices, thereby enhancing the trustworthiness of the innovative IoT network. It lessens the malicious threats and prevents unauthorized access while exploring an AI-recommended system for reliable routing decisions and communication stability. In Fig. 1, the proposed layers for an AI recommendation system and for blockchain-based data security with effective decision-making are illustrated. It reduces response time for critical systems and enhances lightweight security measures against potential attacks by enabling intelligent edge processing. In Fig. 2, the main stages of the proposed framework, along with their interaction, are illustrated. The IoT devices are interconnected, and their trust values are computed. If they are more trusted than the selected devices, they can participate in the routing decision. The forwarders are selected based on cost, and if the cost exceeds a certain threshold, the routes are reformulated and their records are maintained in the routing table. Moreover, trusts are updated in response to specific events and network conditions to enhance data reliability and network robustness.

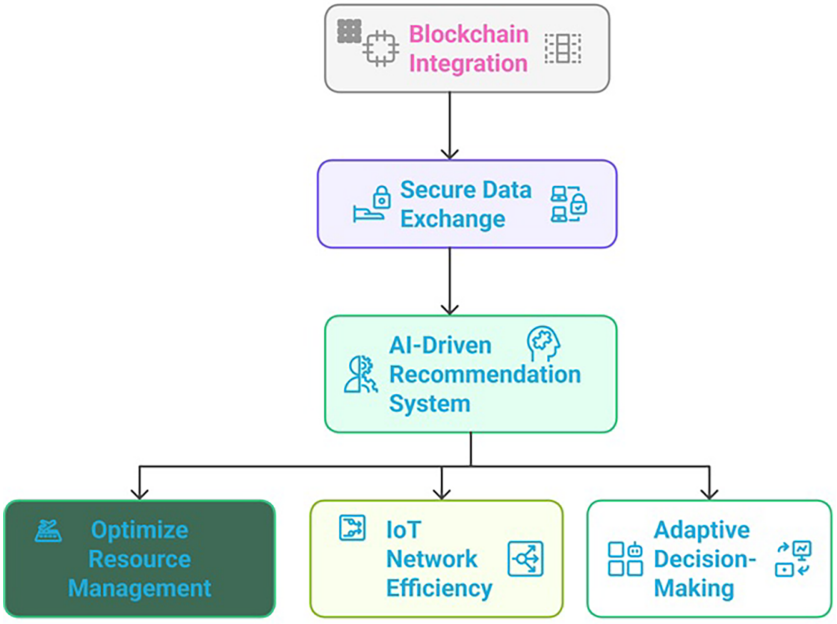


Figure 1: The flow of developed components using a blockchain-integrated AI-recommendation system

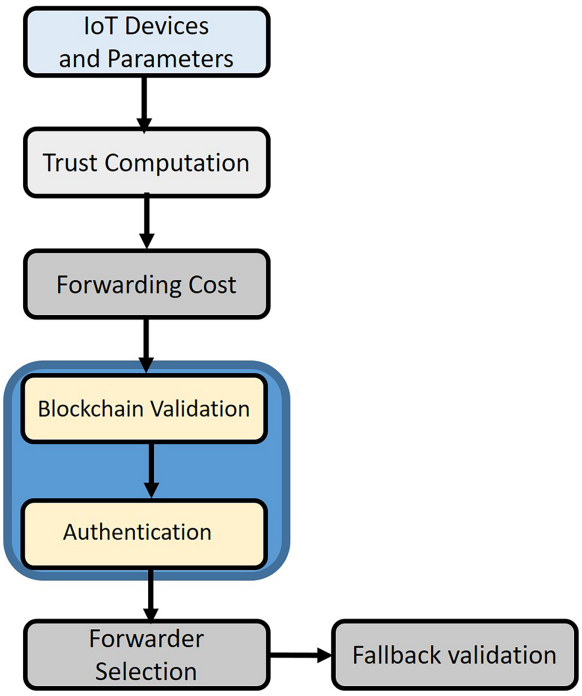


Figure 2: Stages and workflow of the proposed trust-aware routing framework

Initially, node's identity *ID*, transmission power *Trp*, residual energy *RE*, and node location *NL* are collaboratively collected for node i to formulate the routing entries *RE*. It optimizes routing decisions and proposes a more reliable communication paradigm when selecting data forwarders in a dynamic IoT system. The routing entries are defined as follows in Eq. (1):

$$RE(i) \rightarrow \begin{cases} ID, \\ Trp, \\ RE, \\ NL \end{cases} \tag{1}$$

In the proposed framework, graph-based traversal methods are explored to identify all solutions for reaching the source data at the sink node. Later, it selects the optimal solution from the existing solutions. Let us consider that to reach destination *DS* with n nodes, the set of possible routes R is computed using Eq. (2).

$$R = RE(i-1), RE(i-2), \ldots, R(i) \tag{2}$$

At the end of each step of data transmission or receiving, the energy consumption of each node i is computed, as given in Eq. (3).

$$RE_i(t+1) = RE_i(t) - \Delta E_i \tag{3}$$

where ΔE_i denotes the depletion of energy of node i at time t. To initiate the data routing, source node NS_i identifies the set of neighbours within its transmission range and selects a forwarder *NF* to transmit the data by evaluating the cost using Eq. (4).

$$C(i) = \frac{1}{RE} + \frac{1}{D_{NF \rightarrow SN}} + ER \tag{4}$$

where $D_{NF \rightarrow SN}$ denotes the distance of the forwarder node to the sink node. The error rate, denoted by *ER*, is computed based on the total packets, *TP*, and lost packets, *LP*, using Eq. (5).

$$ER = \frac{TP}{LP} + DR \tag{5}$$

where *DR* denotes the delay ratio. *NF* backtracks to the source node with a route request *RREQ*, when there is not appropriate route is available. The source node recomputes the cost and selects a forwarder from its neighbour list based on an AI recommendation system. This system, leveraging past network performance and learned patterns, predicts and recommends the most efficient forwarder, optimizing routing decisions. This is a recursive process that progressively converges on an optimal solution. Later, source nodes continuously compute the cost $C(i)$ for each neighbor, where $C(i)$ represents the cost function for node i based on factors such as latency, energy consumption, or packet loss, and incorporate AI recommendations to select the optimal data forwarder NF^*, as defined in Eq. (6).

$$NF^* = \arg \min_{NF \in N_i} \left(C(i) + \alpha \cdot \hat{R}_i \right) \tag{6}$$

where:

- routing cost for forwarder i is denoted by $C(i)$
- $\hat{R}_i$ and α denote recommendation score, and weighted factor.

Using Eq. (7), a route lifetime RL and error rate ER are explored to determine the trust of a data forwarder $Tr(NF)$, and ensuring an authentic communication along with data reliability.

$$Tr(NF) = ER \cdot RL \tag{7}$$

Using Eq. (8), both the past trust values and new data regarding route lifetime and error rate are utilized to dynamically compute the trust value $Tr(NF)$. Also, a weighting factor $\alpha \in [0,1]$ is used to balance the past and new computed trust score based on the network conditions.

$$Tr(NF)_{(t+1)} = \alpha \cdot Tr(NF)_{(t)} + (1-\alpha) \cdot \left(1 + \frac{ER}{RL}\right) \tag{8}$$

Afterward, using AI integration, an updated trust-driven score X_t is calculated based on past trust observations and network behavior. This score is then committed to the blockchain ledger L, where each entry is secured using a cryptographic hash $H(\cdot)$ to ensure immutability and verifiable traceability. The process reflects the sequential coupling of AI-generated recommendations with blockchain-backed trust validation, as given in Eqs. (9) and (10).

$$X_t = \alpha\, Tr(NF)_{t-1} + (1-\alpha)\left(1 + \frac{ER}{RL}\right) \tag{9}$$

$$H\left(Tr(NF)_t\right) = H(X_t) \tag{10}$$

In the proposed framework, another significant measurement is to attain security in terms of privacy and authentication. The edges in the proposed framework identify non-registered devices in the IoT system, and after verification, the collected data is securely forwarded to the sink node. The edge node generates a secret key k_i which is composed of various shares as defined in Eq. (11).

$$k_i = \begin{cases} S_i, \\ S_{i+1}, \\ S_{i+2}, \\ \vdots \\ S_k \end{cases} \tag{11}$$

(t, n) a threshold-based Shamir's secret sharing technique [35] is used to divide a secret key k_i among a group of n forwarders. The secret key k_i can be reconstructed using any t subset of forwarders. Nevertheless, the k_i cannot be reconstructed with fewer than n subkeys. The shares are sent to forwarders with the integration of time stamps t_0. On receiving each share S_i, the forwarder exploits it in the transmission of collected data d_i using Eq. (12). Later, a particular edge receives all the encrypted data, and it verifies the identity of the forwarder from its trust table, which comprises node identity NID and route identity RID.

$$E_i = (S_i \cdot d_i) + n_0 \tag{12}$$

Algorithms 1 and 2 outline the stages of the proposed framework for energy-aware trust computing in IoT-assisted networks and for selecting reliable forwarders to achieve effective route establishment and maintenance. The proposed framework selects the optimal forwarder from a node's neighbor list using an AI recommendation engine and Blockchain trust data. The forwarder selection process considers both the cost function and the recommendation score, which is adjusted using trust values stored in the Blockchain.

The optimized decision-making AI-recommended engine, along with trustworthiness communication, ensures a secure and authentic IoT network while maintaining the integrity of sensitive data.

Algorithm 1: Energy-aware trust computation

Input: Residual energy $RE_i(t)$, energy cost ΔE_i, neighbor set $\mathcal{N}_i$, trust $Tr(NF)^{(t)}$, route lifetime RL, error rate ER, forgetting factor γ
Output: $RE_i(t+1)$, updated $Tr(NF)^{(t+1)}$

Energy Update
$RE_i(t+1) \leftarrow RE_i(t) - \Delta E_i$;
if $RE_i(t+1) < EnergyThreshold$ **then**
    Mark node as low-energy;
end
Trust Update
foreach $NF \in \mathcal{N}_i$ **do**

$$Tr(NF)^{(t+1)} = \gamma\, Tr(NF)^{(t)} + (1-\gamma)\frac{RL}{1+ER}$$

end
return $RE_i(t+1)$, $Tr(NF)^{(t+1)}$;

Algorithm 2: Forwarder selection using continues trust updation

Input: Neighbor set $\mathcal{N}_i$, cost function $C(\cdot)$, AI-score $\hat{R}(NF)$, updated trust $Tr(NF)^{(t+1)}$, weights α, β
Output: Selected forwarder NF^*

minCost $\leftarrow \infty$,;
$NF^* \leftarrow \varnothing$;
foreach $NF \in \mathcal{N}_i$ **do**

$$c_{\text{adj}} = C(NF) + \alpha \hat{R}(NF) - \beta\, Tr(NF)^{(t+1)}$$

    if $c_{\text{adj}} <$ minCost **then**
        minCost $\leftarrow c_{\text{adj}}$,;
        $NF^* \leftarrow NF$;
    end
end
if $NF^* = \varnothing$ **then**
    Select fallback node;
end
return NF^*;
Complexity: $\mathcal{O}(|\mathcal{N}_i|)$

4 Results Analysis

In this section, the effectiveness of the proposed framework is analyzed with GBTR scheme [29] and LSR algorithm [31]. The experiments were conducted using NS-3 and TensorFlow. Malicious devices, sensors,

and edge and sink nodes make up the simulated environment. The sensors rotate along a circular path and are mobile. They are constrained by energy, processing, and storage limitations. The initial energy levels of the mobile nodes are heterogeneous, ranging 5000 mJ. We evaluate the proposed framework and existing solutions for energy consumption, packet loss ratio, system latency, and device overheads. The execution environment is created using NS-3 on Ubuntu 22.04 OS, Intel core-i7 with 32 GB RAM. Experiments were conducted using varying numbers of packets and fault durations. The simulation parameters are depicted in Table 2.

Table 1: Main Contributions and Limitations

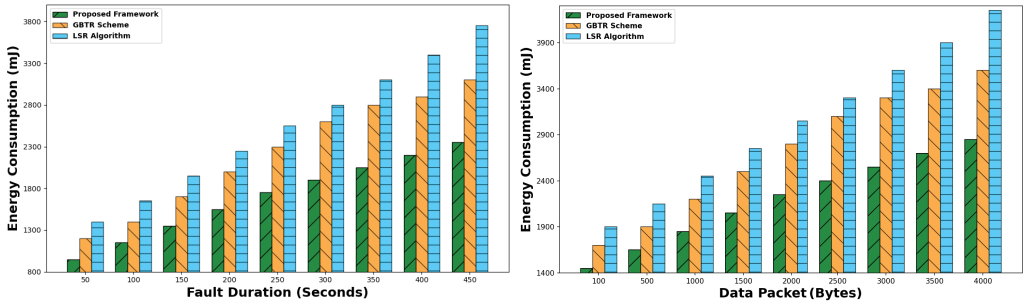
Approaches	Main contributions	Limitations
GBTR [29]	Introduces a trust-enabled routing model that improves network performance and reduces security risks.	Involves high computational cost and additional performance overhead in large-scale scenarios.
Lightweight blockchain-based authentication [30]	Ensures attack-resilient authentication and enhances privacy and integrity using GA-based secure routing.	Consumes extra energy and adds communication overhead due to GA and blockchain operations.
LSR Algorithm [31]	Provides lightweight trust-QoS routing with adaptive decisions and improved throughput.	Shows limited scalability and slow trust updates in rapidly changing environments.
Secure routing for IoT healthcare [32]	Uses fuzzy-whale optimization to enhance trust, energy efficiency, and routing security.	Imposes high computational load and lacks real-world deployment validation.
ATST algorithm [33]	Implements attribute-based trust access control with strong protection against insider threats.	Requires continuous attribute collection, raising privacy concerns, and performs poorly in highly dynamic networks.
Three-layer IoT security architecture [34]	Combines AI and blockchain for improved threat detection and secure data exchange in smart cities.	Demands high resource usage and faces scalability issues in dense IoT environments.
Proposed Framework	Offers AI-enabled adaptive trust management, real-time route recommendation, and secure decentralized delivery via blockchain.	Requires large-scale real-world testing and further optimization for resource-constrained IoT devices.

Table 2: Simulation parameters

Parameter	Value
Initial energy	5000 mJ
IoT sensors	300
Nodes deployment	Random
Malicious devices	10
Sensing radius	5 m
Simulations run	50
Data packet	100 to 4000 bytes
Fault duration	50 to 450 s
Evaluation Scenarios	Varying fault duration and data packets
Baseline methods	GBTR and LSR
Trust window	20 rounds
Decay factor	0.6

Fig. 3a demonstrates that the proposed framework improves energy consumption by an average of 45.3% and 58% compared to existing solutions in terms of fault duration. This improvement is achieved by selecting optimal forwarders using an AI-driven recommendation system that incorporates historical network data and Blockchain trust values to optimize routing. In the prediction phase, forwarder selection is based on intelligent methods that consider congestion and load balancing. Furthermore, it ensures that the system updates trust dynamically, preventing malicious nodes from transmitting false data and reducing network load. This leads to more efficient resource allocation and reduced packet loss. Fig. 3b shows that the proposed framework outperforms existing studies by 37% and 43% in energy consumption under varying data packets. Optimizing resource allocation with an AI-driven approach, along with trust-based mechanisms, enhances system security and ensures reliable blockchain-based IoT-edge communication. It enhances network integrity, ensures robust transmission, and improves the overall system's effectiveness through effective and robust strategies. Fig. 4a illustrates the performance evaluation of the proposed framework and related solutions in terms of data loss rate. Across varying fault durations, the proposed framework reduces data loss rates by 38.6% and 43.2%. The integration of AI-driven recommendation systems and Blockchain trust data enables the framework to optimize performance by intelligently managing network congestion and efficiently controlling IoT resources. By selecting key parameters based on real-time network conditions, the framework ensures reliable communication links and consistent next-hop selection, thereby enhancing long-term connectivity for continuous data routing. In Fig. 4b, the proposed framework outperforms existing solutions by 41.5% and 47% in performance analysis. Continuous updates lead to improvement in routing paths, identification of trustworthy neighbors, and enhanced route lifetime, all supported by Blockchain integration for secure and immutable trust data. The AI-based optimization algorithm balances the load on data links, increases trust between devices, and ensures fault tolerance. Moreover, the system dynamically adapts by invalidating overused routes and notifying the source node to select alternative paths. Fig. 5a compares the performance of the proposed framework with existing solutions, focusing on system latency for varying fault durations. The results demonstrate a 34.5% to 40% improvement in minimizing latency, attributed to the collaboration of sensors, intermediate devices, and Blockchain-integrated trust management. The framework leverages AI-driven decision-making to reroute crucial IoT data and continuously updates trust scores, enhancing reliability and security. By identifying faulty channels

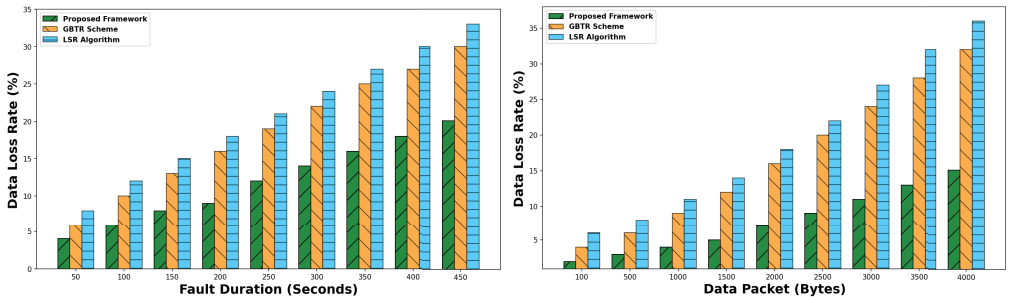
through multi-factor trust computation, the system prevents unauthorized devices and potential threats from injecting malicious route requests. In Fig. 5b, the proposed framework outperforms existing approaches with a 37% to 48% improvement in system latency under varying data packet sizes. This success results from integrating AI-driven multi-factor analysis to optimize decision-making in collaboration with edge devices. The system dynamically updates routing flags and efficiently manages transmission costs through latency-aware data forwarding. Additionally, the proactive routing strategy ensures prompt mitigation of network vulnerabilities. Fig. 6a presents a comparison of the proposed framework and existing approaches in terms of device overhead across varying fault durations. The proposed framework demonstrates a 33% to 38% improvement, achieved by integrating an efficient anomaly detection mechanism. Trust scores are computed, adaptive thresholds are set, and pattern analysis is performed during device communication, reducing false traffic on communication links and enhancing the system's trustworthiness. Agents play a key role in ensuring that only verified devices send real-time data to cloud stations, thereby minimizing device overhead and ensuring the participation of authentic devices. Fig. 6b presents the performance analysis under varying data packets, where the proposed framework shows a significant reduction in communication overhead by 39% to 46%. The AI-driven decision-making process efficiently classifies network traffic, optimizing resource allocation and reducing device overhead from false alarms. The system minimizes resource waste from false notifications and ensures devices are not burdened with unnecessary computations. By combining trust-based AI mechanisms with a robust security and alerting protocol, the framework enhances IoT network security and overall performance while maintaining minimal device overhead.



(a) Energy consumption and fault duration.

(b) Energy consumption and data packets.

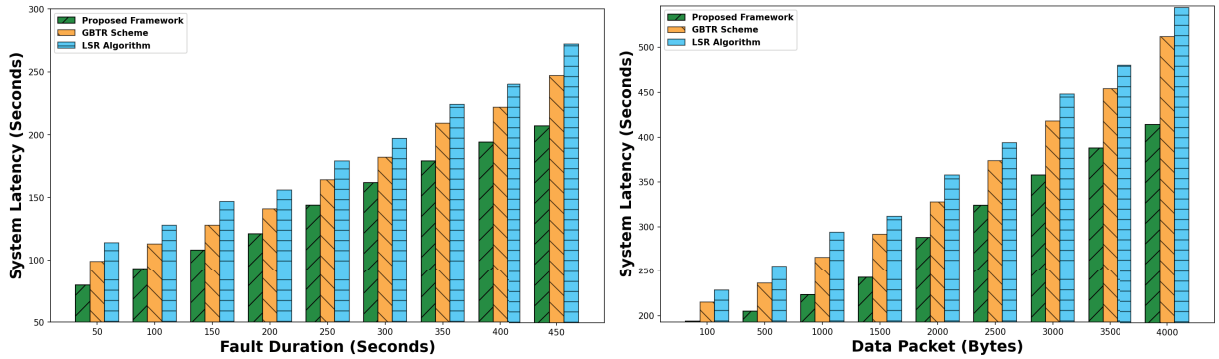
Figure 3: Analysis of energy consumption for proposed framework, GBTR, and LSR: (**a**) Varying fault duration and (**b**) Varying data packet sizes



(a) Data loss rate and fault duration.

(b) Data loss rate and data packets.

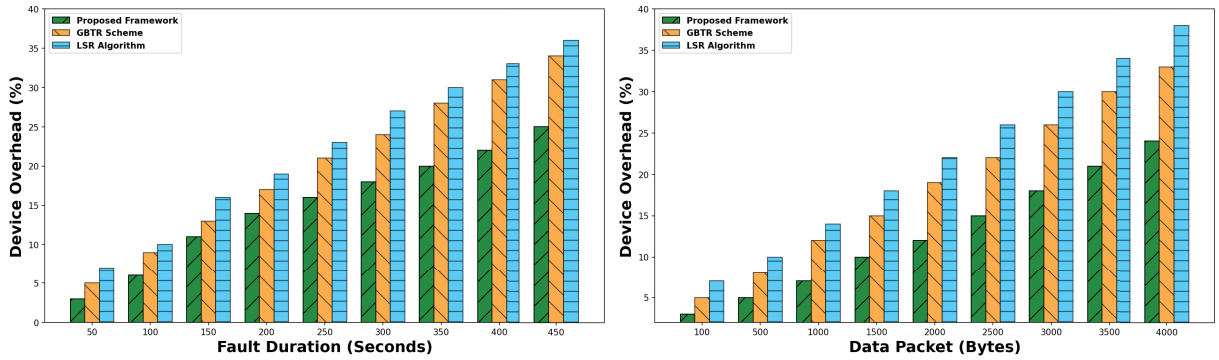
Figure 4: Analysis of data loss rate for proposed framework, GBTR, and LSR: (**a**) Varying fault duration and (**b**) Varying data packet sizes



(a) System latency and fault duration.

(b) System latency and data packets.

Figure 5: Analysis of system latency for proposed framework, GBTR, and LSR: (**a**) Varying fault duration and (**b**) Varying data packet sizes



(a) Device overhead and fault duration.

(b) Device overhead and data packets.

Figure 6: Analysis of device overhead for proposed framework, GBTR, and LSR: (**a**) Varying fault duration and (**b**) Varying data packet sizes

5 Conclusion

Smart cities have adopted emerging technologies and IoT systems to advance intelligent communication. Such systems perform data analysis and processing with human involvement, thereby advancing a sustainable environment. Real-time monitoring of harsh conditions enables an effective communication paradigm and supports timely resource management for responding to requested devices. Although many approaches have been proposed to address the automation system's routing and enhance optimization processes, many solutions still lack reliable data transfer and trust integration. Furthermore, the involvement of faulty channels in data sensing and fusion introduces additional overhead and reduces privacy among IoT-connected systems. The trustless environment has a highly significant impact on security measurement when dealing with constrained resources and optimizing decision-making systems. Our research proposed an AI-recommended framework, along with blockchain technology, for energy-efficient, collaborative network infrastructure. It offers fault-tolerant communication services across network-wide interconnected devices and addresses the unpredictable conditions that can undermine trust between peer devices. It also extends connectivity without imposing additional computational load on bounded sensors and ultimately exposes malicious activities through high-level security analysis. We intend to explore machine learning algorithms

to improve the scalability of the proposed framework against distributed attacks and to minimize complexity across diverse large-scale IoT networks.

Acknowledgement: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant No. (DGSSR-2024-02-02152).

Funding Statement: This research was supported by the Deanship of Graduate Studies and Scientific Research at Jouf University under Grant No. DGSSR-2024-02-02152.

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

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

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

References

1. Hashem IA, Siddiqa A, Alaba FA, Bilal M, Alhashmi SM. Distributed intelligence for IoT-based smart cities: a survey. Neural Comput Appl. 2024;36(27):16621–56. doi:10.1007/s00521-024-10136-y.
2. 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(2):50296–339. doi:10.1109/access.2025.3551750.
3. 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.
4. Houssein EH, Othman MA, Mohamed WM, Younan M. Internet of things in smart cities: comprehensive review, open issues and challenges. IEEE Internet Things J. 2024;11(21):34941–52. doi:10.1109/jiot.2024.3449753.
5. Alshammeri M, Humayun M, Haseeb K, Alwakid GN. AI-driven sentiment-enhanced secure IoT communication model using resilience behavior analysis. Comput Mater Continua. 2025;84(1):433–46. doi:10.32604/cmc.2025.065660.
6. Kanellopoulos D, Sharma VK. Dynamic load balancing techniques in the IoT: a review. Symmetry. 2022;14(12):2554. doi:10.3390/sym14122554.
7. Osamy W, Alwasel B, Salim A, Khedr AM, Aziz A. LBAS: load-balancing aware clustering scheme for IoT-based heterogeneous wireless sensor networks. IEEE Sensors J. 2024;24(9):15472–90. doi:10.1109/jsen.2024.3381852.
8. Duan S, Wang D, Ren J, Lyu F, Zhang Y, Wu H, et al. Distributed artificial intelligence empowered by end-edge-cloud computing: a survey. IEEE Commun Surv Tutorials. 2022;25(1):591–624.
9. Luzolo PH, Elrawashdeh Z, Tchappi I, Galland S, Outay F. Combining multi-agent systems and artificial intelligence of things: technical challenges and gains. Internet Things. 2024;28(15):101364. doi:10.1016/j.iot.2024.101364.
10. Al-Hejri I, Azzedin F, Almuhammadi S, Syed NF. Enabling efficient data transmission in wireless sensor networks-based IoT applications. Comput Mater Continua. 2024;79(3):4197–218.
11. Islam S, Abdulsalam AZ, Kumar BA, Hasan MK, Kolandaisamy R, Safie N. Mobile networks toward 5G/6G: network architecture, opportunities and challenges in smart city. IEEE Open J Commun Soc. 2024;6(20065):3082–93. doi:10.1109/ojcoms.2024.3419791.
12. 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.

13. Xiong R, Cheng J, Pu J, Dong X, Chen C, Xu Z. Enhancing trust and collaboration: a reputation-driven mechanism for cross-chain IoT data sharing. Comput Netw. 2025;264(1):111266. doi:10.1016/j.comnet.2025.111266.
14. Gill SS, Golec M, Hu J, Xu M, Du J, Wu H, et al. Edge AI: a taxonomy, systematic review and future directions. Cluster Comput. 2025;28(1):18.
15. Zhang C, He Q, Li F, Yu K. Intelligent task offloading and resource allocation in knowledge defined edge computing networks. IEEE Trans Mobile Comput. 2025;24(5):4312–25. doi:10.1109/tmc.2024.3522253.
16. Lai B, Wen J, Kang J, Du H, Nie J, Yi C, et al. Resource-efficient generative mobile edge networks in 6G era: fundamentals, framework and case study. IEEE Wirel Commun. 2024;31(4):66–74. doi:10.1109/mwc.007.2300582.
17. Deng Y, Lyu F, Xia T, Zhou Y, Zhang Y, Ren J, et al. A communication-efficient hierarchical federated learning framework via shaping data distribution at edge. IEEE/ACM Trans Netw. 2024;32(3):2600–15. doi:10.1109/tnet.2024.3363916.
18. Nag A, Hassan MM, Das A, Sinha A, Chand N, Kar A, et al. Exploring the applications and security threats of Internet of Thing in the cloud computing paradigm: a comprehensive study on the cloud of things. Trans Emerg Telecomm Technol. 2024;35(4):e4897. doi:10.1002/ett.4897.
19. Almutairi M, Sheldon FT. IoT-Cloud integration security: a survey of challenges, solutions, and directions. Electronics. 2025;14(7):1394. doi:10.3390/electronics14071394.
20. D'aniello G, Fotia L. Blockchain and AI-based methods for trust management in IoT: a comprehensive survey. Internet Things. 2025;34(27):101755. doi:10.1016/j.iot.2025.101755.
21. 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.
22. Ali I, Ahmedy I, Gani A, Munir MU, Anisi MH. Data collection in studies on Internet of things (IoT), wireless sensor networks (WSNs), and sensor cloud (SC): similarities and differences. IEEE Access. 2022;10(8):33909–31. doi:10.1109/access.2022.3161929.
23. Ullah A, Anwar SM, Li J, Nadeem L, Mahmood T, Rehman A, et al. Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment. Compl Intell Syst. 2024;10(1):1607–37.
24. 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.
25. Priyadarshi R, Kumar RR, Ranjan R, Kumar PV. AI-based routing algorithms improve energy efficiency, latency, and data reliability in wireless sensor networks. Sci Rep. 2025;15(1):22292. doi:10.1038/s41598-025-08677-w.
26. Darabkh KA, Al-Akhras M. Towards optimized IoT sensor networks for smart cities: centrality-aware position-based occlusion-driven and role dynamics solutions for clustering and routing. IEEE Internet Things J. 2025;12(15):30282–301. doi:10.1109/jiot.2025.3570612.
27. Khanh QV, Nguyen VH, Minh QN, Van AD, Le Anh N, Chehri A. An efficient edge computing management mechanism for sustainable smart cities. Sustain Comput Inform Syst. 2023;38(1):100867. doi:10.1016/j.suscom.2023.100867.
28. Ajao LA, Apeh ST. Secure edge computing vulnerabilities in smart cities sustainability using petri net and genetic algorithm-based reinforcement learning. Intell Syst Appl. 2023;18(1):200216. doi:10.1016/j.iswa.2023.200216.
29. Alam I, Manjul M, Pathak V, Mala V, Mangal A, Thakur HK, et al. Efficient and secure graph-based trust-enabled routing in vehicular ad-hoc networks. Mobile Netw Appl. 2024;29(6):1732–52. doi:10.1007/s11036-023-02274-9.
30. Abbas S, Javaid N, Almogren A, Gulfam SM, Ahmed A, Radwan A. Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things. IEEE Access. 2021;9:139739–54. doi:10.1109/access.2021.3118948.
31. Pathak A, Al-Anbagi I, Hamilton HJ. An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs. IEEE Internet Things J. 2022;9(23):23826–40. doi:10.1109/jiot.2022.3189832.
32. Xu H, Wd Liu, Li L, Dj Yao, Ma LFSRW. Fuzzy logic-based whale optimization algorithm for trust-aware routing in IoT-based healthcare. Sci Rep. 2024;14(1):16640. doi:10.1038/s41598-024-66392-4.
33. Zhang X, Deng H, Xiong Z, Liu Y, Rao Y, Lyu Y, et al. Secure routing strategy based on attribute-based trust access control in social-aware networks. J Signal Process Syst. 2024;96(2):153–68. doi:10.1007/s11265-023-01908-1.
34. Khan BUI, Goh KW, Khan AR, Zuhairi MF, Chaimanee M. Integrating AI and blockchain for enhanced data security in IoT-driven smart cities. Processes. 2024;12(9):1825. doi:10.3390/pr12091825.
35. Shamir A. How to share a secret. Commun ACM. 1979;22(11):612–3.