Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.063077

ARTICLE

Integrating Edge Intelligence with Blockchain-Driven Secured IoT Healthcare Optimization Model

Khulud Salem Alshudukhi[1], **Mamoona Humayun**[2,*] and **Ghadah Naif Alwakid**[1]

[1]Department of Computer Science, College of Computer and Information Sciences, Jouf University, Sakaka, 72388, Saudi Arabia
[2]Department of Computing, School of Arts Humanities and Social Sciences, University of Roehampton, London, SW15 5PH, UK

*Corresponding Author: Mamoona Humayun. Email: mamoona.humayun@roehampton.ac.uk

Received: 04 January 2025; Accepted: 27 February 2025; Published: 16 April 2025

ABSTRACT: The Internet of Things (IoT) and edge computing have substantially contributed to the development and growth of smart cities. It handled time-constrained services and mobile devices to capture the observing environment for surveillance applications. These systems are composed of wireless cameras, digital devices, and tiny sensors to facilitate the operations of crucial healthcare services. Recently, many interactive applications have been proposed, including integrating intelligent systems to handle data processing and enable dynamic communication functionalities for crucial IoT services. Nonetheless, most solutions lack optimizing relaying methods and impose excessive overheads for maintaining devices' connectivity. Alternatively, data integrity and trust are another vital consideration for next-generation networks. This research proposed a load-balanced trusted surveillance routing model with collaborative decisions at network edges to enhance energy management and resource balancing. It leverages graph-based optimization to enable reliable analysis of decision-making parameters. Furthermore, mobile devices integrate with the proposed model to sustain trusted routes with lightweight privacy-preserving and authentication. The proposed model analyzed its performance results in a simulation-based environment and illustrated an exceptional improvement in packet loss ratio, energy consumption, detection anomaly, and blockchain overhead than related solutions.

KEYWORDS: Smart cities; load balancing; blockchain; health systems; edge computing

1 Introduction

The rapid development of smart cities using edge technologies brings forth a demand for managing IoT data and critical operations in real-time systems [1,2]. Wireless systems and next-generation IoT are combined in different ways for significant growth in healthcare systems [3,4]. Future sensing technologies [5,6] with IoT systems observe the targeted areas and ease the rapid data analysis for health operations [7,8]. Cloud-centric data processing models have struggled to meet such applications' dynamics, especially when balancing scalability with sustainability [9,10]. Despite advancements, several IoT-based healthcare applications rely on centralized cloud storage, vulnerable and ineffective for data breaches [11,12]. These systems often lack resilience and scalability research issues for large-scale architecture [13,14]. Consequently, due to the demands of end users, there is an increasing shift toward distributed architectures for healthcare systems with edge computing to ensure continuity and fault-tolerant communication [15–17]. In addition, establishing trust between constrained devices is another significant way to attain a reliable monitoring system and resource optimization. In smart cities, enhancing security is crucial for avoiding malicious traffic and preventing unauthorized access to sensitive data [18,19]. It can compromise the network infrastructure and disrupt essential services, thus adapting robust and secured measurement promotes resilient communication against attacks to guarantee a trustworthy environment [20,21]. The contributions of the proposed model are highlighted as follows:

i. It investigated stochastic routing techniques with multiple factors and network uncertainties to develop a recursive decision-making system for network optimization.
ii. It probed the blockchain transactions and intelligence of edges, with the lightweight role of validators for e-health data and effective communication cost.
iii. Designed a cooperative-driven trusted scheme for increasing the consistency and fault tolerance of connected e-health devices.

The research work is structured as follows. Section 2 presents related work. The proposed model is described in Section 3. Section 4 provides performance results. In the end, Section 5 concludes this research work.

2 Related Work

Edge computing with IoT systems has performed a crucial role in the growth of smart cities and sustainable development [22,23]. It enables seamless and timely interaction between wireless technologies by utilizing gateway devices and ensuring efficient communication in a real-time environment [24,25]. The rapid evolution of edge-driven processing systems, and autonomous IoT networks facilitate and support dynamic data analysis with learning techniques [26–28]. The environment continues monitoring the targeted data and forwards it to the cloud users based on their demands to attain a real-time surveillance system. The authors in [29] proposed an IoT network architecture for energy vehicles (EV) by using a data fusion technique based on fuzzy logic. The proposed data fusion algorithm considers human input from the crowd and sensory data and computes the location-specific congestion. Moreover, an open source routing (OSRM) determines the shortest congestion-aware route by reacting to the collected real-time traffic updates. Based on fuzzy logic, authors [30] developed a Trusted Routing Protocol for Vehicular Cloud Networks (FTRP), which constructs the protected paths for the delivery of data. A node candidacy value is computed using fuzzy logic and accordingly route is either selected or rejected. Cloud assigns a confidence score to each node based on the information it obtained from other nodes. In addition to analyzing multiple factors, the proposed approach computes the trust for selecting a secure route. A novel blockchain-based framework is proposed in [31] to guarantee data security and integrity for IoT systems. It comprised various phases and integrated with diverse security mechanisms for robust security in terms of privacy and data integrity. The experimental analysis of the proposed SecPrivPreserve revealed that its performance improved than existing studies. Authors [32] introduced an intelligent approach to determine the set of optimal border nodes by exploring the Lion Swarm Optimization algorithm (LSOA). The network area is divided into clusters and determines the set of border nodes within each cluster and associated inter-cluster communication. The main factors for finding the optimal border nodes are maximum energy and minimum distance. Later, a routing mechanism is generated based on the selection of optimal border nodes. Fuzzy logic-based secure hierarchical routing scheme is proposed [33] by utilizing the firefly algorithm (FSRF). It is developed for IoT-based healthcare systems and is composed of three main frameworks. To evaluate the trust, a fuzzy logic-based trust framework is presented that tackles with different routing attacks. In addition, using various metrics, the proposed framework supports the clustering of IoT devices and identifies the effective cluster head nodes. Moreover, FSRF provides an on-demand routing framework to attain consistent and energy-efficient routes for data transmission. Authors [34] integrate software-defined networking (SDN) and blockchain technology to cope with energy efficiency and security research obstacles. 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. Authors [35] proposed a security strategy for the detection and prevention of forwarding attacks from healthcare IoT systems, and composed of five phases. Initially, a topology is developed for finding the cluster heads and discovering the best route. In addition, to identify the selective forwarding attacks, the proposed solution performed packet validation based on the details of transmitted and received packets. Table 1 presents a benchmarking comparison of existing solutions alongside our proposed model.

Table 1: Benchmarking of existing solutions and proposed model

	Highlighted discussion
Related work	Healthcare applications face critical research challenges for real-time data analysis and processing. These challenges include the need for network optimization, scaling IoT systems with minimal overhead, and ensuring data trust between constrained healthcare devices by using adaptive wireless technologies. Sustainable development demands scalable and dynamic routing solutions to balance network traffic in e-health systems, reducing network emissions. Additionally, reliable solutions must incorporate appropriate security policies to ensure protected and authentic data sharing while developing a resilient and fault-tolerant healthcare system.
Proposed model	Unlike most of the existing work, our proposed methodology is composed of optimized stochastic techniques with multiple IoT healthcare systems. The generated decisions provide intelligence for constraint devices and also validate the health data before central computing. Integrated blockchain technology offers a trusted and reliable connection between e-health devices.

3 Proposed Model

This section proposes a model for addressing the research challenges that are demanded in healthcare IoT applications. Our proposed model introduces resource optimization, enhancement in healthcare security, and lightweight processing of real-time data using intelligence of network edges. The following subsections describe the flow of the proposed model.

3.1 Overview and Workflow

The proposed model is composed of data preprocessing, blockchain-integrated security, and optimized trusted communication stages. All stages have their contribution to the development of smart healthcare systems using IoT systems.

i. Firstly, the main roles are provided by health sensors and edge nodes. Health sensors collect real-time patient data and send it to the nearest edge node. When received, edge nodes preprocess and lightweight artificial intelligence analytics are used to detect anomalies. Based on some routing metrics, the proposed model aggregates the data on a priority basis.
ii. Secondly, blockchain transactions are established by exploring preprocessed data, and edge devices perform the role of data validation. After the data verification, it is securely transmitted among smart contracts.
iii. In the end, optimal routes are determined with the support of stochastic models, as a result, the proposed healthcare model decreases the usage of energy consumption and enhances consistency. In

addition, using multi-factors, trust scores are also computed to maximize reliability and efficiency for medical devices.

Fig. 1 depicts the Sequential Stages of the proposed healthcare model using Blockchain-Enabled edge intelligence. It highlights the step-by-step interaction of processes to guarantee trusted, efficient, and optimized data management for healthcare applications. Moreover, the proposed model emphasizes the smooth coordination between network edges and blockchain nodes for attaining real-time and crucial healthcare services.

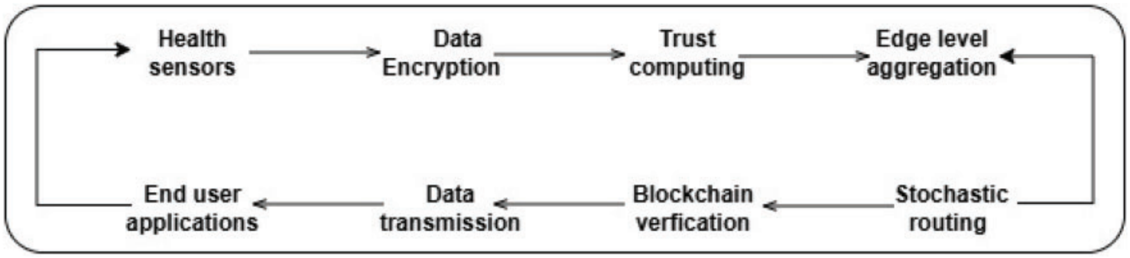


Figure 1: Sequential stages of the proposed healthcare blockchain–enabled edge intelligence model

3.2 Blockchain Integrated Scalable and Secured IoT-Healthcare

the proposed model is structured in the form of a weighted graph $G(V,E)$ with vertices V and edges E, where V denotes a set of sensors/edges, and E denotes a communication link. Initially, the health sensor h_S senses the patient's data P_d at regular intervals α, as given in Eq. (1).

$$P_d(i)(\alpha) = \{d_p(i), t_{Stamp}(i), P_{Sig}(i), Nc(i)\} \tag{1}$$

where:

- $d_p(i)$: Actual health data.
- $t_{Stamp}(i)$: Timestamp of data generation.
- $P_{Sig}(i)$: Digital signature using private key.
- $Nc(i)$: Nonce for the uniqueness of healthcare.

Before data aggregation at edge nodes, each sensor needs to compute its trust factor trt using quality QL and reliability RE scores, as defined in Eq. (2). In case, any sensor generates faulty data, then it reflects the trust score and decreases its trustworthiness in the data aggregation process.

$$trt(i) = \beta_1 \cdot QL + \beta_2 \cdot RE \tag{2}$$

where:

- β_1 and β_2 are weighted factors with uniform contributions.
- QL: Quality score
- RE: Reliability score

Eq. (3) uses packets latency P_{len} with prefixed threshold $Pre_{threshold}$ to compute QL. In case, communication incurs lower latency, it results in better network performance in terms of QL.

$$QL = 1 - \frac{P_{len}^{k}}{Pre_{threshold}} \tag{3}$$

RE is inversely proportional to communication disruption. Its evaluation is based on link failure Lnk^f and devices' request Com^r using Eq. (4).

$$RE = \frac{Packets(Lnk)^f}{(Dev)^r} \tag{4}$$

After each sensor computes the trust factor, IoT edge devices perform the data aggregation AG_D function along with the trusted factors defined in Eq. (5).

$$AG_D(ED) = \sum_{i=1}^{N} Trt(i) \cdot D(i) \tag{5}$$

Edge nodes create blockchain transactions TR and store the aggregated data of sensor i using time stamp $Time_S$ and other related information, as defined in Eq. (6).

$$TR = \{ID_i, AG_D(i), Time_S(i), P_{Sig}(i)\} \tag{6}$$

It ensures that the recorded transaction log can be modified and affects its integrity due to the decentralized behavior. Eq. (7) determines the efficiency of the blockchain based on the block rate BR and volume of transactions VT. The blockchain transaction's validation can be computed using Eq. (8), where the hash value is compared with a predefined threshold.

$$D_{\text{blockchain}} = \frac{VT}{BR} \tag{7}$$

$$(TR_i) = \begin{cases} 1 & if H(TR_i) \leq TR_{thres} \\ 0 & otherwise \end{cases} \tag{8}$$

In the next phase, the stochastic cost $SC(i, j)$ is analyzed for healthcare routing by utilizing multiple factors such as latency $L_{i,j}$, and trust score $Trt_{i,j}$ as given in Eq. (9). Based on the computed stochastic cost $SC(i, j)$, the proposed model establishes an optimal total cost multi-hop route R OTC_R from health sensors i to j as given in Eq. (10).

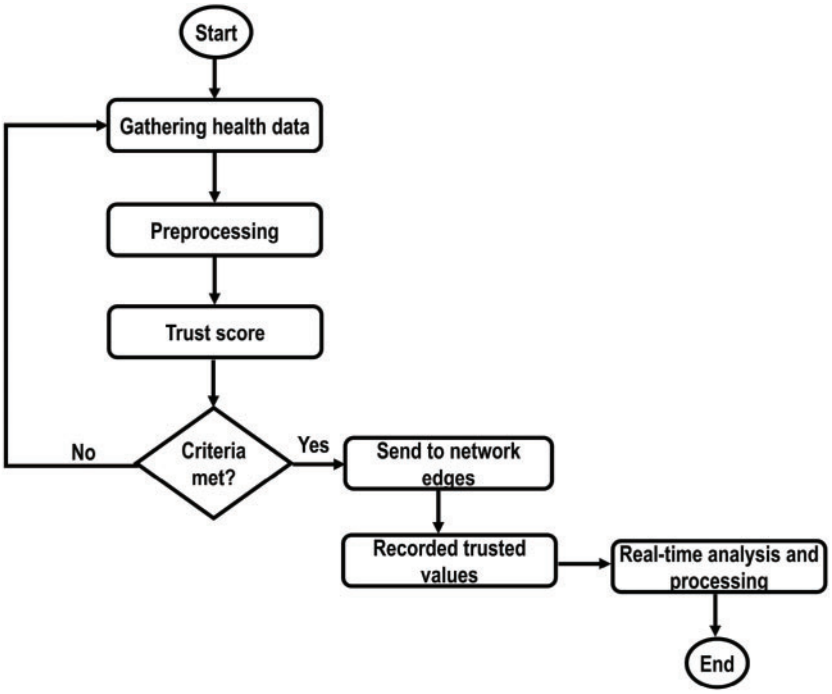
$$SC(i, j) = L_{i,j} + Trt_{i,j} \tag{9}$$

$$OTC_R = \sum_{e_{ij} \in R} SC(i, j) \cdot R(e_{ij}) \tag{10}$$

In the healthcare system, due to the patients' sensitive data, the proposed model makes use of homomorphic encryption at the edges for further processing without decryption. Let us consider that d_i and d_j are collected data, then multiplicative homomorphic encryption using key k can be computed as defined in Eq. (11).

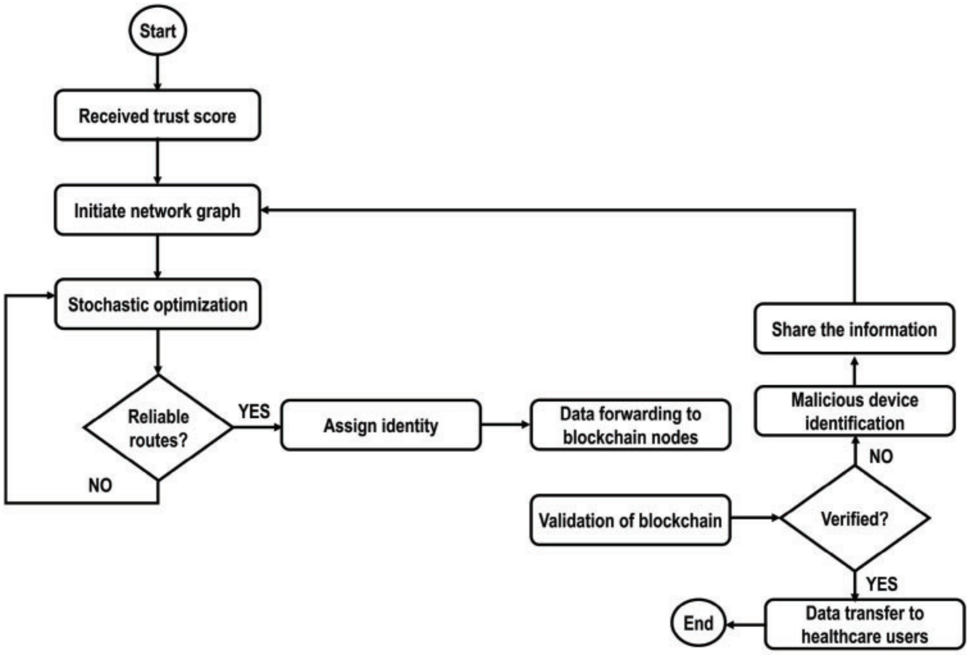
$$En(d_i \cdot d_j) = E_k(d_i) \cdot E_k(d_j) \tag{11}$$

Fig. 2a,b depicts the flowcharts of the proposed model for the healthcare system using optimized, trusted, and blockchain-driven validation. It initiates the process of collecting e-health records from medical sensors, and after preprocessing the trust scores are computed to attain a reliable healthcare system. Later, trusted data is transmitted to edges for further analysis. Moreover, the stochastic optimization criteria are explored based on multiple parameters, and it balances the energy consumption of the health sensors with the least interruption in communication. The blockchain nodes are integrated into the transaction, and before sending the sensitive data to health users, the validation process is applied to extract the trustworthiness of forwarders. In case, malicious devices are found in blockchain transactions, then information is flooded in the network and routes are reformulated using stochastic criteria based on network conditions. Algorithm 1 optimizes the routes for health sensors using stochastic computing based on trust score and latency factors. It is designed to address the unique research challenges for healthcare applications due to the constraints of resources. Unlike many existing studies, this iterative practice selects the most efficient routes using lightweight probabilistic techniques methods to enhance the decision-making for prioritizing communication links while tacking privacy preserving of health data. It refines the routes for transmitting health data by evaluating the network conditions.



(a) Edge computing with integrated trust-aware healthcare routing system.

Figure 2: (Continued)



(b) Stochastic-based optimization with Blockchain-driven e-health data validation

Figure 2: Flowchart of the proposed healthcare model: (**a**) Edge-integrated trusted healthcare system. (**b**) Stochastic-based optimization with blockchain-driven e-health data validation

Algorithm 1: Stochastic routing optimization for healthcare network

```
Input: IoT sensors data $\{D_i\}$, edge node set $\{ED\}$.
Output: Optimal end-to-end route $\{R\}$.
Initialize routing paths set $P \leftarrow \varnothing$.
for each sensor node $i$ do
    Calculate stochastic cost $SC(i)$ based on latency and trust score.
    Update potential paths $P$ by considering the least-cost paths.
    Select the optimal path $OTC_R$.
end for
return optimal path $OTC_R$.
```

Algorithm 2 illustrates the integration process of health records for the sensors in blockchain ledgers. It guarantees privacy and security by establishing the transactions, and edge devices verify each transaction for onward processing and computation. The proposed model validates the blockchain nodes and ensures tamper-free and reliable communication even with malicious devices. As a result, the health system provides more authentic and consistent data-exchanging solutions over untrusted communication channels. In contrast to much existing healthcare IoT solutions, the design of the proposed algorithm ensures the validation of the transactions by computing trust scores and digital signatures. It provides a secure method for the inclusion of only authentic and trusted data into the blockchain.

Algorithm 2: Blockchain-based secure data transmission

```
Input: Encrypted IoT sensor data $\{Enc(D_i)\}$, blockchain transaction $TR$, and trust scores $trt$.
Output: Verified data on blockchain.
for each encrypted patient data $Enc(d_i)$ do
    Generate a blockchain transaction using $TR = \{ID_i, AG\_D(i), Time\_S(i), P_{Sig}(i)\}$.
    Verify transaction $TR$.
    Integrate transactions $TR$ to the blockchain.
    if transaction is valid then
        Authenticated transaction.
    else
        Ignore the transaction and notify the neighbors.
    end if
end for
return verified blockchain contracts.
```

Algorithm 3 computes trust scores for IoT sensors based on their reliability, energy consumption, and data quality. It dynamically updates these scores and adjusts communication routes, ensuring secure and optimized data transmission in the network. By leveraging blockchain technology in the proposed model, it validates and authenticates the encrypted data with unique identifiers, signatures, and timestamps. It provides integrity of health data and authentic transactions are not processed. Moreover, due to the robust methods, the routing nodes are timely informed about the compromised information increasing the fault tolerance of the IoT system. Table 2 illustrates the developed features of proposed algorithms for the trustworthiness and optimization of healthcare systems.

Algorithm 3: Trusted and secured computation for healthcare-IoT sensors

```
Input: Sensor data $\{d_i\}$, weight coefficients $\{\beta_1, \beta_2\}$, trust scores $trt$.
Output: optimized and secured routes for e-health records.
for each sensor node $i$ do
    Compute aggregated data $AG_D(ED) = \sum_{i=1}^{N} Trt(i) \cdot D(i)$.
    Calculate an initial trust score $Trt$ using reliability and data quality.
    Update the trust score $TS_i$ using additional factors.
    Homomorphic encryption for sensitive health records.
end for
return updated trust scores and optimized secured e-health routes.
```

Table 2: Developed features of proposed model for securing and intelligent healthcare system

Feature	Resource optimization	Mitigation against attacks
Edge weights	Multi-factors for route selection	Prioritizes paths based on trust scores
Stochastic decision-making	Route selection with minimal cost	Enhances fault tolerance and reliability
Trust computing	Assigns trust scores and prioritize the routes	Detects low-trusted nodes for reliability

(Continued)

Table 2 (continued)

Feature	Resource optimization	Mitigation against attacks
Security enforcement	Ensures data encryption and authenticates nodes	Prevents unauthorized access and ensures privacy
Data integrity	Records logs for blockchain transactions	Protects against tampering
Decentralized trust management	Utilizes blockchain nodes and authenticates the aggregated data	Enhances security by avoiding single-point failures

4 Simulations and Results

In this section, we evaluate the performance of the proposed model with related work through simulations. The testing environment is created in NS-3 and scripting files are used to observe the behavior of the network. The collected data from health sensors are securely transmitted through a combination of blockchain transactions and maintain privacy and data integrity. The edges are responsible for resource management, data encryption, trust evaluation, and blockchain validation. The network field is fixed to 5000 m × 5000 m, populated by 50 to 200 health sensors, with 2j of initial energy level. 35 edge devices are deployed for the support of data aggregation and validation. To evaluate the real-world applicability of the proposed model, Table 3 depicted the varied key parameters.

Table 3: Simulation parameters

Parameter	Value
Simulation area	5000 m × 5000 m
Number of edge devices	35
Initial energy	2j
Number of sensors	50 to 200
Transaction rate	10–50 TPS
Simulations run	50
β_1, β_2	0.5, 0.5
Probability of link failure	0.1 to 0.3

The evaluation of the packet drop ratio for the proposed model and existing solutions under varying transmission rates and bandwidth is depicted in Fig. 3a,b. The experimental results illustrate that the proposed model outperforms existing approaches by an average of 33% and 38%. It employs the concept of edge computing and intelligent route identification while attaining reliable communication channels for the healthcare system. Robust decision-making using stochastic optimization also decreases the chances of network disruption and enhances resource optimization in e-health operations. Furthermore, various parameters are re-computed to balance the load on the transmission links with efficient traffic distribution on the constraint devices. Additionally, edges are mobile and crucial components of the proposed model, they intelligently collected the IoT aggregated data and decreased the transmission distance with effective trust management. Moreover, the security analysis is another significant stage of the proposed model, it reduces the communication threats and provides more trustworthiness forwarding based on blockchain transactions.

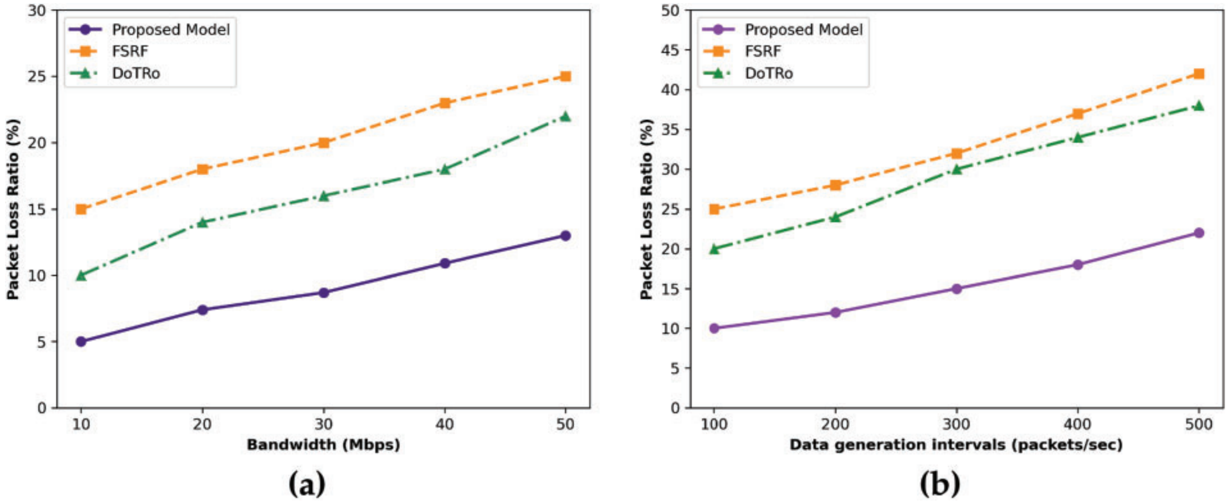


Figure 3: Performance of proposed model and related approaches for packet drop ratio for data generation rate and bandwidth

The proposed model's experimental results compared to the existing solution are illustrated in Fig. 4a,b. The proposed model balances resource consumption and node congestion to optimize sensor performance with the use of distributed computing, which is based on multi-facet analysis. It was noticed that the proposed model increases the energy efficiency by an average of 41% and 52% under different transmission rates and bandwidths, owing to the selection of several criteria parameters by exploring network conditions. The network edges not only limit the transmission power of the health sensors but also eliminate congested and faulty links for data transmission. Accordingly, the next-hop is more reliable and consistent for continuous routing and offers high performance in e-health data delivery. The routing paths are continuously updated by identifying nearby trustworthy neighbors based on the trust scores, and enhancing the routes' lifetime while decreasing traffic load on network-wide IoT devices. In addition, routes are authenticated using blockchain integration and marked as infectious entries incurred during data transmission.

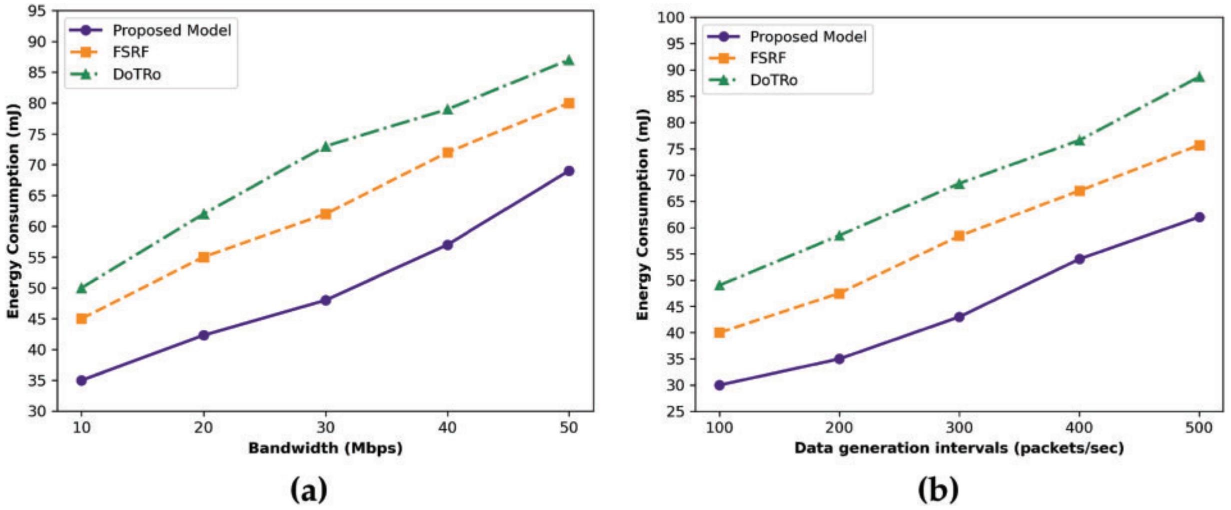


Figure 4: Performance of proposed model and related approaches for energy consumption for data generation rate and bandwidth

Compared to existing solutions, the proposed model improves the computational time for varying the data generation rate and bandwidth by an average of 38% and 46%, as illustrated in Fig. 5a,b. This is because forwarding routes are re-evaluated at both the device and edge level. In case, any device in the route is malicious, the entire route is labeled as faulty, and the route is reformulated for transmission of e-health records. In addition, mobile edges perform a crucial role in the identification of faulty channels based on trust and blockchain integration. It copes to identify the unauthentic devices on the medium and avoid the keys or resending the fake route requests. If any channel closer to the edge device is suspicious, then the edge device announces alarming messages to inform the neighbors that fall in its proximity. In such cases, the proposed algorithm effectively manages the communication cost and latency rate.

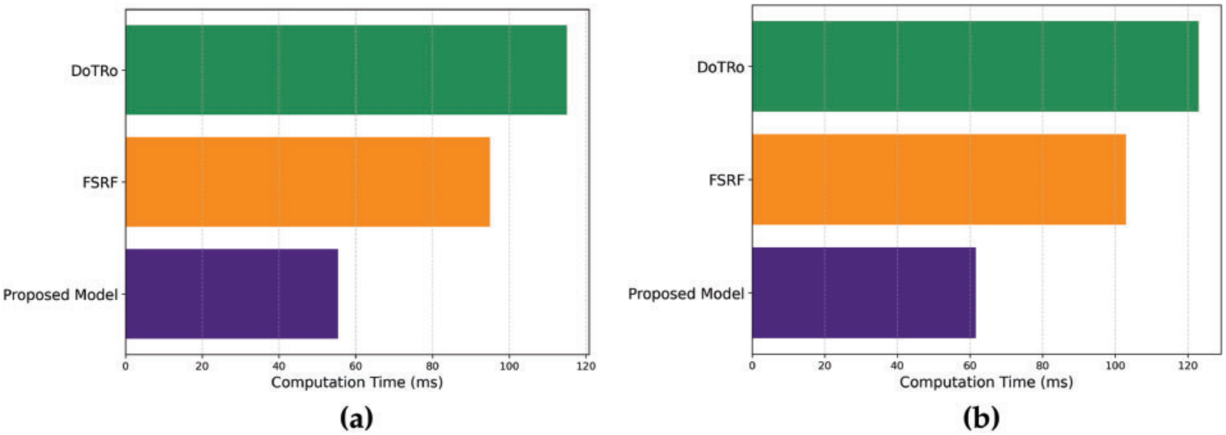


Figure 5: Performance of proposed model and related approaches for computation time for data generation rate and bandwidth

In Fig. 6a,b, the performance evaluation of the proposed model is compared with existing solutions in terms of blockchain overhead. Based on the results, it was noticed that performance results improved for varying data generation rate and bandwidth by an average of 45% and 49% by utilizing a more reliable anomaly detection mechanism using integration of lightweight blockchain computation. Moreover, the support of network edges along with the lightweight cryptographic methods, dynamic thresholds, and validation patterns, ensure the proposed model for efficiently detecting misclassification of normal data traffic as communication threats. Unlike existing work, this strategy enables the optimal usage of network resources and prevents additional blockchain overhead caused by false positives. Consequently, the proposed model reduces the chances of false alerts and offers more trustworthiness in blockchain-based security mechanisms for crucial healthcare systems.

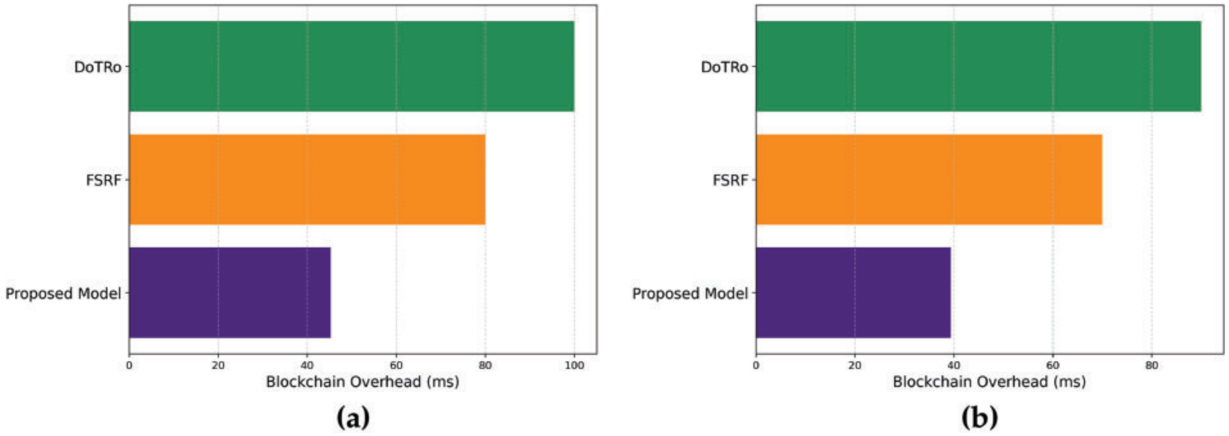


Figure 6: Performance of proposed model and related approaches for blockchain overhead for packet generation rate and bandwidth

5 Conclusion

Smart cities are interconnected using advanced network technologies and intermediate wireless services to observe the unpredicted environment. In crucial applications, the bounded limitation of sensors, IoT gateways, etc., are not enough to provide an earlier response in the decision-making process and raise significant challenges for network optimization. In addition, the security of distributed systems also poses another research issue in attaining data preservation and authentication. This work presents a blockchain-driven secured and load-balanced routing model for health applications with efficient data flow supported by edge intelligence. It leads to a lightweight communication system using stochastic optimization and enhances trustworthiness between connected devices despite network threats. Moreover, the proposed model secures the exchange of IoT data using integrated blockchain transactions and reduces the probabilities of anomalous behaviors. However, to enhance the robustness of the proposed model, adaptive resource allocation algorithms with lightweight encryption techniques are demanded to decrease the computing load on low-powered devices.

Acknowledgement: The authors would like to thank the support by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant No. (DGSSR-2024-02-02090).

Funding Statement: This work was funded by the Deanship of Graduate Studies and Scientific Research at Jouf University under grant No. (DGSSR-2024-02-02090).

Author Contributions: The authors confirm contribution to the paper as follows: Conceptualization: Khulud Salem Alshudukhi, Mamoona Humayun; methodology: Khulud Salem Alshudukhi, Mamoona Humayun; software: Ghadah Naif Alwakid; validation: Ghadah Naif Alwakid, Mamoona Humayun; formal analysis: Ghadah Naif Alwakid; investigation: Mamoona Humayun, Ghadah Naif Alwakid; resources: Khulud Salem Alshudukhi; data curation, Mamoona Humayun; writing—original draft preparation: Khulud Salem Alshudukhi, Mamoona Humayun; writing—review and editing: Ghadah Naif Alwakid; visualization: Ghadah Naif Alwakid; supervision: Mamoona Humayun; project administration: Khulud Salem Alshudukhi, Ghadah Naif Alwakid; funding acquisition: Khulud Salem Alshudukhi, Mamoona Humayun. 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. Alahi MEE, Sukkuea A, Tina FW, Nag A, Kurdthongmee W, Suwannarat K, et al. Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends. Sensors. 2023;23(11):5206. doi:10.3390/s23115206.
2. Hussain I, Elomri A, Kerbache L, El Omri A. Smart city solutions: comparative analysis of waste management models in IoT-enabled environments using multiagent simulation. Sustain Cities Soc. 2024;103(6):105247. doi:10.1016/j.scs.2024.105247.
3. Ahad A, Jiangbina Z, Tahir M, Shayea I, Sheikh MA, Rasheed F. 6G and intelligent healthcare: taxonomy, technologies, open issues and future research directions. Internet Things. 2024;25(7):101068. doi:10.1016/j.iot.2024.101068.
4. Nissar G, Khan RA, Mushtaq S, Lone SA, Moon AH. IoT in healthcare: a review of services, applications, key technologies, security concerns, and emerging trends. Multimed Tools Appl. 2024;83(33):80283. doi:10.1007/s11042-024-18580-7.
5. Krishnamoorthy S, Dua A, Gupta S. Role of emerging technologies in future IoT-driven Healthcare 4.0 technologies: a survey, current challenges and future directions. J Ambient Intell Humaniz Comput. 2023;14(1):361–407. doi:10.1007/s12652-021-03302-w.
6. Morchid A, El Alami R, Raezah AA, Sabbar Y. Applications of internet of things (IoT) and sensors technology to increase food security and agricultural sustainability: benefits and challenges. Ain Shams Eng J. 2024;15(3):102509. doi:10.1016/j.asej.2023.102509.
7. Alotaibi A, Barnawi A. Securing massive IoT in 6G: recent solutions, architectures, future directions. Internet Things. 2023;22(1):100715. doi:10.1016/j.iot.2023.100715.
8. Benlloch-Caballero P, Wang Q, Calero JMA. Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. Comput Netw. 2023;222(2):109526. doi:10.1016/j.comnet.2022.109526.
9. Hazra A, Rana P, Adhikari M, Amgoth T. Fog computing for next-generation internet of things: fundamental, state-of-the-art and research challenges. Comput Sci Rev. 2023;48(5):100549. doi:10.1016/j.cosrev.2023.100549.
10. Ahmad T, Madonski R, Zhang D, Huang C, Mujeeb A. Data-driven probabilistic machine learning in sustainable smart energy/smart energy systems: key developments, challenges, and future research opportunities in the context of smart grid paradigm. Renew Sustain Energ Rev. 2022;160(1):112128. doi:10.1016/j.rser.2022.112128.
11. Heng L, Yin G, Zhao X. Energy aware cloud-edge service placement approaches in the Internet of Things communications. Int J Commun Syst. 2022;35(1):e4899. doi:10.1002/dac.4899.
12. Poojara SR, Dehury CK, Jakovits P, Srirama SN. Serverless data pipeline approaches for IoT data in fog and cloud computing. Future Gener Comput Syst. 2022;130(8):91–105. doi:10.1016/j.future.2021.12.012.
13. Prokhorenko V, Babar MA. Architectural resilience in cloud, fog and edge systems: a survey. IEEE Access. 2020;8:28078–95. doi:10.1109/ACCESS.2020.2971007.
14. Alsadie D. Artificial intelligence techniques for securing fog computing environments: trends, challenges, and future directions. IEEE Access. 2024;12(4):151598–648. doi:10.1109/ACCESS.2024.3463791.
15. Golpayegani F, Chen N, Afraz N, Gyamfi E, Malekjafarian A, Schäfer D, et al. Adaptation in edge computing: a review on design principles and research challenges. ACM Trans Auton Adapt Syst. 2024;19(3):1–43. doi:10.1145/3664200.
16. 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 Tutor. 2022;25(1):591–624. doi:10.1109/COMST.2022.3218527.
17. Rana B, Singh Y, Singh PK, Hong WC. A priority based energy-efficient metaheuristic routing approach for smart healthcare system (SHS). IEEE Access. 2024;12:85694–708. doi:10.1109/ACCESS.2024.3411564.
18. Haseeb K, Alzahrani FA, Siraj M, Ullah Z, Lloret J. Energy-aware next-generation mobile routing chains with fog computing for emerging applications. Electronics. 2023;12(3):574. doi:10.3390/electronics12030574.

19. Haque AB, Bhushan B, Dhiman G. Conceptualizing smart city applications: requirements, architecture, security issues, and emerging trends. Expert Syst. 2022;39(5):e12753. doi:10.1111/exsy.12753.
20. 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.
21. Berger C, Eichhammer P, Reiser HP, Domaschka J, Hauck FJ, Habiger G. A survey on resilience in the iot: taxonomy, classification, and discussion of resilience mechanisms. ACM Comput Surv. 2021;54(7):1–39.
22. Xue H, Chen D, Zhang N, Dai HN, Yu K. Integration of blockchain and edge computing in internet of things: a survey. Future Gener Comput Syst. 2023;144(1):307–26. doi:10.1016/j.future.2022.10.029.
23. Rahmani AM, Tanveer J, Gharehchopogh FS, Rajabi S, Hosseinzadeh M. A novel offloading strategy for multi-user optimization in blockchain-enabled mobile edge computing networks for improved internet of things performance. Comput Electr Eng. 2024;119(2):109514. doi:10.1016/j.compeleceng.2024.109514.
24. Xu M, Ng WC, Lim WYB, Kang J, Xiong Z, Niyato D, et al. A full dive into realizing the edge-enabled metaverse: visions, enabling technologies, and challenges. IEEE Commun Surv Tutor. 2022;25(1):656–700. doi:10.1109/COMST.2022.3221119.
25. Tripathi A, Singh AK, Choudhary P, Vashist PC, Mishra K. Significance of wireless technology in Internet of Things (IoT). In: Machine learning and cognitive computing for mobile communications and wireless networks. Scrivener Publishing LLC. 2020;131–54. doi:10.1002/9781119640554.ch6.
26. Firouzi F, Farahani B, Marinšek A. The convergence and interplay of edge, fog, and cloud in the AI-driven Internet of Things (IoT). Inf Syst. 2022;107(12):101840. doi:10.1016/j.is.2021.101840.
27. Yan W, Wang Z, Wang H, Wang W, Li J, Gui X. Survey on recent smart gateways for smart home: systems, technologies, and challenges. Trans Emerg Telecomm Technol. 2022;33(6):e4067. doi:10.1002/ett.4067.
28. Haseeb K, Din IU, Almogren A, Ahmed I, Guizani M. Intelligent and secure edge-enabled computing model for sustainable cities using green internet of things. Sustain Cities Soc. 2021;68(6):102779. doi:10.1016/j.scs.2021.102779.
29. Rout RR, Vemireddy S, Raul SK, Somayajulu DV. Fuzzy logic-based emergency vehicle routing: an IoT system development for smart city applications. Comput Electr Eng. 2020;88(4):106839. doi:10.1016/j.compeleceng.2020.106839.
30. Kait R, Kaur S, Sharma P, Ankita C, Kumar T, Cheng X. Fuzzy logic-based trusted routing protocol using vehicular cloud networks for smart cities. Expert Syst. 2024;42(1):e13561. doi:10.1111/exsy.13561.
31. Padma A, Ramaiah M. Blockchain based an efficient and secure privacy preserved framework for smart cities. IEEE Access. 2024;12:21985–2002. doi:10.1109/ACCESS.2024.3364078.
32. Keshari SK, Kansal V, Kumar S, Bansal P. An intelligent energy efficient optimized approach to control the traffic flow in Software-Defined IoT networks. Sustain Energy Technol Assess. 2023;55(3):102952. doi:10.1016/j.seta.2022.102952.
33. 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.
34. 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 Serv Comput. 2020;13(4):625–38. doi:10.1109/TSC.2020.2966970.
35. Srinivas TAS, Manivannan S. Black hole and selective forwarding attack detection and prevention in IoT in health care sector: hybrid meta-heuristic-based shortest path routing. J Ambient Intell Smart Environ. 2021;13(2):133–56. doi:10.3233/AIS-210591.