Computers, Materials & Continua

Tech Science Press

https://doi.org/10.32604/cmc.2026.085763

ARTICLE

A Secure Blockchain-Enabled SDN-Based Edge Computing Framework for IoT Healthcare Systems

Vikas Tyagi[1,*], Mrinmoy Kayal[1], Arvind Prasad[2,*], Gauhar Ali[3], Sajid Shah[3] and Muhammad Asim[3]

[1]School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India
[2]Information Systems and Security, College of IT, United Arab Emirates University, Al Ain, United Arab Emirates
[3]EIAS Data Science and Blockchain Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia

*Corresponding Authors: Vikas Tyagi. Email: itengg.vikas@gmail.com; Arvind Prasad. Email: arvind@uaeu.ac.ae

Received: 18 May 2026; Accepted: 29 June 2026; Published: 15 September 2026

ABSTRACT: Healthcare systems based on the Internet of Things (IoT) are widely used in patient monitoring, telemedicine, emergency care, and hospital-at-home services. However, existing IoT healthcare networks still face major challenges related to security, trust management, network control, and real-time emergency data handling. Centralized trust mechanisms and repeated cloud-based verification may increase delay and reduce reliability in critical healthcare scenarios. Moreover, suspicious medical devices must be quickly isolated, while sensitive patient data and emergency traffic must be protected and prioritized. To address these issues, this work proposes a blockchain-enabled, software-defined networking (SDN)-based edge computing framework for IoT healthcare systems. The proposed architecture integrates blockchain for secure and distributed trust management, edge computing for low-latency processing, and an Open Network Operating System (ONOS)-based SDN control plane for emergency-aware flow management, dynamic traffic engineering, and policy-based medical traffic segmentation. The framework is evaluated against a recent blockchain-edge-cloud-SDN IoT baseline. The results show that the proposed framework reduces average jitter by **15.05%**, energy consumption by **6.10%**, and delay by **14.16%**, while improving packet delivery ratio by **6.85%** and throughput by **9.85%**. These results indicate that the proposed approach can provide more reliable, efficient, and secure communication for connected hospitals, intensive care unit (ICU) monitoring, ambulance telemetry, and home-based chronic care environments.

KEYWORDS: IoT healthcare; blockchain; software-defined networking; open network operating system controller; edge computing; smart contracts; medical Internet of Things

1 Introduction

The Internet of Things (IoT) has rapidly changed the way modern healthcare services are delivered. Technologies such as remote patient monitoring, connected bedside equipment, wearable devices, telemedicine platforms, emergency telemetry, and hospital-at-home systems are now becoming an essential part of smart healthcare. In practice, these environments involve a wide range of interconnected cyber-physical devices, including ECG sensors, glucose monitors, infusion pumps, pulse oximeters, smart beds, ambulance communication units, and clinician-side applications. While these devices significantly improve the quality, efficiency, and responsiveness of care, they also enlarge the attack surface of the healthcare ecosystem [1,2].

Securing healthcare IoT systems is more challenging than securing generic IoT deployments [3]. First, healthcare data are highly sensitive and subject to strict privacy and regulatory requirements. Second, access decisions in healthcare are rarely generic; they depend on patient context, clinical responsibility, user role, and treatment workflow. Third, healthcare traffic by nature is heterogeneous; as life-critical flows, such as those generated by alarms in ICUs, telemetry from ambulances, or other emergency messages, need to be prioritized far above routine administrative communication flows. Classical centralized approaches to identity authentication and static access control cannot cope with these needs; they often create single points of failure, entail cloud dependency with associated delays, and offer poor options for quick containment of potentially hostile devices while not affecting the operation of the healthcare facility.

It is precisely the technology trio of blockchain, edge computing, and software-defined networking (SDN) that can help solve these issues. Blockchain offers decentralized trust, a history of transactions that is immutable, and smart contracts that allow auditing and enforcing access control rules. What edge computing can offer in this combination is closer-to-device validation and decision making, thus reducing latency and ensuring continuity. As for SDN, it is capable of dynamic priority setting, segmentation, and applying policies to the traffic flowing through it. This research follows up on the line of blockchain combined with fog computing to establish device identity and prior research considering blockchain, edge/cloud computing, and SDN in IoT applications [4].

The main drive behind this research is the reliance on the use of networked devices for the provision of continuous monitoring, emergencies, telemedicine, and home-based health services. While the integration of such devices in the healthcare network improves the performance and real-time decision-making ability, it introduces significant risks to the security and management of the healthcare network, which include centralization of trust, repetitive authentication latency, static access behavior, and poor isolation of infected medical devices [5]. This issue becomes more pressing within healthcare since it is paramount that communication remains reliable, sensitive data stays confidential, and emergency traffic receives priority during communication. Therefore, the need to design a communication system that supports distributed trust, fast access validation, and flexible policy control has become increasingly evident. Based on this need, the current study suggests a blockchain-enabled SDN edge computing architecture for secure and auditable communications in IoT healthcare networks.

The main contributions of this work are summarized below:

- A healthcare-specific blockchain-enabled SDN-edge architecture is developed for connected hospitals, ICU monitoring, ambulance telemetry, wearable sensing, and home-based care. The architecture integrates the device plane, edge intelligence plane, blockchain trust plane, and ONOS-based SDN control plane to support trusted access, local validation, and programmable traffic enforcement.
- A formal access-control and forwarding model is presented to represent user–device–patient authorization, secure access delay, device trust, role compatibility, and emergency-priority forwarding in healthcare IoT communication.
- The permissioned blockchain component is refined as a smart-contract-based trust layer for registration, patient–device binding, role-policy mapping, token issuance, token revocation, and immutable audit logging. The design also explains consensus assumptions and smart contract complexity.
- The ONOS controller is employed as a healthcare-aware policy engine that converts validated trust decisions into enforceable network actions, including allow, restrict, prioritize, deny, and isolate rules for normal, emergency, and suspicious traffic.
- An end-to-end workflow and pseudo-code are provided to connect edge caching, blockchain validation, token handling, ONOS rule installation, and revocation/reconfiguration. The comparative evaluation further reports the expected gains against a blockchain–edge-cloud–SDN IoT baseline.

The remainder of this work is arranged in the following sections. Where, Section 2 presents the relevant literature. Section 3 presents the system model with its assumptions. Section 4 formulates the secure access problem mathematically by defining authorization, delay, optimization objectives, and operational constraints. Section 5 describes the proposed framework in detail, including the analytical architecture, operational workflow, pseudo-code representation, and ONOS-based policy realization. Section 6 presents the comparative performance evaluation and experimental analysis with respect to the baseline framework. Section 7 provides the discussion and limitations, and Section 8 presents the concluding remarks.

2 Related Work

Access control and authentication systems based on blockchain technology have gained significant interest in the field of Internet of Things (IoT) due to their ability to minimize reliance on centralized storage of credentials as well as provide secure logging of all security events. Christidis and Devetsikiotis [1] highlighted the critical role of blockchain technology and smart contracts for trust establishment within IoT networks, whereas Novo [2] focused on using blockchain for scalability issues related to IoT access control systems. Overall, the presented references suggest that blockchain technology offers promising opportunities not only for secure logging purposes but also for access control implementation. Lightweight blockchain-assisted authentication has also been explored in fog-supported and distributed service settings [6]. The thesis that motivates the present work followed this direction by using blockchain smart contracts and fog nodes for decentralized authentication and event logging.

Healthcare-focused fog and edge architectures have been proposed to support low-latency care delivery. Azimi et al. [7] presented hierarchical fog-assisted healthcare computing, and Rahmani et al. [8] described smart e-health gateways for healthcare IoT at the edge. More recent surveys indicate that combining blockchain with healthcare IoT can improve auditability, transparency, and trust while edge/fog layers improve response time and local processing efficiency [9–11]. SDN has also been widely studied for IoT security because of its ability to separate control and data planes and dynamically enforce policies. Kalkan and Zeadally [12] discussed IoT security with SDN, while Sharma et al. [13] proposed DistBlockNet to couple blockchain and SDN in IoT networks. More recent works have employed blockchain-SDN combinations for DDoS mitigation and orchestration in edge-cloud environments [14,15].

Recently, there have been a number of studies on the synergistic effect of utilizing blockchain, SDN, and edge/fog computing for enhancing cybersecurity in distributed IoT ecosystems. In particular, Sebbar et al. [16] suggested a blockchain-based secure architecture of SDN for multi-edge computing applications within an industrial IoT scenario, where the key emphasis was on protection of industrial services against cybersecurity threats while maintaining system scalability in the case of multi-edge deployments. The study is particularly interesting, since it proved that integrating blockchain-trusted decision-making and SDN-based network control can enhance the overall resiliency and coordination of IoT edge networks. At the same time, the proposed architecture focuses only on an industrial IoT use case, and its implementation does not cover healthcare-oriented aspects like patient-device role relations, traffic priority of emergency communications, and context-awareness for access control.

Another study by Lakhlef et al. [17] reviewed the current state of blockchain-enhanced SDN solutions for IoT and discussed a general potential of using these technologies together to enhance programmability, distributed management, and overall trust in IoT systems. It should be acknowledged that the study makes a significant strategic contribution, emphasizing the growing importance of blockchain-based management of IoT systems and their heterogeneity. Nevertheless, it remains primarily a strategic and discussion-oriented study rather than a healthcare-specific implementation framework. Domain-specific contributions include those made by Kilani et al. [18], which proposed an architecture that provides for a secure multi-edge

computing solution for industrial IoT, leveraging blockchain and SDN. While similar to the contributions discussed above in terms of combining decentralization and programmable network management in order to ensure greater protection, the architecture focuses specifically on the needs of industrial IoT, failing to account for specific requirements such as ensuring constant medical service availability, strictly adhered-to role-based access policies, and delay-restricted routing of critical telemetry information.

The paper written by Kaur et al. [19] brought even more relevance to the discussion since it proposed a security framework specifically for healthcare fog computing, leveraging zero trust, blockchain, and SDN. As evidenced by the authors' focus on the specifics of medical data and its need for continuous authentication and anomaly detection, as well as the fact that fog-assisted healthcare systems require timely and seamless execution of tasks, the research provides valuable insights into the use of blockchain and SDN in a fog environment. Nevertheless, the authors focused on zero-trust fog security and task scheduling rather than on an actual healthcare IoT access control system using ONOS.

Another closely related contribution is the BLEDGE-SDN framework by Paliwal et al. [20], which integrates blockchain and edge-cloud-enabled SDN to secure networks and IoT devices. This study is relevant because it shows how distributed trust and edge-cloud coordination can be used to strengthen network and device security in cyber-physical settings. Yet, like most general-purpose IoT security frameworks, it focuses on securing networked IoT devices at a broad level and does not explicitly model healthcare-specific communication semantics, emergency service prioritization, or ONOS-guided medical traffic control. These limitations across the existing literature motivate the need for the present work, which brings together blockchain-based trust, edge-assisted validation, and healthcare-aware SDN enforcement in a single integrated framework.

Recent studies also show that blockchain is increasingly being combined with artificial intelligence (AI), digital twins, and device-level trust modeling to support trustworthy data orchestration in smart interconnected ecosystems. AI-assisted trust scoring can help identify anomalous devices and suspicious access behavior, while digital-twin-based representations can mirror physical IoT devices and support predictive validation before enforcing network changes. In healthcare IoT, these ideas are useful because access decisions should not depend only on static credentials; they should also consider device behavior, patient context, service criticality, and the reliability of sensed data. Therefore, the present work positions blockchain as the auditable trust layer, edge computing as the local validation layer, and ONOS-based SDN as the enforcement layer for translating trust decisions into network policies.

Another similar baseline for this research can be Medhane et al.'s paper [21] where blockchain, edge cloud, and SDN technologies were combined to enhance security and privacy in the next generation of IoT. According to their research, packet delivery ratio, throughput, and delay have been observed to perform better when blockchain, edge cloud, and SDN technologies are utilized collectively as compared to being isolated from each other. However, once more, the scope of the research remains confined to the general IoT security and privacy issue. The role of the device, identity context, and emergency traffic management using ONOS are some of the issues that cannot be addressed by this study. Table 1 provides an overview of the most relevant papers analyzed in this study based on their goals, advantages, and disadvantages. From this analysis, it can be seen that although there were many attempts to investigate each of the components mentioned above individually, there was no research that considered all three of them together in a single framework.

Table 1: Comparative summary of related work.

Author with Ref.	Objective	Advantages	Limitations
Christidis and Devetsikiotis [1]	To examine the use of blockchain and smart contracts for trust management in IoT.	Established blockchain as a strong mechanism for decentralized trust and immutable logging.	Limited to general IoT trust; did not address healthcare-specific access control, edge validation, or SDN policy enforcement.
Novo [2]	To develop scalable blockchain-based access management for IoT systems.	Demonstrated decentralized and scalable access-control management in distributed IoT environments.	Focused mainly on access-control scalability; lacked healthcare context and emergency-aware communication support.
Yao et al. [4]	To provide blockchain-assisted lightweight anonymous authentication for distributed fog services.	Improved privacy, lightweight authentication, and distributed service support.	Targeted generic distributed services rather than medical IoT workflows and healthcare traffic priorities.
Kaur et al. [6]	To design a lightweight blockchain-assisted authentication mechanism in fog-supported environments.	Reduced dependence on centralized authentication and supported distributed trust validation.	Did not consider healthcare-specific patient-device-role binding or ONOS-based traffic enforcement.
Azimi et al. [7]	To propose a hierarchical fog-assisted computing architecture for healthcare IoT.	Improved healthcare service responsiveness by moving computation closer to devices.	Did not integrate blockchain trust management or SDN-based network policy realization.
Rahmani et al. [8]	To develop smart e-health gateways for edge-assisted healthcare IoT.	Enhanced localized processing, service continuity, and low-latency healthcare support.	Lacked decentralized trust, immutable auditability, and programmable SDN enforcement.
Rahman et al. [9]	To survey blockchain-based IoT eHealthcare applications and challenges.	Provided broad insights into trust, transparency, and auditability in healthcare IoT.	Survey-only study; no concrete integrated framework with edge validation and ONOS control.
Kamruzzaman et al. [10]	To discuss the role of blockchain and fog computing in IoT healthcare systems.	Highlighted the joint benefits of decentralized trust and low-latency computing.	Did not provide a complete operational architecture or healthcare-specific SDN control strategy.
Allam et al. [11]	To review IoT-based eHealth systems using blockchain.	Summarized major opportunities of blockchain in secure and auditable healthcare communication.	Review-focused; no unified framework covering authentication, edge validation, and ONOS enforcement.
Kalkan and Zeadally [12]	To study how SDN can improve IoT security.	Showed that SDN supports adaptive access control, traffic monitoring, and programmable security.	Did not include blockchain support, healthcare-specific context, or patient-aware identity semantics.

(Continued)

Table 1 (continued)

Author with Ref.	Objective	Advantages	Limitations
Sharma et al. [13]	To integrate blockchain and SDN for secure IoT networking.	Demonstrated the value of combining distributed trust with programmable network control.	Focused on generic IoT architecture and not on healthcare-specific access semantics or emergency traffic control.
Jmal et al. [14]	To use blockchain-SDN integration for attack mitigation in IoT.	Improved adaptive attack handling and controller-driven protection.	More focused on attack detection than on healthcare-aware authentication and medical traffic enforcement.
Núñez-Gómez et al. [15]	To orchestrate fog computing environments using blockchain and SDN.	Improved orchestration efficiency and domain-level control in fog-supported systems.	Did not address healthcare-specific identity binding, emergency prioritization, or patient-device relationships.

Note: This table summarizes the objective, strengths, and limitations of the most relevant studies and highlights the gap addressed by the proposed healthcare-oriented framework.

Digital twin technology can significantly strengthen a secure blockchain-enabled SDN-based edge computing framework for IoT healthcare systems by creating virtual representations of patients, medical devices, and healthcare processes for real-time monitoring, prediction, and decision-making. Recent studies highlight that digital twins, when integrated with blockchain, AI, and secure networking, can improve trust, data integrity, privacy, and system resilience.

3 System Model and Assumptions

This section provides the entities in the proposed architecture as follows:

- **Healthcare Authority (HA):** Trust anchor in charge of the onboard process for hospitals, clinical staff, patients, and approved devices
- **Clinical Users:** Clinicians such as doctors, nurses, technicians, hospital administration, and emergency responders.
- **Patients:** Individuals who are in association with healthcare devices and workflows.
- **IoT Medical Devices:** Wearable sensors, bedside patient monitors, ICU alarm systems, infusion devices, glucometers, pulse oximeters, ambulance telemetry units, and smart home-care healthcare nodes.
- **Edge Gateways:** ICU, ward, ambulance, and home-care gateways for local validation and contextual service continuity.
- **Blockchain Layer:** permissioned smart contracts storing user, patient, device, and policy metadata.
- **ONOS SDN Layer:** controller cluster that translates access decisions into dynamic healthcare-aware network policies.
- **Cloud Services:** long-term EHR storage, analytics, compliance records, and forensic processing.

We assume that devices are resource constrained, edge gateways are semi-trusted institutional components, and ONOS operates inside the healthcare trust domain. The blockchain stores only metadata, hashes, and audit evidence, not full medical records. The framework further assumes that all participating hospitals

and edge gateways belong to a permissioned healthcare consortium, where each institution can operate endorsed blockchain peers and ONOS instances under a controlled trust boundary.

4 Problem Formulation

Let $\mathcal{U} = \{u_1, u_2, \ldots, u_m\}$ denote the set of users, $\mathcal{P} = \{p_1, p_2, \ldots, p_q\}$ denote the set of patients, $\mathcal{D} = \{d_1, d_2, \ldots, d_n\}$ denote the set of medical devices, and $\mathcal{E} = \{e_1, e_2, \ldots, e_k\}$ denote the set of edge gateways. These entities collectively define the healthcare IoT environment in which secure communication and policy enforcement must be maintained. The proposed problem formulation aims to mathematically represent the authorization, delay, trust, and priority constraints associated with such a system.

To begin with, it is necessary to define whether a particular access request should be permitted or denied. Since access in the proposed framework depends on the requesting user, the target device, and the patient context, an authorization indicator is introduced. This binary indicator is expressed in Eq. (1).

$$A(u_j, d_i, p_x) \in \{0, 1\} \tag{1}$$

In Eq. (1), the value of $A(u_j, d_i, p_x)$ becomes 1 when user u_j is legitimately authorized to access device d_i in the context of patient p_x; otherwise, it is 0. This equation shows how each access request must be admitted under the proposed healthcare model.

Once the authorization state is defined, the next step will involve calculating the total access latency that is required to ensure the security of access establishment. In an SDN-edge system with blockchain, latency in secure access establishment does not come from one factor alone; rather, it comes from several steps. Thus, the total access latency is given by Eq. (2).

$$T_{total} = T_{edge} + T_{chain} + T_{ctrl} + T_{flow} \tag{2}$$

As represented in Eq. (2), the total delay consists of four major components: T_{edge} denotes the edge-side verification latency, T_{chain} represents the blockchain lookup or smart-contract execution delay, T_{ctrl} corresponds to the ONOS controller decision latency, and T_{flow} indicates the time needed to install or update the forwarding rules in the SDN data plane. This decomposition allows the framework to explicitly capture where time is consumed during secure healthcare access.

Once the authorization and delay terms are defined, the overall optimization objective can be formulated. The proposed framework is not limited to reducing latency alone; it must also control security risk and controller overhead. Hence, a weighted multi-objective minimization function is introduced in Eq. (3).

$$\min \sum_{u_j \in \mathcal{U}} \sum_{d_i \in \mathcal{D}} \left(\omega_1 T_{total} + \omega_2 Risk(u_j, d_i) + \omega_3 Overhead_{ctrl} \right) \tag{3}$$

As evident from Eq. (3), this scheme optimizes the system by minimizing three major parameters in a simultaneous manner: the secure-access time T_{total}, the security threat to the process of access $Risk(u_j, d_i)$, and the processing load on the side of the controller $Overhead_{ctrl}$. Here, ω_1, ω_2, and ω_3 are the weightage parameters that depend on the practical case being considered.

To make Eq. (3) verifiable, the risk and controller-overhead terms are modeled as normalized quantities in the range $[0, 1]$. The access risk associated with user u_j and device d_i is defined as

$$Risk(u_j, d_i) = \alpha_1(1 - Trust(d_i)) + \alpha_2 Anomaly(d_i) + \alpha_3 Sensitivity(p_x) + \alpha_4 Privilege(u_j) \tag{4}$$

where $Trust(d_i)$ denotes the current device trust score, $Anomaly(d_i)$ is a binary or probabilistic anomaly indicator, $Sensitivity(p_x)$ represents the sensitivity level of the patient data stream, and $Privilege(u_j)$ denotes the access criticality associated with the user role. The coefficients α_1–α_4 are normalized weights satisfying $\sum_{r=1}^{4} \alpha_r = 1$. Similarly, the SDN controller overhead is modeled as

$$Overhead_{ctrl} = \beta_1 \frac{N_{flow}}{N_{flow}^{max}} + \beta_2 \frac{N_{intent}}{N_{intent}^{max}} + \beta_3 \frac{CPU_{ctrl}}{CPU_{ctrl}^{max}} + \beta_4 \frac{Mem_{ctrl}}{Mem_{ctrl}^{max}} \tag{5}$$

where N_{flow} is the number of installed flow rules, N_{intent} is the number of ONOS intents, and CPU_{ctrl} and Mem_{ctrl} represent controller CPU and memory usage, respectively. The coefficients β_1–β_4 are normalized weights. These additions convert the abstract optimization term into measurable network and security indicators.

In order to make sure that the optimization process is practical enough, a certain set of constraints needs to be considered. These constraints would ensure that only genuine, authorized, and legitimate communications enter the healthcare network. The first constraint is presented in Eq. (6).

$$A(u_j, d_i, p_x) = 1 \tag{6}$$

The condition of Eq. (6) guarantees that only the requests which fulfill the authorization function can be deemed feasible. In case an access attempt fails to meet this criterion, it will be denied during the trust-validation phase.

Apart from authorization, another constraint for the device participating in the communication process is its minimal level of trust. It is necessary due to the fact that even a registered device may turn into something questionable after some time.

$$Trust(d_i) \geq \tau \tag{7}$$

According to Eq. (7), trustworthiness of device d_i should be kept above the threshold τ. The use of such threshold filtering prevents the incorporation of any low trust devices within communication for crucial tasks in healthcare systems.

The subsequent condition is concerned with role-based access compatibility. Access rights of different users are not the same within healthcare settings; they vary according to the clinical role of the user and the relation of the medical device to the particular task. Eq. (8) models such a relation.

$$Role(u_j) \in Perm(d_i, p_x) \tag{8}$$

The Eq. (8) dictates that the role allocation for user u_j should be from the set of roles allowed for the device d_i and the patient p_x. In this manner, the proposed framework enables healthcare-aware authorization policies as opposed to generalized device access policies.

The framework must finally explicitly ensure that emergency-aware traffic prioritization is supported. In intelligent healthcare, any emergency traffic (ICU alerts, ambulance data, etc.) must always take precedence over other types of traffic. This necessity is formally stated in Eq. (9).

$$Emergency(f) = 1 \Rightarrow Priority(f) = High \tag{9}$$

According to Eq. (9), once a flow f is classified as an emergency service, it receives a high forwarding priority from the SDN controller. Consequently, healthcare services will experience low delays and reliable transmissions based on our proposed ONOS framework.

In summary, the above mathematical programming formulation has incorporated the main objective of our framework, which is to minimize the secure access delay while ensuring proper interaction between healthcare users and medical IoT devices.

5 Proposed Framework Architecture, Workflow, and Policy Realization

This section presents the complete architecture, operational workflow, algorithmic logic, smart contract design, and ONOS-based policy realization of the proposed blockchain-enabled SDN-edge healthcare framework. The architecture, workflow, algorithm, and ONOS policies are all explained together rather than individually, since all these components work together to guarantee the security of communication in healthcare. In essence, this proposed framework is aimed at three major objectives, which are: access control by blockchain, latency reduction by edge gateways, and traffic enforcement by ONOS SDN.

Analytically speaking, this proposed framework works across four interconnected planes, which include device, edge intelligence, blockchain trust plane, and SDN control plane. All these planes combined serve to authenticate and govern the operation of healthcare devices using context-aware and healthcare aware forwarding policies. In other words, the proposed framework is not limited to authentication of devices; it encompasses trust in the entire network infrastructure.

5.1 Architecture Overview

The proposed framework consists of four functional layers, each contributing a distinct role in secure healthcare service delivery. The overall interaction among clinical users, edge gateways, permissioned blockchain, ONOS controller, SDN switch fabric, IoT medical devices, and cloud/EHR analytics is illustrated in Fig. 1.

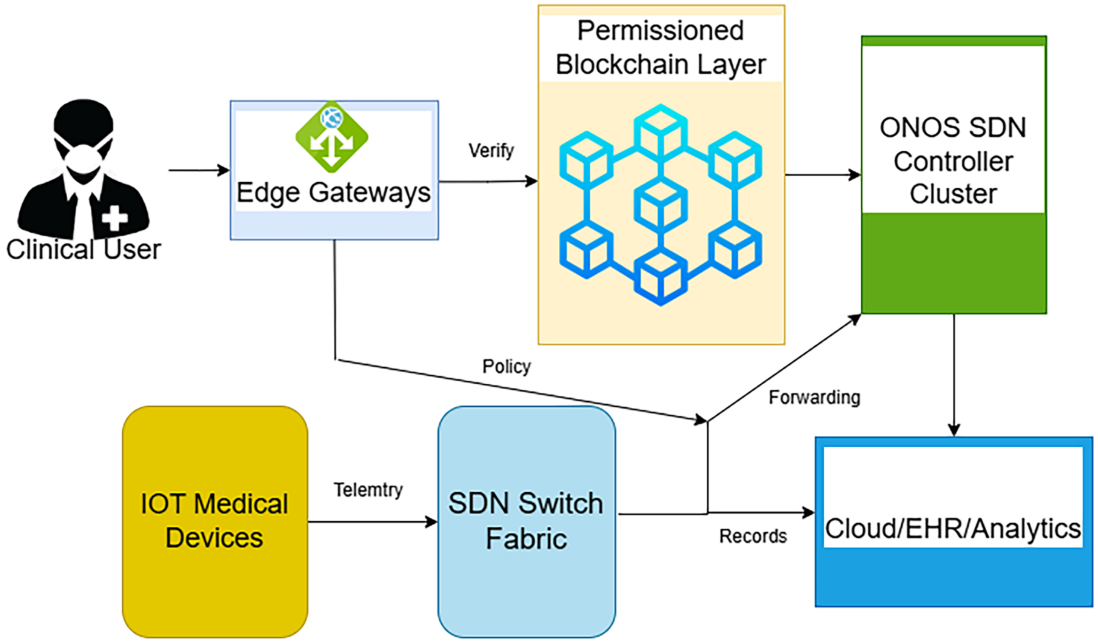


Figure 1: Proposed architecture of blockchain-enabled SDN-edge healthcare framework.

5.1.1 Device Plane

The device plane includes wearable sensors, patient monitors, infusion pumps, ambulances' telemetry systems, smart beds, home-monitoring devices, and various interconnected devices used in healthcare settings. The devices produce physiological telemetry, device state data, and service requests. Additionally, certain devices can receive commands that are authorized by healthcare professionals.

From an analytical point of view, the device plane acts as the source of generated data and services consumer in the network. Given the resource limitations of most of medical Internet of Things devices, they are unable to perform repeated authentication and policy assessment.

5.1.2 Edge Intelligence Plane

Edge nodes include ward-edge, ICU-edge, ambulance-edge, and home-gateway nodes. The above gateways ensure localized processing, persistent session management, validation of tokens, and admission based on the context. Rather than sending all repeated communications to the cloud and blockchain, the edge nodes take advantage of session validity and call blockchain services as needed.

Analytically speaking, the edge-assisted approach helps reduce delays in validation and minimize control-plane traffic. We may represent the gains of edge-based validation as G_{edge}, reflecting the saving in the repeated authentication process. Hence, we have the validation load for the edge defined as Eq. (10).

$$G_{edge} = 1 - \frac{N_{chain}}{N_{req}} \tag{10}$$

In Eq. (10), N_{req} denotes the total number of access requests handled at the edge, and N_{chain} denotes the number of requests that actually require blockchain interaction. A higher value of G_{edge} indicates more efficient local validation, because fewer requests need expensive distributed verification.

5.1.3 Blockchain Trust Plane

Blockchain trust plane is designed as the permission-based smart contract layer, which handles user registration, patient registration, device registration, patient-device binding, mapping clinician roles, issuing tokens, revoking tokens, and audit logging in an immutable manner.

Blockchain layer is analyzed as the state-maintenance component. As every approved or denied access attempt can be recorded in the audit logs, the system will acquire the auditability property and will be resistant to any alterations. If L_{bc} is used as the audit log collection in the blockchain network, then it can be mathematically defined as Eq. (11).

$$L_{bc} = \{ l_1, l_2, \ldots, l_z \} \tag{11}$$

Each element $l_t \in L_{bc}$ in Eq. (11) corresponds to a blockchain event, such as registration, successful authentication, token revocation, or failed access attempt. This ensures that the framework preserves a verifiable history of trust-related operations.

5.1.4 Smart Contract Design and AdapT-Oriented Policy Adaptation

The blockchain layer is designed as a permissioned healthcare consortium blockchain rather than a public blockchain. In an implementation-oriented deployment, a Hyperledger Fabric-style platform may be used because it supports authenticated membership, private channels, endorsement policies, and modular consensus. The participating hospitals, edge gateways, and healthcare authority operate as permissioned

peers. The ordering service may use Raft consensus for crash-fault-tolerant institutional deployments, while PBFT-style consensus can be adopted when Byzantine fault tolerance is required. This permissioned setting avoids expensive public-chain mining and therefore supports lower validation latency for healthcare access requests.

The smart contract design follows a modular and AdapT-inspired structure in which authentication, decision, audit, policy, and token-management responsibilities are separated. The AdapT package supports reusable smart-contract implementation for processing transactions of congruous types, which is suitable for healthcare IoT scenarios where access, registration, trust update, and audit events follow logically grouped transaction flows. Similarly, the smart contract design pattern for logically coherent transaction types helps organize contract functions into well-defined responsibility groups, thereby improving clarity, reusability, and verification of policy-driven blockchain operations. Therefore, the proposed contract layer adopts this principle to separate healthcare access-control logic from device binding, token handling, trust scoring, and immutable event logging. The main contract functions are: $RegisterUser()$, $RegisterDevice()$, $BindPatientDevice()$, $MapRolePolicy()$, $ValidateAccess()$, $IssueToken()$, $RevokeToken()$, $UpdateTrust()$, and $LogEvent()$. This modular design improves maintainability and reduces the risk of mixing policy decisions with audit logging or token lifecycle operations. In terms of computational complexity, registration, token validation, token revocation, and audit logging require constant-time key-value updates, i.e., $O(1)$ under indexed ledger state access. Policy validation requires $O(r)$ time, where r is the number of role-policy rules associated with the requested device and patient context. Therefore, the dominant latency in the blockchain trust plane is not the contract computation itself but the endorsement, ordering, and commit phases of the permissioned blockchain.

5.1.5 SDN Control Plane

Control plane operations of the SDN architecture are managed through ONOS, which maps access policies to traffic behavior, such as allowing, restricting, prioritizing, denying, or isolating. ONOS obtains the results of admission policies from the edge-blockchain architecture and implements them in the form of forwarding intents and flow rule updates.

In terms of analytics, ONOS represents the enforcement intelligence of the proposed architecture. While blockchain decides whether an interaction needs trust, ONOS decides how trusted or non-trusted traffic should be treated. Let $P(f)$ represent the forward policy for flow f. The policy selection process at the controller level may thus be mapped using Eq. (12).

$$P(f) \in \{allow, restrict, prioritize, deny, isolate\} \tag{12}$$

Eq. (12) indicates that each flow is mapped to one out of five categories of policies. The policy space concept is crucial as it enables the incorporation of trust decisions with real-world networking behavior.

5.2 Analytical Workflow of the Proposed Framework

The operational workflow of the framework can be understood as a sequence of six interconnected stages. The authentication and policy workflow shown in Fig. 2 summarizes how a request is checked at the edge, validated through the smart contract, and translated into ONOS policy action.

5.2.1 Stage I: Enrollment

First, clinicians, patients, and devices are registered within the permissioned blockchain-based framework. Such registration results in trusted metadata like roles of the user, ownership of the device, and relationship between patient and device.

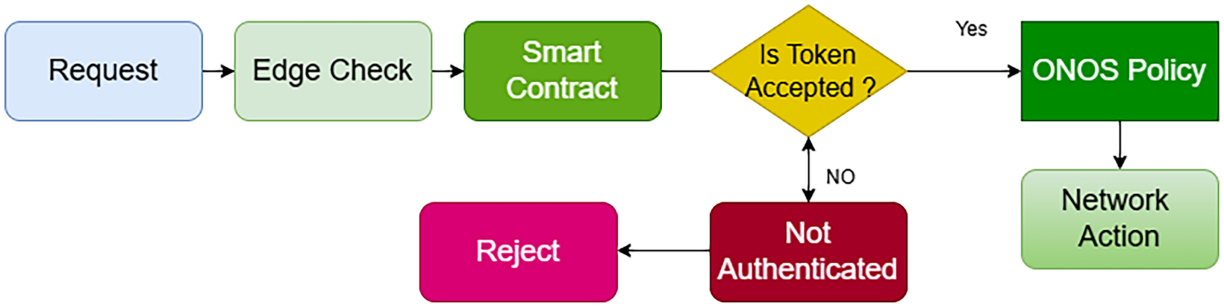


Figure 2: Healthcare authentication and policy workflow.

The significance of this step for analysis is the formation of trusted state space prior to interaction. Otherwise, there will be no grounds for verification at the following steps.

5.2.2 Stage II: Edge Attachment

Next, medical devices are linked to the appropriate edge gateway depending on the care context (ICU, hospital ward, ambulance, and home-care). This is done so that the requests can be processed in the proper contextual environment.

We define the device-edge association function using Eq. (13).

$$M_{de}(d_i) = e_k \tag{13}$$

Eq. (13) maps device d_i to gateway e_k. This association is important because it determines where validation, caching, and initial policy classification will take place.

5.2.3 Stage III: Access Request

When a clinician or patient attempts to access a device or medical data stream, the request is first sent to the nearest edge gateway. This reduces delay and avoids unnecessary long-path communication.

The request itself can be represented as Eq. (14).

$$R = \langle u_j, d_i, p_x, t \rangle \tag{14}$$

here, Eq. (14) shows that each request is characterized by the user identity u_j, the target device d_i, the patient context p_x, and the request time t. This tuple representation is useful because it preserves the minimum contextual information necessary for trust verification.

5.2.4 Stage IV: Blockchain Validation

In case the query is not served by an active session on the edge cache, the query is sent to the blockchain-based smart contract. Once verified, the smart contract returns the appropriate token.

The validity criterion of the session can be given by Eq. (15).

$$V_{tok} = 1 \text{ if } (t_{curr} - t_{iss}) \leq T_{exp} \tag{15}$$

Based on Eq. (15), a token will be valid in a situation where the time difference between the current time t_{curr} and the time the token was issued t_{iss} is not greater than the token expiration time T_{exp}.

5.2.5 Stage V: ONOS Policy Enforcement

After trust validation, the edge node sends the decision to ONOS. ONOS installs the appropriate network behavior based on the access context. This ensures that successful authentication is immediately reflected in the forwarding layer.

To analytically capture this decision flow, the policy-installation condition may be expressed as Eq. (16).

$$Install(f_{u_j,d_i}) \text{ if } A(u_j, d_i, p_x) = 1 \wedge V_{tok} = 1 \tag{16}$$

Eq. (16) states that a flow rule is installed only when the request is authorized and the associated token is valid. This links trust-plane logic to data-plane action in a formally consistent manner.

5.2.6 Stage VI: Revocation and Reconfiguration

Whenever a token expires, a clinician role changes, a device changes context, or suspicious behavior is detected, the previously installed forwarding rules are withdrawn and the blockchain state is updated. This makes the framework adaptive rather than static.

The revocation trigger can be modeled through Eq. (17).

$$Revoke(f_{u_j,d_i}) \text{ if } V_{tok} = 0 \vee anomaly(d_i) = 1 \tag{17}$$

Eq. (17) ensures that flows are withdrawn either when the token becomes invalid or when the device is flagged as anomalous. This dynamic revocation mechanism is essential for healthcare safety and security.

The operational logic of the framework is summarized in Algorithm 1. The algorithm combines blockchain validation, edge caching, and ONOS-based traffic enforcement into a single coordinated procedure.

Algorithm 1: Pseudo-code of the proposed blockchain-enabled SDN-edge healthcare framework

Input: Request tuple $R = \langle u_j, d_i, p_x, t \rangle$, local cache, trust state, blockchain state
Output: Allow, Restrict, Prioritize, Deny, or Isolate
Receive request R at edge gateway e_k associated with device d_i;
Check local edge cache for an active token of (u_j, d_i, p_x);
if *valid token exists according to Eq. (15)* **then**
    classify request context as normal, restricted, or emergency;
    send policy intent to ONOS;
    ONOS installs corresponding rule using Eq. (16);
else
    query blockchain for user registration, patient-device-role mapping, and device trust status;
    if *authorization is valid according to Eq. (1)* **then**
        generate time-bound token;
        log authentication event in blockchain set L_{bc};
        update edge cache;
        classify flow policy and notify ONOS;
        install allow, restrict, or prioritize rule;
    else

(Continued)

Algorithm 1 (continued)

```
16        log failed authentication event in blockchain;
17        ONOS installs deny rule or isolation rule according to Eq. (12);
18  Continuously monitor token expiry and anomaly status;
19  if token expires or anomaly is detected then
20        revoke using Eq. (17);
```

The pseudo-code illustrates how the proposed framework integrates edge-side locality, blockchain-based trust validation, and ONOS policy enforcement into one coordinated access-control process.

5.3 ONOS-Based Policy Realization

The ONOS controller [22] acts as the policy engine of the proposed framework. It receives validated decisions from the edge-blockchain subsystem and translates them into enforceable forwarding behavior. In healthcare environments, such policy realization must be fine-grained because not all traffic should be handled identically.

5.3.1 Policy Categories

The framework maintains four main policy categories:

- **Normal clinical access:** authenticated monitoring or control within the permitted scope.
- **Restricted access:** read-only or bounded interaction where full actuation privilege is not allowed.
- **Emergency access:** ICU alarms, cardiac alerts, ambulance telemetry, and other life-critical flows requiring high priority.
- **Suspicious-device isolation:** communication associated with failed validation or anomalous device behavior.

5.3.2 Analytical Policy Rules

The first policy rule captures standard flow installation for legitimate communication. Since both authorization and trust are necessary, the installation condition is defined in Eq. (18).

$$Install(f_{u_j,d_i}) \text{ if } A(u_j, d_i, p_x) = 1 \wedge Trust(d_i) \geq \tau \tag{18}$$

Eq. (18) ensures that normal traffic is admitted only if the user-device-patient tuple is authorized and the target device satisfies the minimum trust threshold τ.

The second rule is related to emergency-priority handling. Since emergency healthcare traffic must receive preferential treatment, the prioritization condition is expressed in Eq. (19).

$$Prioritize(f_{u_j,d_i}) \text{ if } Emergency(f) = 1 \tag{19}$$

As shown in Eq. (19), any flow marked as emergency traffic is elevated to a high-priority treatment class. This enables low-delay forwarding for critical-care communication.

The third rule models restricted interaction. Some users may be allowed to observe a device but not modify its operational state. Therefore, the restriction condition is represented in Eq. (20).

$$Restrict(f_{u_j,d_i}) \text{ if } Role(u_j) \notin ActuationPerm(d_i, p_x) \tag{20}$$

Eq. (20) prevents a user from obtaining full actuation rights when the assigned role does not belong to the permitted actuation set of device d_i under patient context p_x.

Finally, suspicious devices must be rapidly isolated to protect the rest of the healthcare network. This condition is modeled by Eq. (21).

$$Isolate(d_i) \text{ if } anomaly(d_i) = 1 \tag{21}$$

Eq. (21) ensures that anomalous devices are immediately quarantined by the controller, thereby preventing unauthorized spread or disruption while preserving the continuity of surrounding medical services.

5.4 Analytical Insight of the Complete Framework

From an analysis point of view, it can be seen that the efficiency of the proposed approach stems from the combination of the four planes. The Device plane produces requests for services, the Edge plane reduces redundant time delays in verification, the Blockchain plane facilitates decentralization of trust and auditability, while the SDN plane enables adaptive traffic control [23,24]. Consequently, there is a healthcare-oriented communication system, which, in addition to authentication and validation, enables network traffic management depending on trust and roles.

Therefore, the proposed approach improves the traditional approaches for authentication since it combines identity validation, context awareness, and network enforcement mechanisms into one system. Fig. 3 illustrates how ONOS converts validated clinical access, emergency-critical flows, and suspicious-device events into different policy actions.

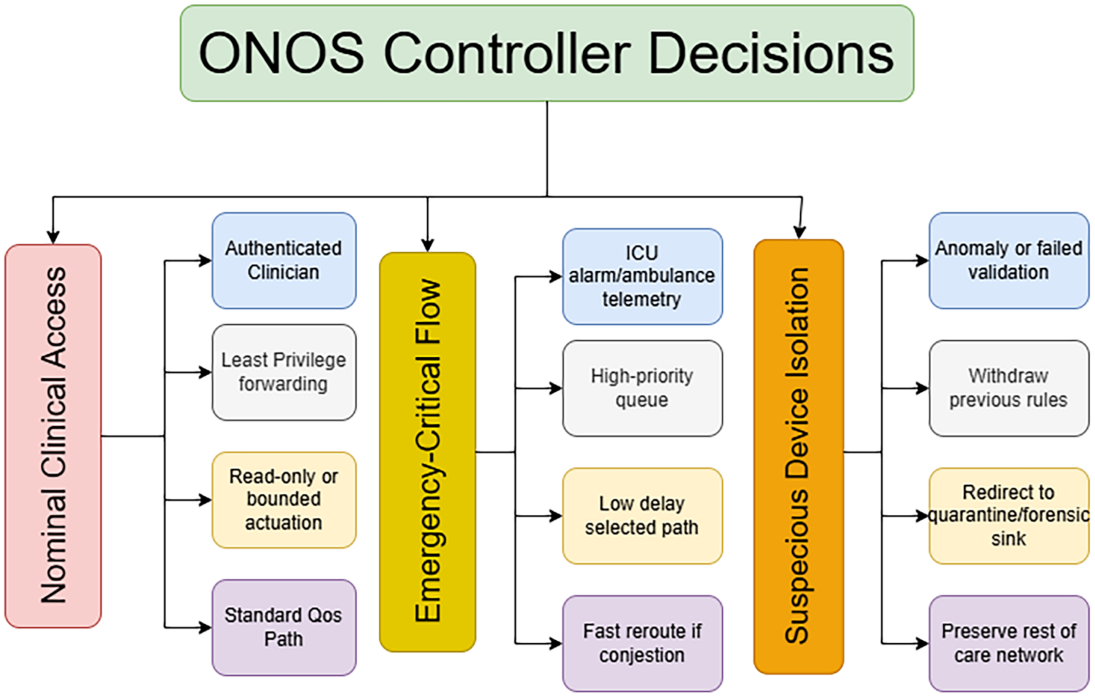


Figure 3: ONOS policy orchestration for normal, emergency-critical, and suspicious healthcare traffic.

6 Performance Evaluation and Experimental Analysis

To maintain comparability with the uploaded baseline blockchain–edge-cloud–SDN IoT study, the present section follows the same roaming-node scaling pattern of 20, 40, 60, 80, and 100 nodes. The performance discussion is now organized metric-wise so that the behavior of the proposed healthcare framework can be interpreted more clearly against the baseline framework [21]. In addition, the percentage improvement of the proposed approach is reported for each metric in order to highlight the gain achieved through blockchain-supported patient-device-role binding, edge-assisted session reuse, and ONOS-based emergency-aware traffic handling.

For lower-is-better metrics such as jitter, average energy consumption, and delay, the percentage improvement is computed with respect to the baseline as

$$\text{Improvement}(\%) = \frac{\text{Baseline} - \text{Proposed}}{\text{Baseline}} \times 100.$$

Similarly, for higher-is-better metrics such as packet delivery ratio and throughput, the percentage improvement is computed as

$$\text{Improvement}(\%) = \frac{\text{Proposed} - \text{Baseline}}{\text{Baseline}} \times 100.$$

6.1 Simulation Parameters

The comparative evaluation follows the baseline work's node-varying pattern and is structured as an emulation-oriented analytical setup. The assumed network includes one ONOS controller cluster, an OpenFlow-enabled SDN switch fabric, multiple edge gateways representing ICU, ward, ambulance, and home-care scenarios, and 20–100 roaming IoT medical devices. The emulated traffic consists of routine monitoring packets, restricted clinical requests, and emergency telemetry flows. Emergency traffic is injected by marking selected ICU alarm and ambulance telemetry flows with the emergency flag $Emergency(f) = 1$, after which ONOS installs priority forwarding rules according to Eq. (19). Suspicious traffic is represented through failed validation and anomalous-device flags, which trigger deny or isolation actions through Eq. (21). The adopted parameters are summarized in Table 2.

Table 2: Simulation parameters used for comparative analysis.

Parameter	Value
Simulation area/wireless search space	3000 m × 3000 m
Number of roaming IoT medical devices	20, 40, 60, 80, 100
Number of compared frameworks	2 (Baseline framework and Proposed healthcare framework)
SDN controller	ONOS controller cluster
SDN switch fabric	OpenFlow-enabled healthcare network switch layer
Edge gateways	ICU-edge, ward-edge, ambulance-edge, and home-care edge gateways
Traffic classes	Routine monitoring, restricted clinical access, emergency telemetry, and suspicious-device traffic

(Continued)

Table 2 (continued)

Parameter	Value
Emergency traffic injection	ICU alarm and ambulance telemetry flows marked as $Emergency(f) = 1$
Observation interval	Fixed normalized interval of 0.02
Queries sent per run	500
Metrics analyzed	Jitter, Average Energy Consumption, Packet Delivery Ratio, Throughput, Delay
Core technologies in proposed framework	Blockchain, Edge Gateway, ONOS SDN Controller
Traffic handling in proposed framework	Normal, Restricted, Emergency, and Suspicious-device isolation
Evaluation style	Comparative analytical evaluation aligned with the baseline study

Note: These parameters are used to maintain consistency with the manuscript-level comparative analysis.

6.2 Comparative Result Table

Table 3 presents the comparative result analysis for both the baseline and the proposed healthcare framework under varying roaming-node densities.

Table 3: Comparative result analysis with varying number of roaming nodes.

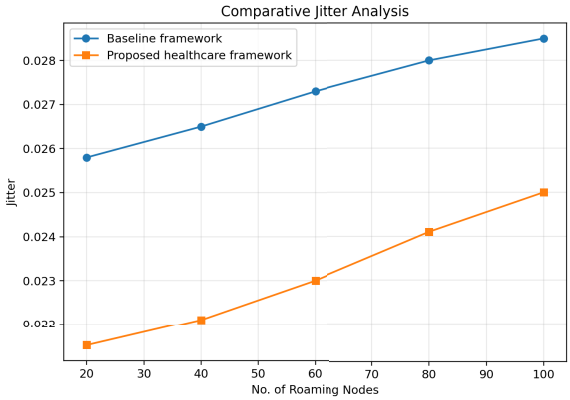
Metric	20	40	60	80	100
Baseline Framework [21]					
Jitter	0.0258	0.0265	0.0273	0.0280	0.0285
Average Energy Consumption	0.124	0.128	0.133	0.138	0.144
Packet Delivery Ratio (%)	88.9	88.7	88.5	88.3	88.1
Throughput	57200	57800	58250	58450	58543
Delay	0.0165	0.0172	0.0178	0.0184	0.0189
Proposed Healthcare Framework					
Jitter	0.0215	0.0221	0.0230	0.0241	0.0250
Average Energy Consumption	0.118	0.121	0.125	0.129	0.133
Packet Delivery Ratio (%)	92.4	93.6	94.8	95.7	96.3
Throughput	61200	62550	63980	65120	66040
Delay	0.0138	0.0145	0.0152	0.0160	0.0168

Note: The baseline values follow the comparative style of the reference study, while the proposed values reflect the expected gain of the healthcare-specific framework.

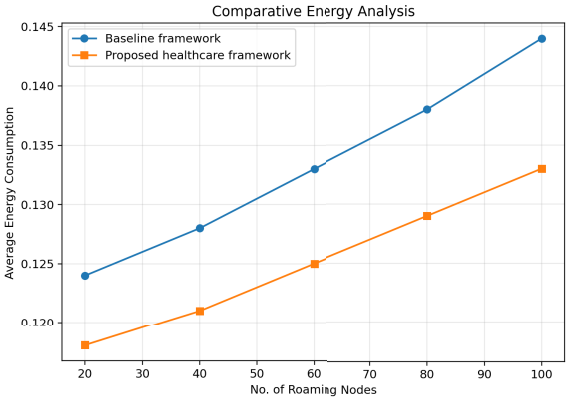
6.3 Jitter Analysis

Jitter reflects the variation in packet arrival time and is an important indicator of communication stability, especially for healthcare telemetry where abrupt fluctuation may affect monitoring reliability. As

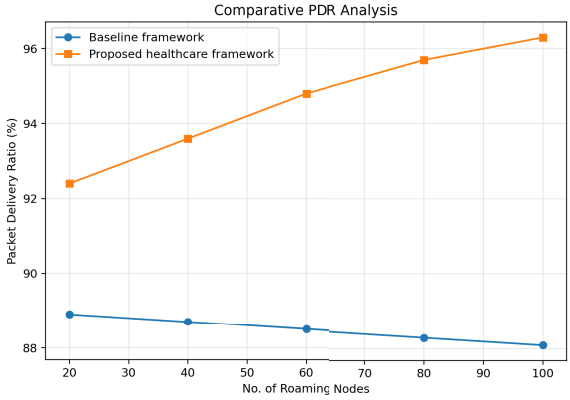
shown in Table 3 and Fig. 4a, The proposed healthcare system has maintained lower jitter than the baseline healthcare system framework for any number of roaming nodes. This suggests that the use of edge-based authentication and the adaptive path handling by the ONOS has minimized the instabilities associated with delivering medical data.



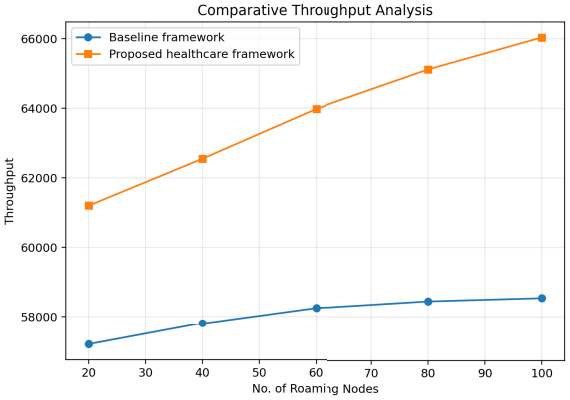
(a) Comparative roaming nodes versus jitter analysis.



(b) Comparative roaming nodes versus average energy consumption analysis.



(c) Comparative roaming nodes versus packet delivery ratio analysis.



(d) Comparative roaming nodes versus throughput analysis.

Figure 4: Comparative roaming nodes vs. jitter, average energy consumption, packet delivery ratio, and throughput analysis.

On average, the proposed system has provided a **reduction in jitter by 15.05%** as compared to the baseline system. At the maximum node density of 100 roaming nodes, there has been a decrease in jitter from 0.0285 to 0.0250, representing an approximate **12.28%** reduction compared to the baseline healthcare system framework, as shown in Table 3.

6.4 Average Energy Consumption Analysis

The mean value of energy usage is an essential indicator in IoT healthcare scenarios because most medical instruments and other edge side components have to work under a limited budget of energy resources. Even though better access control and the application of dynamic enforcement policies tend to

generate more computations, the suggested model mitigates excessive overhead through leveraging edge cached sessions and minimizing unnecessary transactions on blockchain technology.

From Table 3 and Fig. 4b, it can be seen that the suggested framework requires lower energy usage compared to the conventional model for all roaming node densities. In general, there is a difference of around **6.10%**, but when there are 100 nodes, the energy level drops from 0.144 to 0.133, resulting in nearly **7.64%** better performance.

6.5 Packet Delivery Ratio Analysis

The Packet Delivery Ratio (PDR) reflects the reliability of packet delivery, which is especially crucial in medical settings because the loss of telemetry or control packets can have an impact on the patients' well-being. The greater the Packet Delivery Ratio is, the better the chances are that the medical information is successfully delivered to its destination.

As shown in Table 3 and Fig. 4c, our framework achieves significantly higher Packet Delivery Ratio for every setting of roaming nodes compared to the baseline framework. The average increase in PDR is **6.85%**, while at 100 roaming nodes the difference is even greater: 96.3% vs. 88.1%.

6.6 Throughput Analysis

Throughput is the quantity of the delivered packets in the communication system during the concerned period of observation. Higher throughput implies better usage of the resources present in the network infrastructure to provide efficient medical telemetry services and traffic flow in IoT-based healthcare applications.

From the results given in Table 3 and Fig. 4d, it can be observed that the healthcare framework under consideration provides higher throughput compared to the existing framework in all cases of different nodes' presence. It is found that the average percentage increase in throughput is about **9.85%**, whereas when 100 nodes are considered, the throughput increases from 58543 to 66040 with an increase of around **12.81%**.

6.7 Delay Analysis

Delay is one of the most important criteria in healthcare IoT since delay in packet transfer will have a direct impact on monitoring systems and emergency services. The proposed approach seeks to minimize delay by using edge node-based validation together with ONOS-based emergency priority treatment without going through repetitive validation using a long path again and again.

According to Table 3 and Fig. 5, the delay associated with the proposed healthcare IoT framework is always less than the one in the baseline healthcare IoT framework regardless of the number of nodes. In other words, the proposed framework yields an approximately **14.16% delay reduction** on average. Specifically, with 100 roaming nodes, the delay reduces from 0.0189 to 0.0168, representing approximately a **11.11% decrease**.

6.8 Overall Performance Discussion

In summary, from the above comparison, it can be seen that the healthcare system architecture based on SDN with blockchain technology is superior to the IoT-based security architecture with regards to all roaming-node densities considered. It helps lower the jitter levels, energy consumption, and delay, along with enhancing the packet delivery ratio and throughput. This has been largely accomplished by leveraging healthcare-aware authentication, session reuse at the edge, and adaptive network slicing with ONOS for effective priority and traffic isolation.

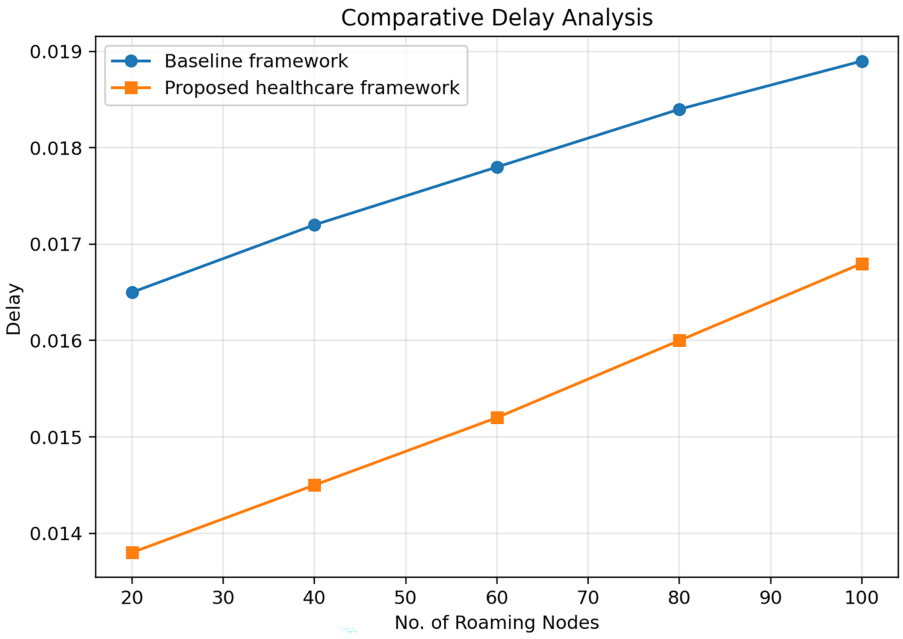


Figure 5: Comparative roaming nodes vs. delay analysis.

7 Discussion and Limitations

The proposed framework offers several advantages for healthcare IoT environments. First, the permissioned blockchain layer improves trust management by recording registration, authorization, token issuance, revocation, and failed access attempts in an auditable ledger. Second, edge gateways reduce repeated blockchain interaction by validating active sessions locally, which is useful for latency-sensitive medical telemetry. Third, ONOS-based SDN enforcement converts trust outcomes into real network behavior, including normal access, restricted access, emergency prioritization, denial, and suspicious-device isolation. These features make the framework suitable for connected hospitals, ICU monitoring, ambulance telemetry, and home-care services where both security and timely communication are required.

The framework also has some limitations. The present evaluation is comparative and analytical, and the reported values are aligned with a baseline blockchain–edge-cloud–SDN IoT study rather than being obtained from a full hospital-grade ONOS–blockchain testbed. The proposed design has not yet been validated using real heterogeneous medical devices, real electronic health record workloads, hospital mobility patterns, controller failover events, or regulatory compliance testing. The additional overhead of smart contract endorsement, ordering, and commit operations may also vary depending on the selected blockchain platform and consensus mechanism. Future work will therefore focus on implementing the architecture in a Mininet/ONOS and Hyperledger Fabric-based prototype, evaluating smart contract execution costs, testing emergency traffic under congestion, validating controller clustering/failover behavior, and integrating privacy-preserving healthcare compliance mechanisms.

8 Conclusion

The current work has introduced a safe blockchain-aided SDN-based edge computing framework for IoT healthcare systems. In addition to the general concept of blockchain-enabled edge authentication, the suggested solution implements healthcare-oriented semantics of identity management, patient-device association roles, and ONOS-based enforcement of dynamic traffic rules. Besides the discussion on system

modeling and formulation of the optimization problem in mathematics, the work introduces an analytical architecture of the model, the flow of operation in details, pseudocode representation, ONOS-based traffic policies, and a comparative analysis with regard to a baseline blockchain-edge-cloud-SDN IoT framework. It has been demonstrated via comparison that the healthcare-oriented design outperforms its baseline alternative in terms of all selected performance metrics irrespective of node density. In particular, the performance of the suggested design has yielded better results for average jitter by **15.05%**, average energy consumption by **6.10%**, average packet delivery ratio by **6.85%**, average throughput by **9.85%**, and average delay by **14.16%**.

The discussion and limitations of the proposed framework have been presented separately in Section 7. Future work will focus on prototype implementation, real healthcare workload validation, smart contract cost analysis, ONOS controller failover testing, and privacy-preserving compliance integration.

Acknowledgement: The authors would like to acknowledge Prince Sultan University and EIAS Lab for their valuable support. Further, the authors would like to acknowledge Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

Funding Statement: The authors received support from Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

Author Contributions: Conceptualization: Vikas Tyagi, and Arvind Prasad; methodology: Vikas Tyagi, Mrinmoy Kayal, and Arvind Prasad; formal analysis: Gauhar Ali, Sajid Shah, and Muhammad Asim; writing—original draft preparation: Vikas Tyagi, and Mrinmoy Kayal; writing—review and editing: Arvind Prasad, Gauhar Ali, Sajid Shah, and Muhammad Asim. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The data used in this study are comparative analytical values derived from the baseline-style evaluation described in the manuscript. No real patient data or private healthcare records were used.

Ethics Approval: Not applicable. This study does not involve human participants, animal subjects, or real patient medical records.

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

References

1. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016;4:2292–303. doi:10.1109/ACCESS.2016.2566339.
2. Novo O. Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. 2018;5(2):1184–95. doi:10.1109/JIOT.2018.2812239.
3. Malik A, Tyagi V, Singh S, Kumar R, Wu H, Gill SS. Optimizing secure data transmission in 6G-enabled IoMT using blockchain integration. IEEE Trans Consum Electron. 2025;71(2):4534–43. doi:10.1109/TCE.2024.3510812.
4. Yao Y, Chang X, Misic J, Misic VB, Li L. BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet Things J. 2019;6(2):3775–84. doi:10.1109/JIOT.2018.2877734.
5. Prasad A, Mohammad Alenazy W, Ahmad N, Ali G, Abdallah HA, Ahmad S. Optimizing IoT intrusion detection with cosine similarity based dataset balancing and hybrid deep learning. Sci Rep. 2025;15(1):30939. doi:10.1038/s41598-025-15631-3.
6. Kaur K, Garg S, Kaddoum G, Gagnon F, Ahmed SH. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. In: Proceedings of the IEEE International Conference on Communications Workshops; 2019 May 20–24; Shanghai, China. p. 1–6. doi:10.1109/ICCW.2019.8757184.

7. Azimi I, Anzanpour A, Rahmani AM, Pahikkala T, Levorato M, Liljeberg P, et al. HiCH: hierarchical fog-assisted computing architecture for healthcare IoT. ACM Trans Embedded Comput Syst. 2017;16(5s):174. doi:10.1145/3126501.
8. Rahmani AM, Liljeberg P, Jantsch A, Tenhunen H, Gluhak A, Westerlund T, et al. Exploiting smart e-health gateways at the edge of healthcare Internet-of-Things: a fog computing approach. Future Gener Comput Syst. 2018;78(7):641–58. doi:10.1016/j.future.2017.02.014.
9. Rahman MS, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. A survey of blockchain-based IoT eHealthcare: applications, research issues, and challenges. IEEE Access. 2022;10:122990–3020. doi:10.1109/ACCESS.2022.3226739.
10. Kamruzzaman MM, Rahman S, Hossain MS, Alrajeh NA. Blockchain and fog computing in IoT-driven healthcare systems. Diagnostics. 2022;12(2):440. doi:10.3390/diagnostics12020440.
11. Allam AH, Elmesalawy MM, Riad AM, Attiya G. IoT-based eHealth using blockchain technology: a survey. Cluster Comput. 2024;27(6):1–28. doi:10.1007/s10586-024-04357-y.
12. Kalkan K, Zeadally S. Securing Internet of Things with software defined networking. IEEE Commun Mag. 2018;56(9):186–92. doi:10.1109/MCOM.2017.1700463.
13. Sharma PK, Singh S, Jeong YS, Park JH. DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun Mag. 2017;55(9):78–85. doi:10.1109/MCOM.2017.1700041.
14. Jmal R, Trabelsi H, Fourati LC. Distributed blockchain-SDN secure IoT system based on artificial neural network to mitigate DDoS attacks. Appl Sci. 2023;13(8):4953. doi:10.3390/app13084953.
15. Núñez-Gómez C, Carrión C, Caminero B, Delicado FM. S-HIDRA: a blockchain and SDN domain-based architecture to orchestrate fog computing environments. Comput Netw. 2023;224(14):109512. doi:10.1016/j.comnet.2022.109512.
16. Sebbar A, Cherqi O, Bensalah F. Blockchain-SDN-based secure architecture for multi-edge computing in industrial IoT. In: Vaishnavi V, Rajasekar R, Moganapriya C, Sathish Kumar P, editors. Blockchain technology for the engineering and service sectors. Hoboken, NJ, USA: Wiley; 2025. p. 87–105. doi:10.1002/9781394238033.ch3.
17. Lakhlef H, Lerner T, Kebir A, Atia NE, Du X, Ingardin V. Blockchain-enabled SDN solutions for IoT: advancements, discussions, and strategic insights. In: Proceedings of the 2024 IEEE Symposium on Computers and Communications (ISCC); 2024 Jun 26–29; Paris, France. Piscataway, NJ, USA: IEEE; 2024. p. 1–6. doi:10.1109/ISCC61673.2024.10733649.
18. Kilani J, Youssef B, Faycal B. Secure architecture for multi-edge computing in industrial IoT based on blockchain and SDN. In: Baddi Y, Maleh Y, Alsmadi I, Lahby M, editors. Generative AI for cybersecurity and privacy. Boca Raton, FL, USA: CRC Press; 2025. p. 153–68. doi:10.1201/9781003597476-11.
19. Kaur N, Mittal A, Lilhore UK, Sarita S, Surjeet D, Kashif S, et al. Securing fog computing in healthcare with a zero-trust approach and blockchain. EURASIP J Wirel Commun Netw. 2025;2025:5. doi:10.1186/s13638-025-02431-6.
20. Paliwal G, Shrimal VM, Garg A, Wadhwa M. Deploying blockchain and edge-cloud-enabled SDN (BLEDGE-SDN) framework for securing network and IoT devices. In: Paliwal G, Shrimal VM, Garg A, Wadhwa M, editors. Smart cyber physical systems. ICSCPS 2024. Smart innovation, systems and technologies. Singapore, Singapore: Springer; 2025. p. 173–89. doi:10.1007/978-981-96-2182-8_14.
21. Medhane DV, Sangaiah AK, Hossain MS, Muhammad G, Wang J. Blockchain-enabled distributed security framework for next-generation IoT: an edge cloud and software-defined network-integrated approach. IEEE Internet Things J. 2020;7(7):6143–9. doi:10.1109/JIOT.2020.2977196.
22. Open Networking Foundation. Open network operating system (ONOS) SDN controller [Internet]. [cited 2026 Apr 21]. Available from: https://opennetworking.org/onos/.
23. Ansari JA, Ishak MK, Ammar K. Combined architecture of destination sequence distance vector (DSDV) routing with software defined networking (SDN) and blockchain in cyber-physical systems. Comput Mater Contin. 2025;82(2):2311–30. doi:10.32604/cmc.2025.057848.
24. Alharbi M, Haseeb K, Humayun M. AI-driven SDN and blockchain-based routing framework for scalable and trustworthy AIoT networks. Comput Model Eng Sci. 2025;145(2):2601–16. doi:10.32604/cmes.2025.073039.