Computer Modeling in Engineering & Sciences

Tech Science Press

https://doi.org/10.32604/cmes.2026.080287

ARTICLE

Trust-Centric Security Architecture and Anomaly Analytics for Distributed Fog-IoT Systems

Maram Fahaad Almufareh[1,*], Mamoona Humayun[2], Sadia Din[3,*], Khalid Haseeb[4] and Amr Munshi[5]

[1]Department of Information System, College of Computer and Information Sciences, Sakaka, Al-Jouf, Saudi Arabia
[2]School of Computing, Engineering and the Built Environment, University of Roehampton, London, UK
[3]School of Computer Engineering, Gachon University, Seongnam-si, Republic of Korea
[4]Department of Computer Science, Islamia College Peshawar, Pakistan
[5]Department of Computer and Network Engineering, College of Computing, Umm Al-Qura University, Makkah, Saudi Arabia

*Corresponding Authors: Maram Fahaad Almufareh. Email: mfalmufareh@ju.edu.sa; Sadia Din. Email: sadiadin@gachon.ac.kr

Received: 06 February 2026; Accepted: 25 March 2026; Published: 27 April 2026

ABSTRACT: The real-time systems perform key functionalities in various fields to automate the communication and response in critical events. The Internet of Things (IoT), integrated with numerous physical objects, gathers environmental data, processes it at the edge, and provides intelligent decisions while routing health records to processing units. However, the dynamic and resource-constrained nature of IoT-based healthcare environments introduces significant challenges related to latency, transmission costs, and the reliable interaction of devices amid uncertain activities. In this work, we propose a framework for a consistent and trustworthy system that uses a weighted trust aggregation model to consider multiple parameters and support timely routing decisions in a Fog-driven healthcare environment. Furthermore, authorized access to critical and sensitive health data is achieved through mutual authentication among devices, ensuring data integrity. The analysis of trust scores dynamically enhances resilience and the timely detection of malicious actions, thereby improving the healthcare system's performance across unpredictable channels. The performance of the proposed framework is tested and validated against CLCSR and FSRF, and performance results revealed the significance for energy consumption, response time, network throughput, trust level, and accuracy across varying fog node capacity and interference scenarios.

KEYWORDS: Fog computing; data privacy; healthcare system; intelligent decision; network attackers

1 Introduction

Future wireless technologies play a crucial role in developing innovative real-time applications by enabling seamless communication [1,2]. They offer and facilitate real-time data sensing and exchange with low-latency connectivity channels for IoT-based solutions in innovative systems [3,4]. Emerging technologies that integrate with the Internet of Things (IoT) have revolutionized innovative development and communication for interaction with the physical world [5,6]. Fog computing enhances the capabilities of IoT networks by improving data processing closer to the source and improving system efficiency [7,8]. In healthcare IoT networks, such computing paradigms enhance real-time decision-making capabilities and reduce computational overhead under resource constraints [9,10]. Also, edge computing [11,12] is being utilized in many innovative applications to process the requested data at the edge, rather than by devices or local servers. However, many approaches have been proposed that combine edge computing with reduced computing power on constrained devices [13,14]. Nonetheless, it remains challenging to

achieve effective load distribution in dynamic networks, particularly when addressing energy holes near the edges. Despite numerous advancements, the quality of service in IoT-based healthcare applications remains a pressing research issue, particularly when devices are heterogeneous [15,16]. On the other hand, trust computing ensures the reliability of e-health records by continuously evaluating and maintaining device trustworthiness [17,18]. In a critical healthcare system, timely identification of malicious behavior and maintenance of integrity are essential to protecting sensitive medical information. 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 [19–21]. This research aims to introduce a fog-based intelligent framework using weigted trusted based aggregation modeling for efficient, and secured IoT-based healthcare communication. It enhances the security of health records and promptly transmits crucial data to processing servers, leveraging authentic fog-IoT-driven routing strategies. In real-time applications, the reliability of health data can be ensured through regular device monitoring using trust computing [22,23]. However, detecting faulty communication and malicious threats in healthcare applications in a timely and accurate manner remains a challenging research problem for IoT-driven systems.

Healthcare systems have become increasingly vulnerable due to inconsistent communication and potential attacks, thereby affecting the overall system. In addition, non-optimised decision-making schemes that do not account for network performance parameters degrade the resilience of critical applications to disruption and high-rate congestion. Despite several proposed approaches, most still lack fault-tolerant, robust trust-aware routing strategies and provide no guarantee of consistent device interactions in the face of malicious activity. Unreliable and compromised data is forwarded by network devices without establishing mutual trust or considering dynamic trustworthiness factors. It undermines the system's confidence in timely decision-making and increases computational complexity when handling faulty traffic flow. Therefore, this study aims to address these issues by introducing an intelligent framework that integrates weighted-based trust aggregation with more reliable transmission channels, thereby ensuring consistent routing in the IoHT environment at the Fog-based communication layer. Based on the aforementioned discussion, the proposed framework addresses the following research questions.

RQ1: How can a healthcare system be scalable and provide reliable communication between devices in fog-based architecture against potential threats?

RQ2: How can a lightweight secured paradigm be attained while routing the healthcare records over an unpredictable environment?

RQ3: How can effective strategies be adopted to maintain the longevity of established routes and enhance the effectiveness of decision making system?

Ultimately, the main contributions of our research works are highlighted as follows.

i. A dynamic and scalable IoT-based healthcare architecture developed and integrated with fog computing to balance the network resources and enhance reliability against threats.
ii. A weighted trust model ensures consistent and secure communication channels while transmitting the gathered data towards processing stations and increases the effectiveness of decision-making in a timely manner, considering multiple factors.
iii. The authentic methods are initiated to dynamically update the trust for the constructed routes and minimise the probabilities of data breaches and network disconnection for diverse systems.

The research work is structured as follows. Related work is covered in Section 2. The proposed framework and its developed components are explained in Section 3. Section 4 provides an experimental discussion. Finally, the conclusion and future work are outlined in Section 5.

2 Related Work

The IoT network enables seamless collection of sensor data by integrating wireless systems, enabling real-time monitoring in unpredictable environments [24,25]. The limitations of bounded networks pose distinct research challenges for processing, storage, and energy efficiency. Furthermore, the critical operations demand low-latency communication and a trust-aware monitoring system across distributed devices [26,27]. Maintaining network scalability and security in dynamic healthcare environments with dynamic conditions and environmental status presents significant challenges. Authors in [28] introduce a context-based adaptive trust model for innovative healthcare systems. It explores Bayesian approaches and similarity measures to address threats such as bad mouthing and ballot stuffing. Moreover, direct and indirect trust are computed using adaptive weights, entropy values to minimize bias, and context similarity to filter out malicious nodes. The proposed solution was simulated in Contiki-Cooja, and the results showed significant improvements in trust and reliability for healthcare systems. In [29], the authors introduce a novel protocol that integrates fog computing and software-defined networking (SDN) to enhance network scalability and support location-based services in VANETs. By exploring network lifetime, average distance, and signal-to-interference-plus-noise ratio, a new cluster-head (CH) selection algorithm is proposed. It reduces the overhead of long-distance transmission control and packet loss. Moreover, a dual-phase strategy is utilised so the AODV protocol acts as a fallback for handling large and complex packets. For the detection of network attacks and preseve data privacy with secure transmission, a study [30] proposed a novel method known as Cross-Layer and Cryptography-based Secure Routing (CLCSR). It is two phase framework: Firstly, a secure clustering mechanism is introduced using cross layer method and secondly a data is protected against threats based on lightweight cryptography principles. In addition, the use of cross-layer parameters and probability models, the proposed method provides the selection of most reliable and optimal cluster heads to improve the overall performance. Moreover, the lightweight Elliptic Curve Cryptography (ECC) is applied to impose the devices authentication and only grant the authorized access to network data. Authors of [31] present a two-layered hierarchical design for fog devices and explore cluster-based techniques for data aggregation and optimizing resources in healthcare applications. Three efficient algorithms are proposed for decreasing additional energy consumption and data latency. The proposed solutions are tested and validated using the iFogSim toolkit, and the performance results have shown significant improvements over existing approaches. Authors in [32] proposes a secure data forwarding mechanism for MQTT a widely used IoT communication protocol. It enhances reliability and data security by integrating fog-based computing resources with the MQTT ecosystem. Moreover, an informed data-transmission decision strategy is proposed that employs trust models for IoT and fog devices. To achieve real-time security and align with real-time network demands, the proposed solution utilizes key components, including TLS/SSL and cryptographic techniques. Authors in [33] introduce the DeW-IoMT framework for fog-cloud communication systems. The novel roof-computing layer reduces latency, processes tasks locally, and enhances security, thereby serving as an intermediary for communication. The proposed framework, simulated using iFogSim, minimizes computational overheads and ensures timely system responses for healthcare applications. Authors [34] introduce a fuzzy logic–based secure hierarchical routing scheme (FSRF) to enhance data privacy and routing effectiveness in healthcare systems. Moreover, a framework for fuzzy-based trust is explored to analyse device authenticity and ultimately increase the reliability of IoT communication against various attacks. In addition, the Firefly Algorithm is utilised for clustering and selecting optimal cluster heads, using a fitness function that evaluates multiple parameters.

3 Proposed Methodology

This section provides a detailed discussion of the Fog-Assisted Anomaly-Aware Trust-Based Routing (FATR) framework, which aims to improve resource efficiency and enable trusted collaboration among health devices. Our proposed framework comprises three main phases: system design, anomaly detection using trusted computing, and communication performance improvement. Eq. (1) determines the device power consumption at the fog layer, P_{fog}, with the weighting sum of a particular power consumption of a device P_{device_i}, and scaling factors α_i reflecting each device's operational state.

3.1 Fog-Based Routing Decision Algorithm

The proposed FATR framework leverages effective resource management and optimized decision-making at the network edge, leveraging the interaction between fog computing and IoT devices. The edges are used to process data closest to the collection points, enabling efficient trust-aware communication and load balancing. It ensures an anomaly-free healthcare environment by computing device trust and dynamically updating it under realistic conditions. The main components of the FATR framework are shown in Fig. 1.

$$P_{\text{fog}} = \sum_{i=1}^{n} \frac{\alpha_i}{\sum_{j=1}^{n} \alpha_j} P_{\text{device}_i} \tag{1}$$

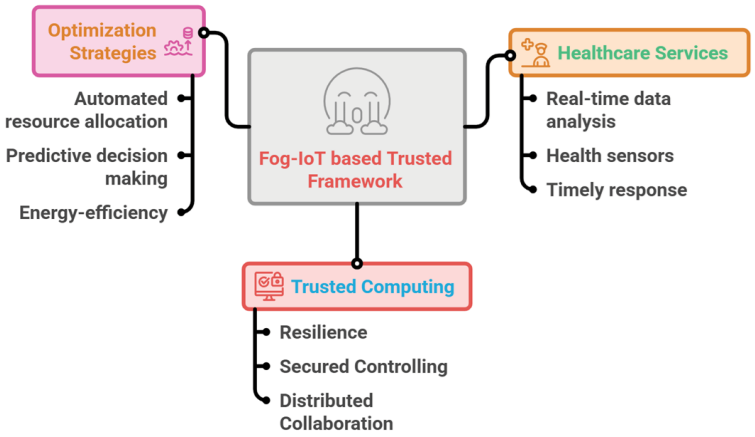


Figure 1: Components of the proposed fog-assisted anomaly-aware trust-based routing framework.

The scaling factor α_i adjusts each device's power consumption according to its importance in the system, thereby ensuring efficient resource allocation and load balancing across the network. By aggregating the contributions of all devices, $\boldsymbol{P}_{\text{device}}$ represents the power consumption of each device in the system as a column vector, and $\boldsymbol{\alpha}$ represents the corresponding scaling factors as another vector. In addition to power consumption, route identification and management are critical tasks for achieving efficient communication in the healthcare system. Our system dynamically selects the set of routes by exploring reliability, latency, and energy efficiency. Thus, the energy efficiency of a route is represented in Eq. (2).

$$E_{\text{total}} = \sum_{p \in \mathcal{P}} \sum_{i=1}^{n} \left(P_{\text{device}_i} \cdot L_i(p) \right) \tag{2}$$

where E_{total} is the total energy consumption across all routes in the set $\mathcal{P}$, P_{device_i} is the power consumption of the i-th device, and $L_i(p)$ is the length of link i along route p. The sum is taken over all routes in the set $\mathcal{P}$,

which represents the possible communication paths in the healthcare IoT network. Furthermore, the system minimizes latency by accounting for each route's reliability using Eq. (3).

$$L_{\text{total}}(p) = \sum_{i=1}^{n} (\lambda_i \cdot L_i(p)) \tag{3}$$

where $L_{\text{total}}(p)$ is the total latency of route p, λ_i is a weight factor adjusting the importance of link i, and $L_i(p)$ is the latency of link i on the route.

In system design, the fog devices collect the health data from IoT devices and perform real-time anomaly detection and trust assessments. It enables continuous monitoring and updates device trust.

3.2 Proposed Trust-Aware Anomaly Detection Healthcare Framework

In this section, the trust-aware route selection and anomaly detection are explained. The proposed FATR framework utilized a weighted trust aggregation model for the formulation of routes. To compute the probability of a route being optimal, multiple parameters such as device trust T_{device_i}, latency L_i, and power $Power_i$ usage are considered; thus, the trust of the route T_{route} can be modeled as expressed in Eq. (4).

$$T_{\text{route}} = \frac{1}{n} \sum_{i=1}^{n} \left(w_1 T_{\text{device}_i} + w_2 L_i + w_3 \text{Power}_i \right), \quad w_1, w_2, w_3 \in [0,1], \quad w_1 + w_2 + w_3 = 1 \tag{4}$$

This process provides the selection of a consistent route by computing the joint probabilities for all possible routes in the set $\mathcal{P}$, selecting the one with the highest probability of success, as expressed in Eq. (5).

$$R^* = \arg\max_{p \in \mathcal{P}} T_{\text{route}}(p) \tag{5}$$

Later, the FATR framework updated the trust value $T_i(t)$ of device i at time t based on the previous trust value and the current anomaly detection score $A_i(t)$, as given in Eq. (6).

$$A_i(t) = \min\left(\frac{F_i(t)}{S_i(t)}, 1 \right) \tag{6}$$

$$T_i = \alpha \cdot \left(w_1 T_{\text{device}} + w_2 L_i + w_3 \text{Power}_i \right) + (1 - \alpha) \cdot A_i(t) \tag{7}$$

where $T_i(t)$ represents the trust value of device i at time t, $T_i(t-1)$ represents the previous trust value of device i, $A_i(t)$ represents the anomaly score of device i at time t, as detected by the anomaly detection algorithm, α is the weight given to the previous trust score, and β is the weight given to the anomaly detection score. The trust-level computation identifies the most reliable forwarders based on their past interactions and existing anomaly scores. A system is in a more accurate state when the most trusted devices at the highest level are selected to formulate routes. Moreover, if the anomaly score $A_i(t)$ exceeds a certain threshold, the device's trust value is adjusted downward, indicating that it may not be reliable for communication, as given in Eq. (8).

$$T_i(t) = \alpha T_i(t-1) + (1-\alpha)\beta A_i(t) \cdot \begin{cases} +1, & A_i(t) \le \theta \\ -1, & A_i(t) > \theta \end{cases} \tag{8}$$

Eq. (9) logs the anomalous behavior of each device i based on the anomaly score $A_i(t)$, recorded when $A_i(t) > \theta$, it integrates these logs for all devices $\mathcal{L}_{\text{all}}$, and ultimately able to monitoring the anomalous behaviors of the malicious devices for the maintenance of trustworthiness communication.

$$\text{GlobalAnomalyLog}[t] = \{i \mid A_i(t) > \theta,\ i = 1, \ldots, n\} \tag{9}$$

In the next phase, the proposed framework incorporates a route maintenance strategy that optimizes path selection. The route cost function, C_{route}, is defined in Eq. (10).

$$C_{route}(p) = \sum_{i=1}^{n} w_i \cdot L_i(p) \tag{10}$$

where $C_{route}(p)$ is the total route cost for path p, w_i is the weight factor for link i based on device reliability, and $L_i(p)$ is the latency of link i in path p. Our proposed framework selects the optimal path by minimizing the route cost, and the path optimization problem can be formulated using Eq. (11).

$$p^* = \arg\min_{p \in \mathcal{P}} \sum_{i \in p} w_i L_i \tag{11}$$

The proposed framework dynamically adjusts the routing strategies and selects the most optimal forwarders based on network conditions and computed trust levels. Accordingly, leads to low latency and high reliability for IoT-healthcare communications. Algorithm 1 outlines a mechanism of trust evaluation and prediction for routing paths in a healthcare network based on a weighted trusted aggregation model. It explores multiple features, along with the success rate, to determine the trust level for device v_i. If the confidence of the computed trust is higher than a predefined threshold θ, then the particular device is marked as trustworthy. Upon detecting a malicious device, the FATR framework isolates it in a separate log and issues a rerouting call to the neighbors. By analysing the network's dynamic properties, the FATR framework maintains stable communication with high trust and data integrity, preventing unauthorized disclosure. Fig. 2 illustrates the workflow of the proposed framework, comprising feature selection, trust computing, route optimisation, and trust maintenance phases. All phases interact with one another in the design and development of a trusted communication Fog-IoT healthcare system.

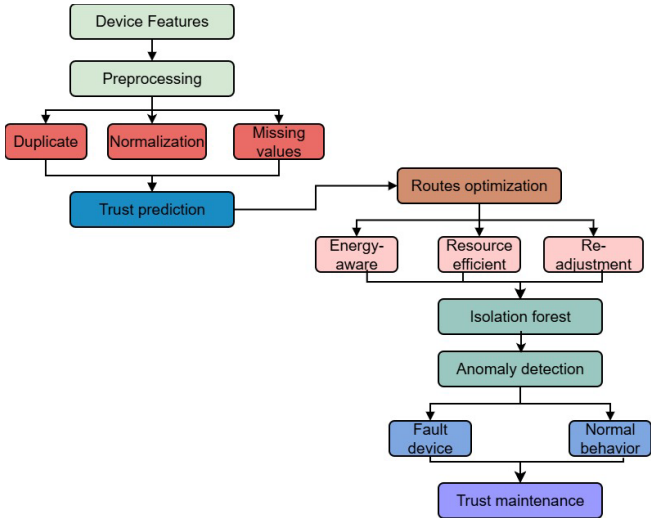


Figure 2: Flow diagram of proposed trusted fog-based IoT healthcare framework.

Algorithm 1: Trust-based route detection and management

Input: Devices $\{v_i\}_{i=1}^{n}$, historical trust $T_i(t-1)$, features: energy E_i, link L_i, power P_i, packets sent S_i, packets forwarded F_i, device weights α_i

Output: Updated device trust $\{T_i(t)\}$, Fog-level trust P_{fog}, optimal route p^*

for *each device* v_i **do**
  $A_i(t) \leftarrow \frac{F_i}{S_i}$ // Compute behavior-based anomaly score
  if $A_i(t) \leq \theta$ **then**
    Normal behavior: maintain/increase trust
  else
    Anomaly detected: reduce trust
$P_{\text{fog}} \leftarrow \sum_{i=1}^{n} \alpha_i \, T_i(t)$ // Aggregate trust at fog node
$p^* \leftarrow \arg\min_{p \in \mathcal{P}} \sum_{i \in p} w_i \, L_i$ // Select optimal route based on weighted link cost
return $\{T_i(t)\}$, P_{fog}, p^*

4 Simulation Description

This section presents a performance evaluation of the FATR framework compared with existing studies. The simulation is conducted using iFogSim, which comprises sensors, fog, and infrastructure. The deployed network comprises various healthcare sensors, including wearable health-monitoring devices, interconnected with fog nodes. Fog devices are more stable and have greater computational and storage resources than IoT sensors. The transmission range is set to 5 m. The initial energy for each sensor is fixed at 5 J, and the simulation dimension is 3000 m × 3000 m. A varying health sensors are deployed to monitor vital parameters such as heart rate, temperature, and blood pressure. Attacker nodes are also introduced at rates of 10%–80% to simulate network threats and inject unauthenticated data. The experimental analysis is conducted across varying fog capacity and attacker intensity levels, focusing on energy consumption, network throughput, response time, and attack resilience. Table 1 declares the default parameters that are utilized in experiments. Moreover, approximately 50 simulations were conducted to generate synthetic data and a dataset for analysing the proposed FATR framework and related approaches. The dataset schema is defined in Table 2 to align with IoT-Fog-driven healthcare systems, including attributes such as device identity, timestamp, sensor readings, threat level, anomaly flag, and threat type.

Fig. 3a,b present the performance analysis of the FATR framework and related studies with respect to network throughput. The results demonstrated that the FATR framework enhances network throughput by an average of 36% and 41% over CLCSR and FSRF, respectively. This improvement is due to intelligent route prediction that accounts for network conditions and effective load balancing between IoT and fog systems. Additionally, integrating trust and secure routing paths enhances the FATR framework's ability to identify anomalies and exclude faulty routes from communication channels. Using the Isolation Forest method, the FATR framework dynamically adjusts and optimizes the resources of healthcare applications, ultimately providing a more reliable ecosystem to handle a higher volume of health records for further processing.

Fig. 4a,b present the performance evaluation of the FATR framework for energy consumption compared with existing approaches. Across varying fog capacity and attacker intensity, the statistical results showed significant performance improvements for the FATR framework, averaging 39% and 46%, respectively. This improvement is due to adaptive routing schemes that integrate intelligence and leverage more stable forwarders within the trusted healthcare ecosystem. The prediction algorithm is developed for trust evaluation using weighted methods that explore multiple parameters, providing a consistent method for selecting the

next-hop for transmitting health data to fog devices. Moreover, network conditions are also exploited to maintain efficient resource management.

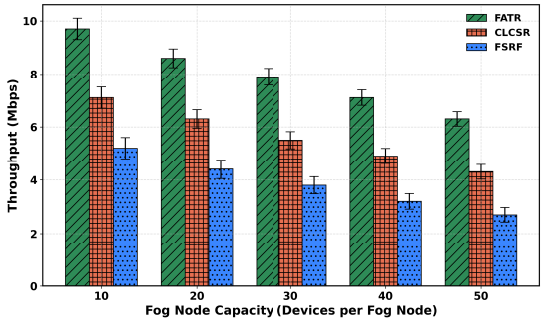
Fig. 5a,b illustrate the performance of the FATR framework with CLCSR and FSRF in terms of attack resilience across varying fog capacity and attacker intensity. The results showed that the FATR framework outperformed existing studies by an average of 43% and 49%, respectively. This is due to the inclusion of dynamic trust updates and the exclusion of malicious devices from data transmission in healthcare applications. It not only provides a consistent path for long-term network connectivity but also enables distributed processing with intelligent threat-detection strategies to ensure data integrity and device authentication. Moreover, by excluding faulty links and devices from real-time health monitoring, the FATR framework reduces the additional delay caused by flooding vulnerable traffic, thereby improving its computational efficiency.

Table 1: Simulation parameters.

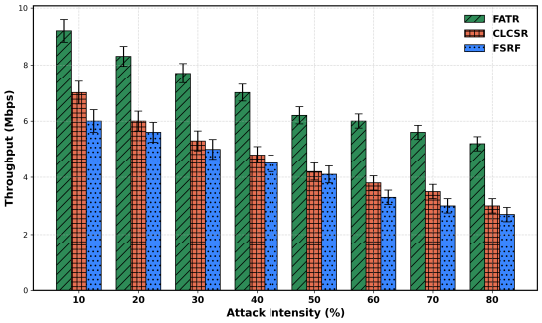
Parameter	Value
Simulation Area	3000 m × 3000 m
Number of Sensors	10–50
Number of attackers	10–80
Initial Energy	5 J
Simulations	50 runs
Fog devices	20
Trust Weighting Factors	w_1, w_2, w_3
Packet Length	256 bits
Anomaly Threshold	θ
Transmission Range	5 m
Traffic patterns	Random

Table 2: Dataset schema with generation details.

Parameter	Detail	Generation
timestamp	Time of record	Every second; fixed start time for reproducibility
device_id	Identity of IoT device	Random integer from 1 to N
reliability	Device reliability	Sampled from Beta distribution Beta$(5,1)$
integrity	Data trustworthiness	Sampled from Beta distribution Beta$(5,2)$
trust_score	Combined trust	Weighted sum of parameters
fog_node_id	Indentity of Fog node	Random integer from 1 to M
latency	Delay (s)	Log-normal
energy_usage	Energy (J)	Normal; device-dependent
anomaly	Anomaly flag	Binary $\{0,1\}$
anomaly_score	Confidence score	0–1; high if anomaly = 1
threat_level	Threat severity	Derived from anomaly_score; 0 = none, 3 = high
threat_type	Anomaly type	Failure, tampering, compromise

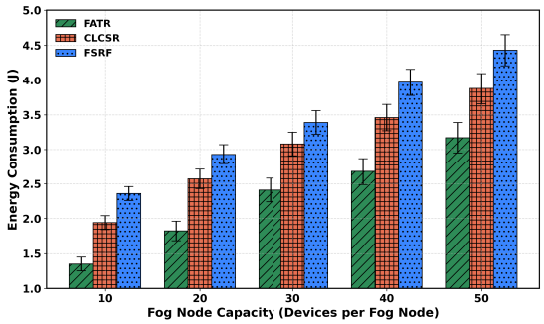


(**a**) Network throughput and capacity of fog node (10–50).

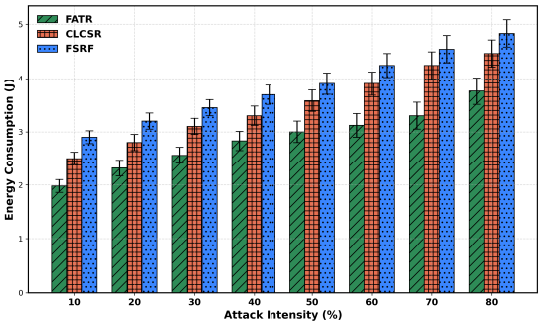


(**b**) Network throughput and attacker intensity (10%–80%).

Figure 3: Performance comparison of the proposed FATR framework with CLCSR and FSRF under varying network conditions.

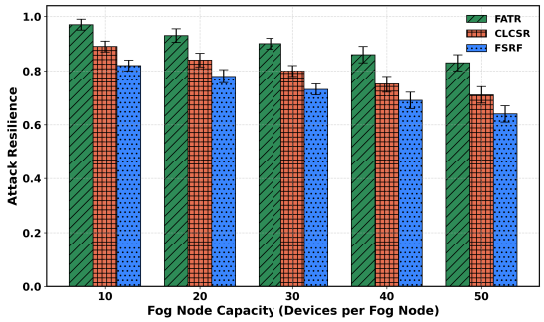


(**a**) Energy consumption and capacity of fog node (10–50).

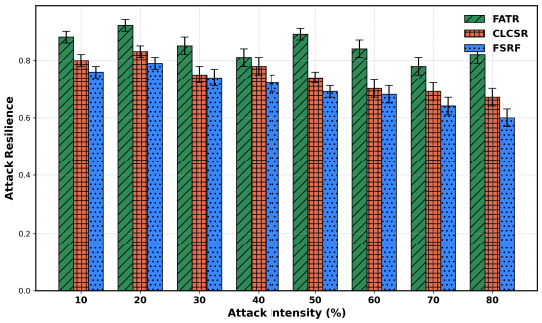


(**b**) Energy consumption and attacker intensity (10%–80%).

Figure 4: Energy consumption comparison of the proposed FATR framework with CLCSR and FSRF under varying network conditions.



(**a**) Attack resilience and capacity of fog node (10–50).

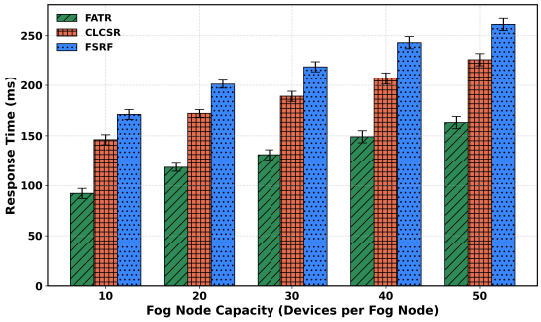


(**b**) Attack resilience and attacker intensity (10%–80%).

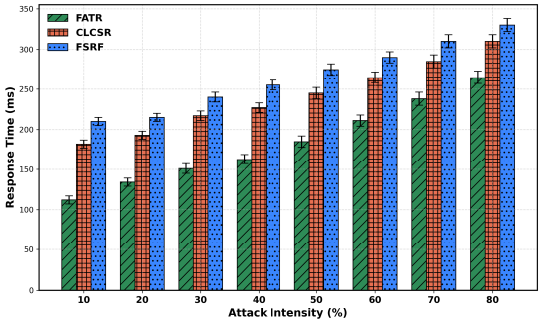
Figure 5: Attack resilience comparison of the proposed FATR framework with CLCSR and FSRF under varying network conditions.

In Fig. 6a,b, the FATR framework and existing approaches are evaluated across varying fog capacity and attack devices in terms of system response. The performance results have demonstrated significant improvements in system response over CLCSR and FSRF, by an average of 47% and 51%, respectively. It is due to the consideration of multiple parameters to identify reliable connections between peer devices and

to enhance the stability of IoT-based healthcare applications. In addition, the devices' lightweight-ness and history are considered when assessing their trustworthiness and reducing the risk of bottlenecks, thereby improving data flow in constrained IoT devices.



(**a**) Response time and capacity of fog node (10–50).



(**b**) Response time and attacker intensity (10%–80%).

Figure 6: Response time comparison of the proposed FATR framework with CLCSR and FSRF under varying network conditions.

5 Conclusion

Fog networks are rapidly utilised in many real-time systems for effective management of resources and timely response in a critical environment. The healthcare devices capture patient records and forward them to a processing platform for feedback from medical experts. The fog devices are placed closer to the source to reduce latency and improve response time when communicating with interacting devices. It not only balances resource consumption but also minimizes overheads in a constrained IoT-based environment. However, due to insecure channels and the presence of numerous malicious activities in an unpredictable network, many approaches fail to propose a trustworthiness solution and ultimately compromise sensitive information through disclosure. We introduce a fog-based framework to mitigate potential threats and optimize the healthcare network through efficient decision-making routing. The integration of a weighted-based trust aggregation model secures the IoT network against malicious threats and enhances the reliability of real-time communication. Moreover, lightweight methods minimize device energy consumption and help ensure a green network with an efficient anomaly-detection system. However, our proposed framework can protect network resources as malicious attacks increase in a distributed manner. In future work, we aim to explore deep learning techniques integrated with blockchain technology to reduce threat probabilities and enable seamless interactions and smarter disease identification.

Acknowledgement: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant No. (DGSSR-2025-02-01291).

Funding Statement: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant No. (DGSSR-2025-02-01291).

Author Contributions: Conceptualization, Maram Fahaad Almufareh, Mamoona Humayun; Formal analysis, Amr Munshi, Sadia Din; Methodology, Mamoona Humayun, Khalid Haseeb; Supervision, Mamoona Humayun, Maram Fahaad Almufareh; Validation, Sadia Din, Khalid Haseeb; Writing—original draft, Maram Fahaad Almufareh, Khalid Haseeb; Writing—review & editing, Mamoona Humayun, Amr Munshi. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: All data is available in the manuscript.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhang Y, Love DJ, Krogmeier JV, Anderson CR, Heath RW, Buckmaster DR. Challenges and opportunities of future rural wireless communications. IEEE Commun Mag. 2021;59(12):16–22. doi:10.1109/mcom.001.2100280.
2. An J, Debbah M, Cui TJ, Chen ZN, Yuen C. Emerging technologies in intelligent metasurfaces: shaping the future of wireless communications. IEEE Trans Antennas Propagat. 2025. doi:10.1109/tap.2025.3571069.
3. Ahmed B, Shuja M, Mishra HM, Qtaishat A, Kumar M. IoT based smart systems using artificial intelligence and machine learning: accessible and intelligent solutions. In: Proceedings of the 2023 6th International Conference on Information Systems and Computer Networks (ISCON); 2023 Mar 3–4; Mathura, India. p. 1–6. doi:10.1109/iscon57294.2023.10112093.
4. Uddin R, Koo I. Real-time remote patient monitoring: a review of biosensors integrated with multi-hop IoT systems via cloud connectivity. Appl Sci. 2024;14(5):1876. doi:10.3390/app14051876.
5. Williams P, Dutta IK, Daoud H, Bayoumi M. A survey on security in Internet of Things with a focus on the impact of emerging technologies. Internet Things. 2022;19(5):100564. doi:10.1016/j.iot.2022.100564.
6. Dang VA, Vu Khanh Q, Nguyen VH, Nguyen T, Nguyen DC. Intelligent healthcare: integration of emerging technologies and Internet of Things for humanity. Sensors. 2023;23(9):4200. doi:10.3390/s23094200.
7. Sabireen H, Neelanarayanan V. A review on fog computing: architecture, fog with IoT, algorithms and research challenges. ICT Express. 2021;7(2):162–76. doi:10.1016/j.icte.2021.05.004.
8. Chuan WC, Ul Arfeen Laghari S, Manickam S, Ashraf E, Karuppayah S. Challenges and opportunities in fog computing scheduling: a literature review. IEEE Access. 2025;13(3):14702–26. doi:10.1109/access.2024.3525261.
9. Alsahfi T, Badshah A, Aboulola OI, Daud A. Optimizing healthcare big data performance through regional computing. Sci Rep. 2025;15(1):3129. doi:10.1038/s41598-025-87515-5.
10. Amiri Z, Heidari A, Zavvar M, Navimipour NJ, Esmaeilpour M. The applications of nature-inspired algorithms in Internet of Things-based healthcare service: a systematic literature review. Trans Emerg Telecommun Technol. 2024;35(6):e4969. doi:10.1002/ett.4969.
11. Kong L, Tan J, Huang J, Chen G, Wang S, Jin X, et al. Edge-computing-driven Internet of Things: a survey. ACM Comput Surv. 2023;55(8):1–41. doi:10.1145/3555308.
12. Andriulo FC, Fiore M, Mongiello M, Traversa E, Zizzo V. Edge computing and cloud computing for Internet of Things: a review. Informatics. 2024;11(4):71. doi:10.3390/informatics11040071.
13. Rancea A, Anghel I, Cioara T. Edge computing in healthcare: innovations, opportunities, and challenges. Future Internet. 2024;16(9):329. doi:10.3390/fi16090329.
14. Alzu'bi A, Alomar A, Alkhaza'leh S, Abuarqoub A, Hammoudeh M. A review of privacy and security of edge computing in smart healthcare systems: issues, challenges, and research directions. Tsinghua Sci Technol. 2024;29(4):1152–80. doi:10.26599/tst.2023.9010080.
15. Alsabah M, Naser MA, Albahri AS, Albahri OS, Alamoodi AH, Abdulhussain SH, et al. A comprehensive review on key technologies toward smart healthcare systems based IoT: technical aspects, challenges and future directions. Artif Intell Rev. 2025;58(11):343. doi:10.1007/s10462-025-11342-3.
16. Islam MM, Nooruddin S, Karray F, Muhammad G. Internet of Things: device capabilities, architectures, protocols, and smart applications in healthcare domain. IEEE Internet Things J. 2023;10(4):3611–41. doi:10.1109/jiot.2022.3228795.
17. Almas A, Iqbal W, Altaf A, Saleem K, Mussiraliyeva S, Iqbal MW. Context-based adaptive fog computing trust solution for time-critical smart healthcare systems. IEEE Internet Things J. 2023;10(12):10575–86. doi:10.1109/jiot.2023.3242126.
18. Lin H, Han J, Wu P, Wang J, Tu J, Tang H, et al. Machine learning and human-machine trust in healthcare: a systematic survey. CAAI Trans Intell Technol. 2024;9(2):286–302. doi:10.1049/cit2.12268.

19. Hussain F, Abbas SG, Shah GA, Pires IM, Fayyaz UU, Shahzad F, et al. A framework for malicious traffic detection in IoT healthcare environment. Sensors. 2021;21(9):3025. doi:10.3390/s21093025.
20. Ibrahim M, Al-Wadi A, Elhafiz R. Security analysis for smart healthcare systems. Sensors. 2024;24(11):3375. doi:10.3390/s24113375.
21. Newaz AI, Sikder AK, Rahman MA, Uluagac AS. A survey on security and privacy issues in modern healthcare systems: attacks and defenses. ACM Trans Comput Healthc. 2021;2(3):1–44. doi:10.1145/3453176.
22. 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.
23. Bhatt K, Agrawal C, Bisen AM. A review on emerging applications of IoT and sensor technology for industry 4.0. Wirel Pers Commun. 2024;134(4):2371–89. doi:10.1007/s11277-024-11054-x.
24. Wang S, Ma T. A two-way trust-based routing approach to identify malicious and energy-aware nodes in fog computing. Clust Comput. 2025;28(7):460. doi:10.1007/s10586-025-05254-8.
25. Fotia L, Delicato F, Fortino G. Trust in edge-based Internet of Things architectures: state of the art and research challenges. ACM Comput Surv. 2023;55(9):1–34. doi:10.1145/3558779.
26. Trivedi HS, Patel SJ. Dynamically scalable privacy-preserving authentication protocol for distributed IoT based healthcare service providers. Wirel Netw. 2023;29(3):1385–409. doi:10.1007/s11276-022-03196-2.
27. Ali TE, Ali FI, Dakić P, Zoltan AD. Trends, prospects, challenges, and security in the healthcare Internet of Things. Computing. 2024;107(1):28. doi:10.1007/s00607-024-01352-4.
28. Nawaz A, Iqbal W, Altaf A, Almjally A, AlSagri H, Alabdullah B. CATcAFSMs: context-based adaptive trust calculation for attack detection in fog computing based smart medical systems. Expert Syst. 2025;42(2):e13687. doi:10.1111/exsy.13687.
29. Darabkh KA, Al-Mistarihi MF, Al-Maaitah MI. Next-gen eration routing for autonomous vehicle networks based on innovative clustering: integrating SDN and fog computing along with AODV upon failure. J Supercomput. 2025;81(2):379. doi:10.1007/s11227-024-06880-6.
30. Kore A, Patil S. Cross layered cryptography based secure routing for IoT-enabled smart healthcare system. Wirel Netw. 2022;28(1):287–301. doi:10.1007/s11276-021-02850-5.
31. Hossam HS, Abdel-Galil H, Belal M. An energy-aware module placement strategy in fog-based healthcare monitoring systems. Clust Comput. 2024;27(6):7351–72. doi:10.1007/s10586-024-04308-7.
32. Hameed FMH, Kurnaz S. An effective mechanism for FOG computing assisted function based on trustworthy forwarding scheme (IOT). Electronics. 2024;13(14):2715. doi:10.3390/electronics13142715.
33. Bhattacharya P, Mukherjee A, Bhushan B, Gupta SK, Gadekallu TR, Zhu Z. A secured remote patient monitoring framework for IoMT ecosystems. Sci Rep. 2025;15(1):22882. doi:10.1038/s41598-025-04774-y.
34. Hosseinzadeh M, Yoo J, Ali S, Lansky J, Mildeova S, Yousefpoor MS, et al. A fuzzy logic-based secure hierarchical routing scheme using firefly algorithm in Internet of Things for healthcare. Sci Rep. 2023;13(1):11058. doi:10.1038/s41598-023-38203-9.