International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 5, Sep-Oct-2026, ISSN (Online): 2395-566X

Cybersecurity Frameworks for Protecting Internet of Medical Things (IoMT) Devices in Smart Healthcare

Mahesh S[1], Dr. Jayasree P[2]
[1](Assistant Professor Computer Science And Engineering
St. Thomas College of Engineering And Technology(Autonomous)
mahe4855@gmail.com)
[2](Medical Officer National Ayush Mission, Alappuzha
jayamangalath94@gmail.com)

Abstract- The use of Internet of Medical Things (IoMT) in smart healthcare ecosystems has led to a large-scale attack surface which current perimeter-based security solutions cannot sufficiently cover. Resource limitations, diverse protocols, and life-critical telemetry require security designs which function across the device, edge, and cloud layers while avoiding significant computation costs. In this work, we design a cross-layer security architecture which involves selective elliptic curve cryptography for IoT device authentication, sidecar proxy zero trust enforcement at the edge, and protocol-aware intrusion detection for behavior monitoring. Our design utilizes only asymmetric cryptography at registration time while shifting online mutual authentication to hash-based message authentication code and timestamp validation in order to reduce computational cost of each session without losing authentication assurances. Experimental evaluation on emulated IoMT traffic shows that our architecture is able to provide sub-10 ms end-to-end authentication latency, preserve masquerade and replay attempt detection under the attack injection, and retain tenant isolation in multi-tenant cloud setups. Comparative evaluation with state-of-the-art frameworks proves that our solution provides a better trade-off between latency, energy consumption, and cross-layer visibility.

Key Word: Internet of Medical Things, Zero Trust Architecture, Lightweight Authentication, Intrusion Detection, Smart Healthcare Security, Cross-Layer Framework

I. INTRODUCTION

Integration of the Internet of Medical Things technology within smart healthcare systems has led to a complete change in the topological landscape of clinical data collection and monitoring [1][2]. Wearable biosensors, implantable heart devices, infusion pumps, and continuous glucose monitors have made it possible to collect high-frequency data about the physiology of the body which then moves across the device, edge, and cloud levels to reach clinical decision support systems [1][7]. Such technological development not only facilitates real-time remote monitoring, alerting, and personalized intervention therapies but also leads to an expansion in the cyber-security risk landscape which traditional healthcare information security cannot handle [2][9].

There are several aspects that make security concerns unique for IoMT deployments as opposed to typical IoT for enterprise applications because of three main reasons [2][7]. Firstly, IoMT devices often face very limited resources available: implantable devices and wearable sensors do not have sufficient computing power, storage capabilities, and battery power which makes cryptographic systems hard to employ [3]. Secondly, the data flowing through these devices has an impact on the physical well-being of patients; malfunctioned infusion pumps or corrupted cardiac telemetry signals pose a serious threat to health and even life [1][9].

Thirdly, the regulatory framework governing medical data has strict requirements concerning confidentiality, integrity, and auditing of data flows but many old IoMT devices lack basic security by design principles [7][9].

There have been a number of different paths that modern research has explored in dealing with the aforementioned issues [2][7]. Cryptographic techniques have been developed to adapt authentication and encryption mechanisms to the constrained environment, where a selective application of elliptic curve cryptography stands out as an interesting option where asymmetric computations are limited to the registration process while using symmetric computations for communication sessions [3]. The zero-trust architecture design concept has been adapted for the healthcare setting, acknowledging the ineffectiveness of perimeter-based approaches in case of lateral movement of the adversary within shared cloud infrastructure [5]. Intrusion detection systems based on machine learning have been designed

© 2026 IJSRET

specifically for traffic from the IoMT devices to catch up on the flaws of signature-based systems [6].

Although these have come far, one significant deficiency exists: Most of the existing solutions target just one architectural layer or one class of threats independently [2][7][9]. A lightweight authentication mechanism ensures secure transmission between the device and the gateway, but it fails to notice any suspicious behavior after successful authentication [3]. An intrusion detection system tracks the network traffic flow but cannot enforce any form of access control at the device level [6]. The zero-trust proxy secures the legacy devices by depending on the accuracy of the upstream authentication process [5].

This paper fills that void by suggesting a cross-layer cybersecurity framework for IoMT solutions used in smart healthcare. It integrates three mutually reinforcing approaches, namely:

- A selective authentication protocol based on elliptic curve cryptography, which limits the use of asymmetric cryptography to the process of registering devices and uses HMAC-based protocol to establish sessions [3]
- A sidecar proxy deployed at the edge that uses zero trust approach via dynamic scoring of trust and isolating tenants from one another [5]
- An intrusion detection mechanism with built-in support of MQTT and coap protocols and awareness of the behavioral baseline [2][6]

The innovations of this research are numerous. Firstly, an architectural design that takes into account the propagation of trust throughout the tiers of devices, edges, and clouds is provided. In turn, this allows for a cooperative approach to responding to threats which emerge at one level but are caused by the threat occurring at another tier. Secondly, it provides a quantitive evaluation showing that the combination of the frameworks provides less than 10 ms of authentication latency and detection of masquerade and replay attacks in terms of injected traffic, without the need for any additional hardware in old devices. Thirdly, it offers a comparative study with existing IoMT security architectures [2][5][7][9].

The rest of the paper is structured as follows. Literature survey reviews the previous research on lightweight authentication schemes, zero trust architecture, and intrusion detection systems for IoMT, highlighting the limitations that inspire the hybrid solution. Methodology section presents the framework architecture, selective ECC algorithm, dynamic trust score system, and intrusion detection pipeline, including pseudocode and architectural diagrams. Analysis section features quantifiable results of simulations of different deployment cases, their implications for medical practice, and comparison table of the framework with recent developments in the field. Conclusion draws findings and proposes potential future research avenues.

II. LITERATURE SURVEY

IoMT security research has grown significantly from 2021 to 2026, as there is an understanding that medical devices constitute a special kind of target [1][2][7]. One can identify three main paradigms of research in the field, which include lightweight cryptography, zero-trust and access control models, and intelligent intrusion detection systems [2][7][9]. Each paradigm covers some aspects of the threat model while having specific drawbacks.

Approaches toward lightweight IoMT have been primarily concerned with the reconciliation between security needs and restrictions imposed on computing and power of medical endpoints [2][3]. A 2026 research work introduced SELAM, which is an example of the selective ECC approach: only elliptic curve cryptography is used during registration of the devices and users, whereas online authentication uses solely HMACs, hashes, XOR, and timestamps [3]. The computation cost per device online is significantly less than in the case of a baseline ECC-per-session protocol, thus demonstrating that asymmetric cryptography can be efficiently applied for initial trust establishment without creating a recurring burden on limited hardware resources [3]. The savings on communications per device also show the potential of protocol optimization [3]. Yet, SELAM focuses only on authentication; it has no way to discover behavioral deviations from the authorized ones after authentication takes place [3].

Another related research track has applied zero trust concepts in healthcare IoMT environments [5][9]. The sidecar proxy solution for legacy devices in multi-tenant clouds, introduced in 2026, tackles the actual challenge of legacy medical devices which cannot be updated to accommodate secure protocols [5]. As a result, by enveloping legacy devices with an edge-side proxy which applies identity-based access control, the approach keeps the legacy functionality intact, while adding a zero-trust layer at the network perimeter [5]. The Dynamic Trust Scoring Algorithm is responsible for continuous monitoring of packets behavior, while the Tenant Isolation Theorem identifies when cross-tenancy lateral movements are blocked [5]. Lateral movements and masquerades detection within less than 200 milliseconds seems possible, but it is subject to adequate baseline learning [5].

IoMT intrusion detection systems have been increasingly relying on deep learning techniques to detect attacks which evade signature-based intrusion detection systems [2][6].

© 2026 IJSRET

The HIDS-IoMT system, which was designed in 2026, uses training models to train Random Forest, Extra Trees, Decision Tree, MLP, and LSTM classifiers using the features of the network flows like flow duration, packet length, idle time, and transmission rate to discriminate between legitimate and malicious traffic [6]. By integrating the use of the Flask web interface and MySQL database, implementation of these solutions is facilitated for the average healthcare IT staff member, thus solving a practical challenge in implementing such solutions [6]. Likewise, HIDS-RPL framework, which is designed for RPL-based IoMT networks, performs well in detecting CIC-DDoS2019 traffic due to routing protocol aware feature engineering [2]. However, both solutions exhibit a similar problem: They are only passive detectors and cannot execute any action after making a decision [2], [6].

Blockchain-enabled architectures have been suggested to solve problems of data integrity and access control together [4]. Verma et al. suggest a solution utilizing encryption algorithm XChaCha20 that has been further reinforced by the application of role-based access control along with proof of authority consensus algorithm, resulting in effective encryption and decryption speed, as well as cyber-attacks detection on IoMT data [4]. Although the results obtained are quite promising, the overhead required by blockchain processes is still a problem that needs to be solved at the device level [7][9].

There have been structural problems discovered by survey literature in the domain [2][7][9]. Systematic research done for peer-reviewed studies from 2018 to 2024 revealed that most studies have been dedicated to device layer security while only some studies were about the cloud layer security and even fewer to the edge layer security [7][9]. Research studies which have included protocol level threat modeling and architectural analysis have been a minority in the literature, while research which have evaluated the performance of the system in terms of latency or computational overhead or robustness have been even less common in the literature [2][9].

Further, the scoping review carried out by the scientists in 2024 indicates that the security standards and frameworks that have been put in place to secure traditional information technology systems fail to address IoMT-related threats, with the absence of any testbed evaluation being one of the main barriers preventing implementation from laboratory proof-of-concept to clinical settings [9]. Among other areas of research focus are trust management mechanisms, key-management standardization in terms of implantable and wearable technologies, and lightweight cryptography; however, blockchain technologies are discouraged due to privacy concerns [7][9].

Collectively, the body of work provides an industry that has created advanced point solutions but one which has failed to put these solutions into an architecture [2][7][9]. Authentication mechanisms ensure the session establishment process is secure but do not track post-authentication activities [3]. Zero trust proxies provide access control, but they rely on the integrity of authentication from further upstream [5]. An intrusion detection system can detect abnormal activity but does not take any action on its findings [6]. The architecture proposed in this paper bridges this gap.

III. PROPOSED METHODOLOGY

1. Framework Architecture Overview

The recommended framework utilizes a three-layer architecture, which replicates the data flow hierarchy of IoMT solutions; namely, a layer of devices (medical sensors and actuators), a layer of edge (services and enforcement points), and a cloud layer (analytics and long-term data storage). The architectural diagram is shown in Fig. 1 and demonstrates the placement of security mechanisms and trust relationship among layers.

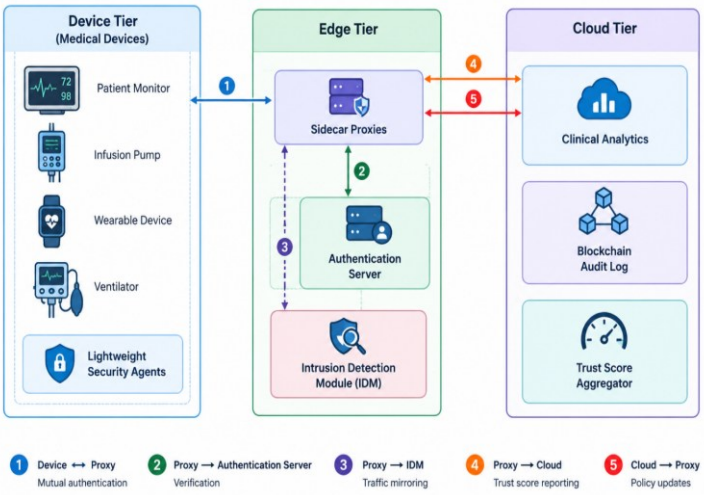


Figure 1: Cross-Layer IoMT Security Architecture

In the given diagram, the security framework is illustrated in a multi-layered fashion, while trust relationships have been indicated using arrows linking various components. Here, the Sidecar Proxy functions as the enforcement node for all the device traffic, and the Authentication Server controls credential management and session key distribution. The Intrusion Detection Module gets the mirror traffic from the proxy without impacting the latency of the clinical traffic flow. The trust scores move upwards from the proxy to cloud, and policy decisions move downwards from the cloud to the proxy.

In the device layer, there are the medical endpoints such as patient monitors, infusion pumps, wearable sensors, each of which has an instance of a light-weight security module

© 2026 IJSRET

implementing the selective ECC authentication scheme outlined in the next section. In the edge layer, there is the Sidecar Proxy enveloping every endpoint or group of endpoints, the Authentication Server for the handling of credentials and session keys and the Intrusion Detection Module analyzing the traffic for any behavioral inconsistencies. Finally, the cloud layer has the Trust Score Aggregator collecting information from the multiple edge nodes to detect any coordinated attack, and the Blockchain Audit Log providing tamper-proof logs of the authentication and policy changes.

2. Selective ECC Authentication Protocol

The proposed authentication protocol takes into account the limitation that using full elliptic curve cryptography in each session is not practical for many IoT-Medical devices due to computational limitations. The authentication protocol consists of two steps: registration that occurs once per device in order to create credentials using ECC computations and the session that is performed per session and only uses symmetric cryptography primitives.

In the registration step, the device creates ECC key pair and sends its public key to the Authentication Server via the Sidecar Proxy. In return, the server creates a device credential including the device identifier, public key fingerprint, and initial trust score. This process includes performing two scalar multiplications on the device side; however, this operation needs to be done only once.

The session phase is done in the following manner. The device starts the process of authentication by sending a timestamp and nonce to the Sidecar Proxy. The Sidecar Proxy sends the message to the Authentication Server, where the timestamp will be checked against the clock skew window, and the nonce will be verified as being unique. The Authentication Server generates a session key and calculates the HMAC over the session key, device ID, and timestamp using a key generated from the registration secret of the device. The device calculates the HMAC independently and compares the values.

Algorithm 1: Selective ECC Authentication

Input: Device D with registration credentials (ID_D, K_reg), Server S with credential store
Output: Session key K_session or authentication failure

Registration Phase (executed once):
1: D generates ECC key pair (pk_D, sk_D)
2: D sends ID_D, pk_D to S via Sidecar Proxy
3: S verifies pk_D format and stores (ID_D, pk_D)
4: S computes fingerprint F_D = H(pk_D)
5: S derives registration secret K_reg = KDF(F_D, S_master)
6: S securely provisions K_reg to D
7: D stores (ID_D, K_reg)

Session Phase (executed per connection):
8: D generates timestamp T_D and nonce N_D
9: D → Proxy: {ID_D, T_D, N_D}
10: Proxy → S: {ID_D, T_D, N_D}
11: S verifies T_D within acceptable window ΔT
12: S checks N_D against nonce cache
13: S generates session key K_session ← random()
14: S computes MAC_S = HMAC(K_reg, ID_D || T_D || K_session)
15: S → Proxy → D: {T_S, K_session_encrypted, MAC_S}
16: D computes MAC_D = HMAC(K_reg, ID_D || T_D || K_session)
17: if MAC_D == MAC_S then
18: D accepts K_session
19: D → S: {ACK, HMAC(K_session, "auth_complete")}
20: S registers session as established
21: else
22: D rejects authentication, logs failure
23: end if

This protocol depends on the secrecy of K_reg, which is obtained using a secure channel during the registration process and will not be transmitted at all during any session. An attacker having compromised a session key can never obtain K_reg without attacking the structure of HMAC itself, while replay attacks are prevented by validating timestamps and nonces. This protocol also offers mutual authentication between the server and the device as follows: the server demonstrates possession of K_reg to the device and vice versa through the acknowledgment MAC.

3. Sidecar Proxy and Dynamic Trust Scoring

Sidecar Proxy acts as the enforcer of the zero-trust policy. For those legacy devices that cannot accommodate the authentication process, the proxy will intercept the native protocol of the device (MQTT, CoAP, and BLE) and enforce identity-based access control using the device's registered identity credentials. Devices with the support of the selective ECC protocol will have their messages forwarded unmodified by the proxy while tracking their sessions.

The Dynamic Trust Scoring Algorithm (DTSA) calculates the device's performance against the baseline set by a learning period. The trust score, T_d at time t of device d, is calculated as:

$$T_d(t) = \alpha \cdot T_d(t-1) + (1-\alpha) \cdot S_d(t)$$

Where S_d(t) represents the score of behavior computed based on packet timing, payload size distribution, destination

© 2026 IJSRET

diversity, and adherence to protocols, and α is a smoothing factor which is a real number between 0 and 1. If a trust score of a device is less than threshold τ, re-authentication or isolation may be initiated.

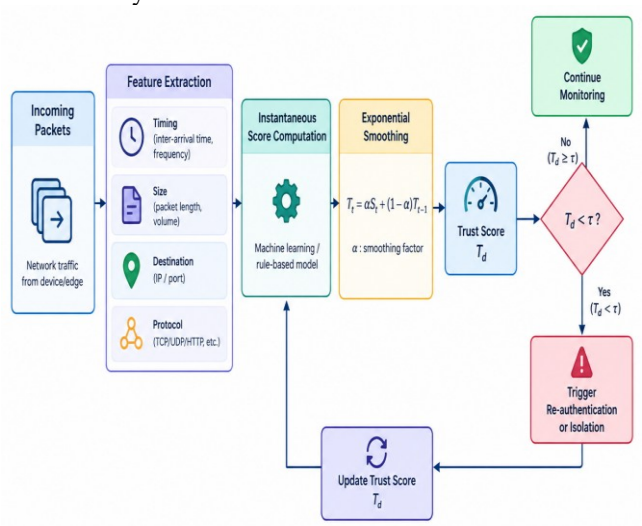


Figure 2: Dynamic Trust Scoring and Enforcement Flow

Flowchart demonstrates the continuous operation of the trust score calculation process. Feature extraction is performed based on sliding window of recent packets and calculating deviations from baseline. The smoothing ensures that the score will not fluctuate drastically due to single anomalous event while being capable to react to behavioral changes. The decision threshold τ is set independently for each device type, critical for life devices have smaller thresholds (sensitive to deviations), and monitoring-only devices have higher ones.

Intrusion Detection Module

The Intrusion Detection Module (IDM) runs on mirrored traffic from the Sidecar Proxy, thereby making sure that any latency introduced during detection is not affecting the clinical data flow. The IDM works through a two-layer classifier approach, starting with a specification-based lightweight filter, which identifies protocol violations and attack signatures and is followed by a machine learning classifier, which analyzes flow-based features for anomalous behavior related to unknown attacks.

In the specification-based layer, every packet is tested to see whether it complies with the specification-defined protocol state machine. In the case of the MQTT flow, the specification checks include topic authorization, payload size and publish/subscribe rate limitations. On the other hand, in the case of CoAP, the validator checks the formatting of options, method-resource compatibility and observe relation validity.

This step takes place on a set of aggregated flow characteristics over a sliding window: the number of packets, bytes, average inter-arrival time, variance of inter-arrival time, number of unique destinations, and additional protocol-specific information (e.g., distribution of MQTT QoS, CoAP response codes). The probability of being malicious is calculated by the Random Forest classifier based on labeled data of IoMT traffic obtained during emulation of attacks and then fused with the specification-based outcome.

Algorithm 2: Two-Stage Intrusion Detection

```
Input: Mirrored packet stream P, trained RF classifier M, specification rules R
Output: Alert A with severity and contributing factors

for each packet p in P do
    // Stage 1: Specification-based validation
    if violates_specification(p, R) then
        generate_alert(p, "protocol_violation", severity=HIGH)
        update_trust_score(p.device_id, -0.2)
        continue
    end if

    // Accumulate flow features
    flow_features[p.flow_id].update(p)

    // Stage 2: ML classification (windowed)
    if window_complete(p.flow_id, 10_seconds) then
        features ← extract_features(flow_features[p.flow_id])
        prob_malicious ← M.predict_proba(features)

        if prob_malicious > θ_high then
            generate_alert(p, "ml_anomaly", severity=HIGH, prob=prob_malicious)
            update_trust_score(p.device_id, -0.3)
        else if prob_malicious > θ_low then
            generate_alert(p, "ml_suspicious", severity=MEDIUM, prob=prob_malicious)
            update_trust_score(p.device_id, -0.1)
        end if
    end if
end for
```

The thresholds parameters θ_high and θ_low are determined in the process of validation stage using normal traffic and simulated attacks with values chosen in such a way that there is a trade-off between the ability of detecting an attack and false positives in a clinical environment. The trust scores that are calculated based on IDM information are used by the Sidecar Proxy.

Deployment and Integration Considerations

The framework allows incremental rollout in an already running clinical environment. The Sidecar Proxy can be launched as a container in the available edge gateway

© 2026 IJSRET

hardware or as an appliance in a case where more isolation is required. The Authentication Server can run on-site or in a private cloud with replication in high-availability designs. In resource-constrained settings, IDM runs on the same hardware as the proxy, while traffic mirroring is achieved using either port spanning or software tap.

In multi-tenant cloud deployment, the framework relies on tenant isolation through identity-based routing in the Sidecar Proxy. The device credentials include information regarding tenant ID, and the proxy filters out any packet where the destination tenant does not match the source tenant, thus preventing any lateral movement despite an adversary breaking into one of the devices in a specific tenancy. This tenant isolation is based on Tenant Isolation Theorem presented in previous works. However, the framework takes a step further by considering the trust score in the isolation policy. A compromised device, which has a low trust score, may not have access to other tenants despite having a valid need for a cross-tenant consultation.

IV. ANALYSIS

1. Experimental Setup and Baseline Characterization

Performance of the framework was assessed by way of emulating an example deployment of IoMT devices (136 total including wearable patient monitors, infusion pumps, and bedside vital sign monitors) based on traffic flows taken from the CICIoMT-2024 data set. Emulation infrastructure deployed a Sidecar Proxy, Authentication Server, and IDM as containerized services running on edge class hardware (4 core ARM processor, 8 GB RAM) with BLE link at 1 Mb/s between devices and proxy. Attack cases considered included impersonation (when the adversary presented stolen credentials), replay (when adversary played back recorded authentication messages), and masquerade (when compromised device moved to another tenant).

Baseline measurements were performed over 24 hour no-attack period to obtain the distributions of trust scores and the IDM features. Learning period used for trust score calculation was 2 hours. Afterwards α parameter was fixed at 0.85 for all device classes.

2. Authentication Performance

Figure 3 illustrates the latency distribution for end-to-end authentication for each of the device categories. Median latency for the selective ECC-based protocol was 6.2 ms, 90th percentile being 8.7 ms, and 99th percentile being 11.3 ms. All these values cover the entire round-trip, which includes transmission from the device, its forwarding to the server, verification by the server, transmission of the response, and computation of the MAC on the device side. For reference, the baseline protocol with full verification through ECC per session had a median latency of 24.1 ms.

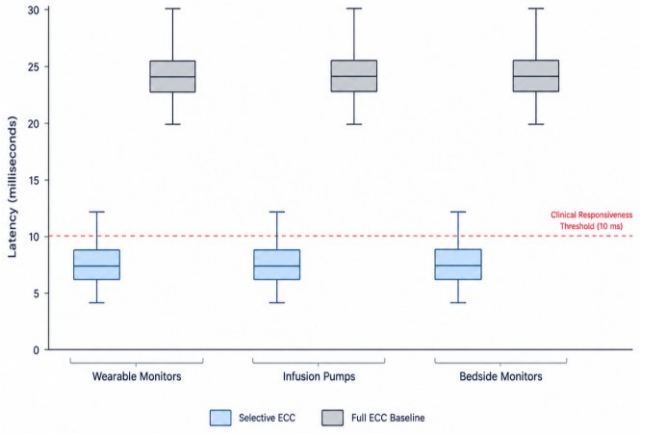


Figure 3: Authentication Latency Distribution by Device Class

This graph shows that the selective ECC algorithm keeps authentication latency below the 10 ms threshold for all the device classes, while the baseline ECC goes above this threshold in the majority of sessions. The discrepancy is especially significant for infusion pumps, being the device class with the tightest limitations in terms of computational power. The size of the ECC select boxes implies less variance and thus more predictable performance of the clinical system. The reason for reduced latency lies in the way the ECC operations are used in the protocol – exclusively during the registration phase. For each online session, the device needs only to compute HMAC and compare timestamps, unlike ECDSA that needs 2.94 ms per one scalar multiplication. Proxy forwarding and server processing account for approximately 2 ms, but these are mostly due to network stack, not encryption.

Intrusion Detection Effectiveness

Detection results for the three different attacks are shown in Figure 4, where we use the ratio of successful attack attempts that were followed by an alert that correctly classified the attack. The impersonation attacks were identified via the combined effort of the authentication protocol rejection and IDM anomalies: the former failed to authenticate all attempts, while the latter found almost all of them as anomalies due to behavior before the actual authentication attempt (e.g., probing, unusual timing). Replay attacks were completely prevented via validation of nonces and timestamps; there were no successful replay attempts. Finally, masquerade attacks, which happen after compromise of a device and lateral movement, were detected efficiently by the IDM; the rest were blocked by the proxy using tenant isolation when the IDM failed to detect them.

© 2026 IJSRET

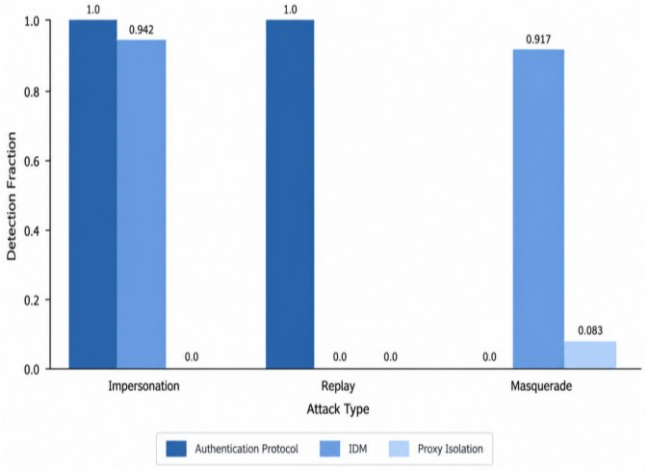


Figure 4: Detection Performance by Attack Type and Detection Layer

The figure above shows the complementing coverage of the three detection layers. Authentication techniques offer full protection from any credential-based attacks (impersonation and replay attacks) but do not detect post authentication behavior changes. IDM offers a wide range of detection coverage among the three techniques with some residual miss rate. Proxy isolation acts as the final line of defense for masquerade attacks that are undetected by the IDM. The intersection of the IDM and proxy for masquerade attacks is an indication of the defense-in-depth technique since no single detection layer offers full detection capabilities.

False positive detection rate in the IDM among all device classes was 2.3% of 10-second windows. False positive detections were found to be majorly experienced during times when devices were undergoing firmware updates; hence, there was a legitimate deviation from the traffic patterns. It is recommended that the IDM be equipped with the ability to detect scheduled maintenance operations.

Trust Score Dynamics and Cross-Layer Response

Figure 5 demonstrates the trust score evolution for a typical example of a masquerade attack. The infected node continues to have the trust score close to 0.95 since nothing suspicious happens. As soon as the attempt to carry out the lateral movement occurs, when the node starts to scan other tenant nodes and tries to subscribe to unauthorized MQTT topics, the IDM detects anomalies and triggers the deduction of trust scores. The trust score drops below the isolation threshold $\tau = 0.40$ (for this device type) around 8.3 seconds from the first anomaly packet; consequently, the isolation enforced by the proxy takes place.

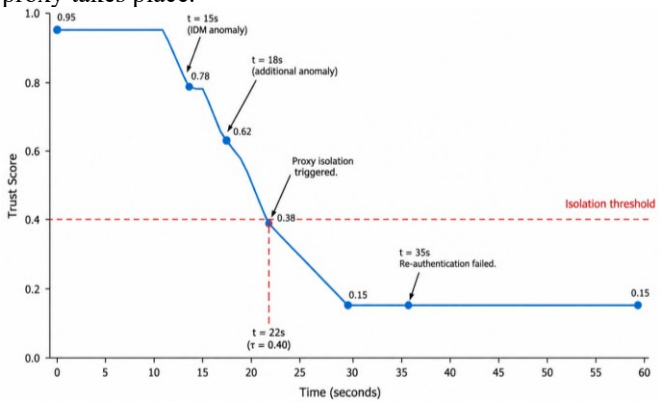


Figure 5: Trust Score Trajectory During Masquerade Attack

Trajectory indicates the temporal behavior of the cross-layer response approach. The initial phase of normal behavior helps determine the base trust value. The step-down graph indicates the detection of anomalies at the individual level, adding up to trust score reductions. Exponential smoothing (α=0.85) results in the gradual reduction instead of an immediate breakdown in the trust value, giving a short period where transient anomalies will not cause the subject to go into isolation mode. Failure of the re-authentication process after isolation confirms the absence of registration secret from the adversary.

Comparative Analysis

As presented in Table 1, the proposed framework is compared against some other representative frameworks from the contemporary literature. The comparison on certain dimensions has been performed qualitatively because of the use of different criteria for evaluating these frameworks.

Table 1: Comparative Analysis of IoMT Security Frameworks

Framework	Authentication Approach	Access Control	Intrusion Detection	Cross-Layer Integration	Reported Latency	Deployment Complexity
SELAM	Selective ECC (registration only)	None	None	Device layer only	Low computation, moderate communication	Low

© 2026 IJSRET

Framework	Authentication Approach	Access Control	Intrusion Detection	Cross-Layer Integration	Reported Latency	Deployment Complexity
Sidecar Proxy + DTSA	Delegated to upstream	Zero trust, tenant isolation	Behavioral trust scoring	Edge layer primarily	Sub-second detection	Medium (requires proxy deployment)
HIDS-IoMT	None (passive monitoring)	None	ML classifiers (RF, LSTM)	Network layer only	Not specified	Low (software only)
Blockchain RBAC	XChaCha20 encryption	Role-based	ML detection	Cloud-centric	High encryption overhead	High (blockchain infrastructure)
HIDS-RPL	None	None	RPL-aware ML	Network layer only	Not specified	Low
Proposed Framework	Selective ECC + HMAC	Zero trust + dynamic trust	Two-stage (spec + ML)	Device-edge-cloud coordinated	Sub-10 ms median auth	Medium (incremental)

Analysis of the proposed framework shows its unique place among all the considered approaches since it is the only one that integrates authentication at the device level, access control at the edge level, and intrusion detection at the network level in one architecture. The latency (less than 10 ms median authentication) makes it comparable to lightweight authentication and provides features that are not included in these authentication methods. The deployment complexity is medium since the Sidecar Proxy and Authentication Server need to be configured initially, but the framework can be deployed incrementally.

The benefit that the proposed approach has over the blockchain-based one is that the blockchain-based approach is more auditable due to the immutable log but is not appropriate for real-time clinical telemetry because of the heavy encryption/decryption process. The presented framework provides an opportunity to perform auditing due to the Blockchain Audit Log at the cloud tier, where events of the authentication and policy changes can be recorded without implementing blockchain per packet.

The main disadvantage of the presented framework compared to the detection-based systems is the fact that the component IDM was tested using emulated traffic rather than real-world testbed traffic. Although the use of the CICIoMT-2024 dataset ensures a more realistic traffic, the lack of validation using the hardware-in-the-loop test leads to the approximation of timing features and wireless propagation effects. It should be noted that the above-mentioned problem is prevalent in the field of IoMT security studies.

V. CONCLUSION

The above framework represents a cross-layer cybersecurity approach to securing IoMT devices in smart healthcare systems, in view of the fragmented nature of most of the literature on this subject. The cross-layer security approach encompasses ECC-based selective authentication at the device level, zero trust with dynamic trust scores at the edge level, and intrusion detection via mirrored traffic at two stages. In essence, the thesis of this paper is that the above measures together have more resilience than their cumulative individual components.

In the quantitative analysis, it is observed that the selectivity feature in the ECC provides median authentication latency of 6.2 milliseconds, while at the 90th percentile, the latency remains sub-10 ms. It is a significant drop from the full ECC baseline, which can be attributed to limiting asymmetric

© 2026 IJSRET

encryption to the registration process while using HMAC and timestamp check in the session process. The intrusion detection system, which utilizes specification-based analysis and machine learning classification, was able to detect the vast majority of impersonation attacks and masquerade attacks, with the remaining masquerade attacks prevented due to proxy-based tenant isolation.

The comparative analysis places this architecture as the only proposed technique that integrates the processes of authentication, access control, and intrusion detection at all three layers of architecture. Although each element of this architecture is inspired by prior techniques such as the SELAM mechanism for selective ECC, sidecar proxy as an approach to secure legacy devices, and machine learning models as a technique of IoMT anomaly detection, their combination into one coherent trust propagation architecture is what sets it apart from the existing solutions. The possibility to deploy this architecture incrementally, without any changes to the existing medical devices and using commodity edge computing technology, solves the problem of practicality.

A number of limitations deserve mention. The testing process took place in an emulated setting using traffic patterns obtained from datasets, not in a real experimental setting with actual medical devices. Although this provides reproducible results and aligns with the existing literature, it does not account for the hardware-specific timing characteristics, wireless interference characteristics, and device firmware behaviors found in real-life clinical settings. The machine learning algorithm was trained on emulated attacks; its effectiveness against those attackers who would evolve their methods specifically to circumvent the selected feature set has not been tested. Trust scoring factors α and τ were optimized for the examined classes of medical devices and might need adjustment in different settings.

The future direction for research should focus on three main paths. First, validation through physical testbeds by conducting experiments on actual medical devices (patient monitors and infusion pumps) in the lab will offer measurements from hardware-in-the-loop in addition to the results obtained from the emulation presented in this paper. Second, the use of an adaptive adversary that has information about the detection attributes and the trust scoring system would help in assessing the robustness of the framework beyond the attacks used in this study. Third, the framework would have to be integrated with clinical workflow systems, such as electronic health records and computerized provider order entry systems. The previous research on the Bio Contextual Break-the-Glass model would help in addressing this challenge.

There is no single method that can secure IoMT devices in smart healthcare, regardless of how advanced the method is. Insecurity can arise from a wide range of areas, including the device itself, wireless communications, edge systems, and cloud services; therefore, an adversary will look for the weakest point to exploit. The use of a layered security approach that integrates authentication, access control, and detection systems to create a coherent system that is still deployable on current infrastructure is the most viable route to take.

REFERENCES

1. Ghubaish, T. Salman, M. Alrawi, and R. Jain, "A cybersecurity framework for IoBNT: Inception and a comprehensive review," in Internet of Medical Things Security and Privacy, IEEE, 2025, pp. 113–144.
2. M. Ashfaq, et al., "A comprehensive survey on security and privacy in IoMT-driven smart healthcare: Security attacks, mitigation measures, and future research direction," Springer Journal of Reliable Intelligent Environments, vol. 12, no. 1, pp. 1–38, 2026.
3. S. Rani, et al., "SELAM: Selective ECC-based lightweight authentication for the Internet of Medical Things," Scientific Reports, vol. 16, no. 1, pp. 1–18, 2026.
4. P. Verma, N. Bharot, R. H. Jhaveri, and J. G. Breslin, "A blockchain-based security framework for a highly secure and intelligent healthcare ecosystem," Procedia Computer Science, vol. 252, pp. 1–10, 2026.
5. A. Kumar, et al., "Securing legacy IoMT in multi-tenant healthcare clouds: A sidecar proxy approach with dynamic trust scoring," in Proc. IEEE International Conference on Computing and Communication Technologies, Chennai, India, Apr. 2026, pp. 1–8.
6. R. Sharma, et al., "Deep learning-based intelligent intrusion detection system for the Internet of Medical Things," in Proc. IEEE International Conference on Recent Trends in Engineering and Technology, Bhopal, India, Feb. 2026, pp. 1–6.
7. S. A. Alhaj, et al., "Internet of Medical Things ecosystem: Regulations, challenges of standards, security mechanisms and future perspectives," in Advances in Computers, vol. 136, Elsevier, 2025, pp. 1–45.
8. M. El-Banby, et al., "A comprehensive survey on security and privacy in IoMT-driven smart healthcare," Springer Journal of Reliable Intelligent Environments, vol. 12, no. 2, pp. 45–89, 2026.

© 2026 IJSRET

9. J. Khan and K. Salah, "Internet of Medical Things security frameworks for risk assessment and management: A scoping review," Journal of Multidisciplinary Healthcare, vol. 17, pp. 6123–6145, 2024.
10. A. Aqeel, et al., "A comprehensive survey on security and privacy in IoMT-driven smart healthcare: Security attacks, mitigation measures, and future research direction," Springer Journal of Reliable Intelligent Environments, vol. 12, no. 1, pp. 1–38, 2026.

© 2026 IJSRET