Scientific Reports

https://doi.org/10.1038/s41598-026-56106-3

Article in Press

A MITRE D3FEND guided blockchain based cyber resilient framework for IPv6 based 6G enabled healthcare networks

Received: 24 March 2026

Accepted: 28 May 2026

Published online: 03 June 2026

Cite this article as: Rohith K., Jain A. & Shaik M.N. A MITRE D3FEND guided blockchain based cyber resilient framework for IPv6 based 6G enabled healthcare networks. *Sci Rep* (2026). https://doi.org/10.1038/s41598-026-56106-3

Katreddi Rohith, Abhishek Jain & Mahmmad Nazir Shaik

A MITRE D3FEND Guided Blockchain Based Cyber Resilient Framework for IPv6 Based 6G Enabled Healthcare Networks

Katreddi Rohith,*Abhishek Jain, Mahmmad Nazir Shaik

School of Engineering and Technology, BML Munjal University, Gurugram 122413, India.

e-mail: katreddi.rohith.21cse@bmu.edu.in, abhishek.jain@bmu.edu.in, shaikmahmmad.nazir.21cse@bmu.edu.in

ORCID: 0009-0004-9484-4753; 0000-0001-9018-9203; 0009-0006-1652-5073

ABSTRACT

The proliferation of Internet of Medical Things (IoMT) devices in 6G-enabled healthcare networks introduces critical cybersecurity challenges, including expanded attack surfaces, device heterogeneity, and real-time security requirements that traditional perimeter-based frameworks cannot adequately address. This paper proposes a Blockchain-Enabled Zero-Trust Architecture (B-ZTA), guided by the MITRE D3FEND defensive ontology, integrating Zero Trust micro-segmentation, a Random Forest-based intrusion detection system, and a lightweight Proof-of-Authority blockchain for deterministic policy enforcement. The framework is validated through MATLAB-based simulations rather than physical IoMT deployment, across 30 independent trials under diverse cyberattack scenarios in a simulated 62-device hospital environment. Under the evaluated scenarios, results indicate a 99.10% Threat Neutralization Rate, mean enforcement latency of 76.68 ms, and 95th percentile latency of 249.86 ms, satisfying 6G eMBB and mMTC latency requirements for IoMT monitoring use cases. Quantitative benchmarking against five state-of-the-art frameworks yields a composite security score of 91.8. These findings suggest promise for the B-ZTA approach within the simulated environment, with physical testbed validation and adversarial robustness evaluation identified as priority directions for future work.

Key Words:

Internet of Medical Things (IoMT), 6G Networks, Zero Trust Architecture (ZTA), Blockchain Security, IPv6, Proof-of-Authority (PoA), Random Forest, Intrusion Detection System (IDS), Cybersecurity, Threat Detection, Threat Neutralization, Ultra-Low Latency, MATLAB Simulation, Healthcare Security, Adaptive Security Framework.

INTRODUCTION

The healthcare industry is undergoing a profound transformation, driven by the synergistic fusion of the Internet of Medical Things (IoMT) and next-generation communication technologies. The advent of 6G networks promises to be a key enabler for this revolution, offering the ultra-reliable low-latency communication (URLLC)[40], massive machine-type communication (mMTC), and enhanced mobile broadband (eMBB) required to support a new generation of medical applications. This technological convergence facilitates a paradigm shift from reactive treatment to proactive and personalized care, enabling capabilities such as continuous, real-time patient monitoring via wearable and implantable sensors, high-fidelity telesurgery with haptic feedback, and AI-driven diagnostic systems that process vast datasets in real time. The simulated environment in this research reflects this complexity, modeling a modern hospital ecosystem with a diverse array of interconnected devices ranging from life-critical ICU ventilators and ECG monitors to diagnostic imaging equipment and administrative workstations all operating on a unified 6G and IPv6 network backbone. While the clinical benefits are undeniable, this hyper-connectivity introduces cybersecurity challenges of significant scale and complexity. Each of the billions of IoMT devices expected to be deployed represents a potential entry point for malicious actors, expanding the attack surface far beyond the confines of a traditional hospital network. The IoMT landscape is fraught with inherent vulnerabilities, including the widespread use of legacy devices with unpatchable firmware, weak or default authentication credentials, insecure communication protocols, and a lack of built-in security features. These weaknesses make IoMT ecosystems prime targets for a range of devastating cyber-attacks, such as ransomware that can cripple hospital operations, Denial-of-Service (DoS) attacks that render critical devices unavailable, and data theft targeting sensitive Protected Health Information (PHI). In the IoMT context, the consequences of a security breach extend far beyond financial loss or data exposure; they pose a direct and immediate threat to patient safety and human life. A compromised smart infusion pump could administer an incorrect medication dose, or a disabled ventilator could impair respiratory support, highlighting the life-critical nature of IoMT cybersecurity. Traditional security strategies, architected around a well-defined network perimeter, are fundamentally ill-equipped to address this new reality. The concept of a trusted internal network and an untrusted external network become obsolete in an environment where data flows seamlessly between on-premises devices, cloud platforms, and remote clinicians. The decentralized, heterogeneous, and dynamic nature of IoMT 4 demands a security paradigm that is data-centric, identity-aware, and continuously adaptive. Existing security frameworks for IoMT, while valuable, often lack the dynamic capabilities to respond to the evolving threat landscape in real time, treating security as a static configuration rather than a continuous process.

This Study addresses these profound challenges by proposing and validating a holistic and adaptive security framework for 6G-enabled IoMT environments. The core contribution of this work is multifaceted, resting on three foundational pillars that collectively create a resilient and intelligent defense architecture: 1. A Practical Implementation of Zero Trust Architecture (ZTA): Moving beyond theoretical principles, this research presents a concrete, policy-driven implementation of ZTA within a simulated hospital network. By enforcing strict access controls based on continuous verification of identity, device posture, and context, the framework fundamentally reduces the inherent trust that attackers exploit for lateral movement. 2. Systematic Threat Modeling and Defense-in-Depth: The framework is built upon a rigorous security foundation established through the systematic application of the STRIDE threat modeling methodology. This process enables the identification of specific threats to each class of IoMT device, which are then mapped to a multi-layered set of defense-in-depth controls, including network micro-segmentation, strong multi-factor and biometric authentication, and ro- bust, context-appropriate encryption standards (e.g., AES-256, WPA3, TLS 1.3). 3. A Novel An adaptive intrusion detection system (IDS) utilizing Random Forest algorithms that persistently assesses network behaviour through traffic and entropy-based characteristics to produce real-time risk assessments: The framework's primary innovation lies in its capacity for autonomous adaptation. It incorporates a machine learning model that serves as an intelligent risk assessment engine. This model continuously analyzes network behavior and device telemetry to predict threats and calculate real-time risk scores. These scores, in turn, drive a dynamic policy engine that can automatically adjust segmentation rules, block malicious communication paths, and isolate compromised devices, creating a self-improving security ecosystem that learns from and responds to attacks.

Research Questions and Contributions

This research is guided by the following questions:

RQ1: Can the integration of Zero Trust micro-segmentation, AI-driven intrusion detection, and PoA blockchain enforcement achieve measurable improvements in threat neutralization rate over individual components in a simulated 6G IoMT hospital environment?

RQ2: What is the end-to-end enforcement latency of the B-ZTA framework, and is it compatible with the latency envelope of 6G eMBB and mMTC use cases for remote patient monitoring?

RQ3: How does the B-ZTA framework perform relative to state-of-the-art IoMT security frameworks across standardised detection and enforcement metrics?

RQ4: What are the scalability and energy efficiency characteristics of the proposed framework as the IoMT device count increases?

In response to these questions, this paper makes the following measurable contributions:

C1: A unified B-ZTA framework that achieves a 99.10% Threat Neutralization Rate across 30 simulation trials under five attack categories in a 62-device simulated hospital network compared to 85% for ZTA-only and 74% for RF-IDS-only baselines.

C2: A mean end-to-end enforcement latency, empirically decomposed across four components: RF Inference (20 ms), ZTA Policy (3.5 ms), AES-256 (0.1 ms), and PoA Verification

C3: A quantitative benchmark demonstrating a composite security score of 91.8 against five published IoMT security frameworks, with the lowest false positive rate (0.3%) among all compared systems.

C4: A systematic MITRE D3FEND technique mapping for all framework components, providing a reproducible and auditable defensive design methodology for 6G IoMT security engineering.

The remainder of this research is organized as follows. Section 3 provides 5 a comprehensive review of related work in IoMT security, Zero Trust Architecture, threat modeling, and AI-driven defense. Section 4 details the system architecture and threat model of the simulated 6G-IoMT hospital network. Section 5 presents the design and methodology of the proposed four-phase adaptive security framework. Section 6 presents and discusses the detailed results of the simulation, evaluating the framework's performance against a series of cyberattacks. Finally, Section 7 concludes the study, summarizing the key findings, acknowledging limitations, and outlining directions for future research. The proposed B-ZTA framework is implemented and validated using MATLAB R2026a, with full details of the simulation environment, methodology, and results presented in the subsequent sections.

Throughout this paper, the proposed framework is referred to as the Blockchain-Enabled Zero Trust Architecture (B-ZTA). The title references MITRE D3FEND to acknowledge the knowledge base that guided the selection and mapping of defensive techniques employed within the B-ZTA framework. Specifically [42], MITRE D3FEND is used as a structured reference taxonomy to ensure that each security control including network micro-segmentation, encryption, anomaly-based detection, and access revocation maps to a recognized and standardized defensive technique. The B-ZTA is therefore the implemented framework, while MITRE D3FEND serves as the guiding ontology that validates and structures its defensive design. These two terms are complementary, not interchangeable, and this distinction is maintained consistently throughout the paper.

RELATED WORK

A comprehensive understanding of the proposed framework requires situating it within the broader context of existing research. This section reviews the state-of-the-art across five critical domains: the IoMT threat landscape, the principles and application of Zero Trust Architecture, methodologies for threat modeling, the use of Artificial Intelligence in cybersecurity, and foundational security controls relevant to IoMT.

A. The IoMT Threat Landscape:

The widespread use of connected medical devices has made an ecosystem that is both rich and fragile. The differences among the devices, the lack of sufficient resources, and the critical importance of the data they manage contribute to numerous security and privacy problems [1]. The IoMT landscape is all about dealing with problems that are happening right now and setting the stage for new research trends in the future [2]. A lot of research is focused on security and privacy frameworks for IoMT [3]. Remote hijacking of devices, impersonation attacks, man-in-the-middle attacks, and password guessing are all common threats that have been well-documented in the literature. These attacks can lead to the unauthorized disclosure or alteration of important patient data [1]. Adapting strategies for IoMT and AI is also part of dealing 6 with new cyber threats in healthcare [4]. Ransomware attacks are more advanced and can make whole hospital systems unusable [1]. Denial-of-Service (DoS) attacks can also stop life-saving equipment from working [1]. Malware and DDoS attacks are also big security holes for IoMT [5]. Cybersecurity threats to healthcare systems that use IoMT are a big worry, and researchers have looked into security holes and smart ways to fix them for IoMT systems[23]. The IoMT is also a key part of smart health monitoring systems, and its progress, along with 5G technology, helps find problems with healthcare cybersecurity [22], [26]. An overview of the Internet of Medical Things (IoMT) also talks about its structure, protocols, and uses [6], [24]. These weaknesses are often caused by basic design problems, like using default credentials, not encrypting communication channels, using old firmware, and having insecure APIs [1]. Researchers have also used Markov chains and the Common Vulnerability Scoring System (CVSS) to find and model security threats for IoMT edge networks [25]. This well-known threat landscape directly informs the simulated attack scenarios, which include Credential-Stuffing, Data-Theft, DoS, and Device-Takeover. This makes sure that the framework is useful for real-world cyber threats [1]. In addition, 6G technology will be used in smart hospitals in the future, which will create both challenges and opportunities for better healthcare services [7]. This includes using Cybertwin technology for next-generation 6G networks to improve healthcare solutions [8] and coming up with security plans to deal with any weaknesses that might be found in 6G technologies used in

healthcare [9]. A full survey has also been done on how 6G technology can improve the Quality of Experience for M-health multimedia apps.

B. Zero Trust Architecture in Critical Infrastructure

To overcome the shortcomings of conventional perimeter-based security, Zero Trust Architecture (ZTA) has arisen as a formidable framework for safeguarding distributed systems. Defined in NIST Special Publication 800-207 [7],[41], Zero Trust Architecture (ZTA) adheres to the idea of "never trust, always verify," hence abolishing implicit trust and mandating ongoing authentication and authorization for each access request. Previous studies [8], [9] illustrate the efficacy of ZTA in alleviating insider risks and limiting lateral movement via micro-segmentation and least privilege access protocols. Nonetheless, actual implementation obstacles remain, especially in IoMT settings marked by outdated medical devices and fluctuating network conditions. As noted in [10], the majority of current ZTA implementations are static and policy-driven, missing the adaptive capabilities and real-time enforcement mechanisms essential for compliance with stringent 6G latency standards.

C. Threat Modeling Methodologies

Threat modeling is essential for discovering vulnerabilities and architecting secure systems. The STRIDE architecture, developed by Microsoft and elaborated in [11], is extensively utilized for its systematic categorization of threats into spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. Alternative methodologies like PASTA and risk-centric threat modeling tools [12] provide thorough analysis; nevertheless, they frequently increase complexity that constrains their use in real-time systems. Regulatory standards, particularly those from the U.S. Food and Drug Administration, underscore the necessity of systematic threat modeling for the validation of medical device security. Nonetheless, current systems generally see threat modeling as a static design-time task and do not include risk assessment into runtime decision-making processes, thereby constraining their efficacy in dynamic IoMT situations.

D. AI-Driven Intrusion Detection Systems

Artificial Intelligence (AI) and Machine Learning (ML) methodologies are essential in contemporary cybersecurity because of their capacity to identify complex and novel threats. Conventional signature-based intrusion detection systems are inadequate for detecting zero-day assaults, resulting in a heightened utilization of machine learning-based anomaly detection methods [14], [27]. Diverse models, such as Random Forest (RF), Support Vector Machines (SVM), and deep learning architectures, have been investigated for intrusion detection in IoT and IoMT systems [15], [16]. Random Forest classifiers are notably beneficial owing to their superior accuracy, resilience to noisy input, and very low computing complexity. Recent studies [13], [17], [31], [32], [38] advance AI-based intrusion detection to adaptive security frameworks that can generate automated responses. Nevertheless, a significant limitation persists, as the majority of AI-driven systems concentrate exclusively on threat detection and lack deterministic enforcement

mechanisms, particularly under real-time operating limitations. Standard IoMT security datasets such as CICIDS2017 [35], TON-IoT, and CICIoMT2024 provide established benchmarks for intrusion detection evaluation. The current framework does not evaluate against these datasets, a limitation that future work will address through cross-dataset validation [36].

E. Blockchain-Based Security in IoMT

Blockchain technology has been explored as a method to improve security in IoMT contexts by offering decentralized trust, immutability, and transparent auditability. Blockchain-based systems have been suggested for safe data sharing, identity management, and access control within distributed healthcare networks[18],[28],[29],[34]. Traditional consensus algorithms, such as Proof-of-Work (PoW), impose considerable latency and computational burden, rendering them inappropriate for time-sensitive medical applications [19]. To mitigate this constraint, new research [20] investigates lightweight consensus solutions like Proof-of-Authority (PoA), which provide diminished computing demands and expedited transaction validation [37]. Notwithstanding these developments, current blockchain-based IoMT solutions predominantly emphasize data integrity and are deficient in integration with AI-driven threat detection systems. Moreover, they are infrequently evaluated under the latency constraints necessary for 6G-enabled healthcare settings.

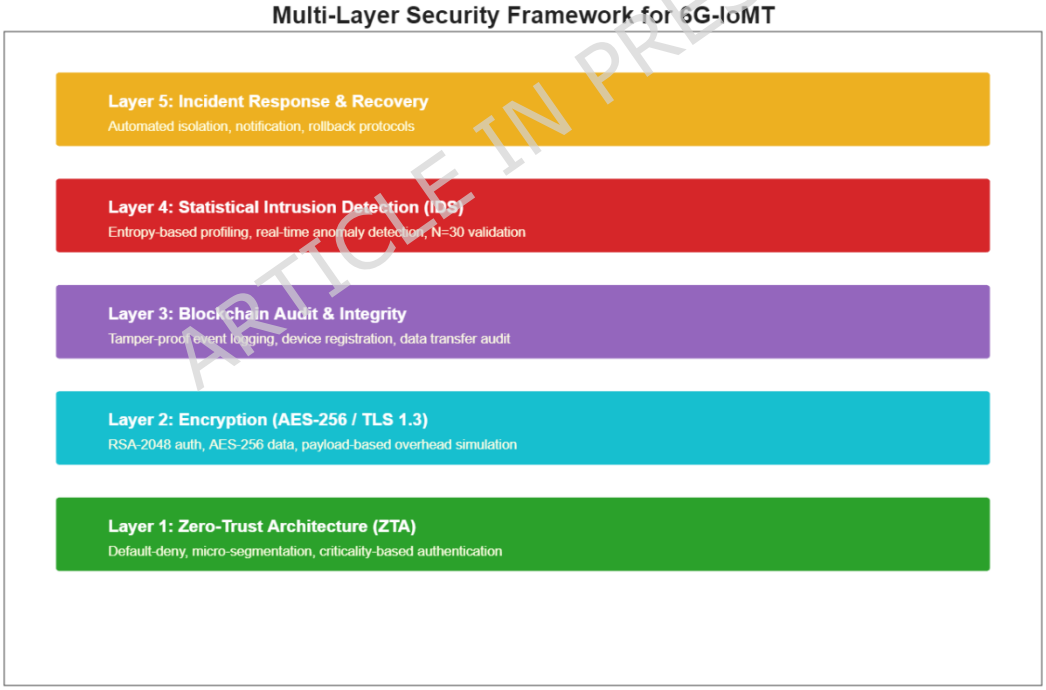


Fig. 1. MATLAB-based system architecture of the proposed B-ZTA framework integrating AI-driven detection and PoA-based enforcement.

F. Positioning of This Work

This work presents a Blockchain-Enabled Zero Trust Architecture (B-ZTA) to mitigate these constraints, incorporating Zero Trust micro-segmentation, a Random Forest-based intrusion detection system, and a lightweight Proof-of-

Authority blockchain for deterministic enforcement. The framework is executed in MATLAB R2026a and assessed via 30 independent simulation experiments. The findings indicate a 99.10% threat neutralization rate, satisfying practical real-time constraints in IoMT systems, confirming the viability of a fully integrated, real-time security solution for next-generation IoMT systems.

The precise novelty of this work lies in four contributions that, taken together, distinguish it from existing IoMT security frameworks. First, while prior works address Zero Trust, AI-based detection, or blockchain enforcement in isolation, this framework is the first to integrate all three within a unified, closed-loop architecture where each component directly informs the others: the Random Forest classifier feeds risk scores to the ZTA policy engine, which triggers the PoA blockchain for deterministic enforcement. Second, the use of MITRE D3FEND as a structured guiding ontology rather than ad hoc control selection ensures that every defensive mechanism is traceable to a recognized technique, providing a reproducible and auditable security design methodology. Third, the introduction of a Composite Risk Score that dynamically weights device connectivity, criticality, and exposure enables context-aware, per-device security decisions that static policy frameworks cannot achieve. Fourth, the framework is the first to evaluate this integrated architecture specifically under 6G eMBB and mMTC latency constraints in a realistic 62-device hospital simulation, providing empirical evidence that the combined overhead of AI detection and blockchain enforcement remains compatible with real-time clinical requirements.

G. Foundational Security Controls in IoMT

The proposed framework incorporates numerous essential security controls, whose significance is well-documented in the literature and vital for safeguarding diverse IoMT environments. Network segmentation and micro-segmentation are fundamental tactics for constraining the impact of a potential security breach. Micro-segmentation efficiently inhibits lateral movement by adversaries through the division of the network into smaller, isolated zones according to device functioning and criticality. This method is especially beneficial in IoMT environments, where legacy devices with restricted security features can be confined within strictly regulated segments, thus minimizing their vulnerability to wider network attacks [17].

Besides segmentation, strong authentication procedures are essential for ensuring safe access control. Conventional password-based authentication methods are widely acknowledged as inadequate for contemporary IoMT settings due to their vulnerability to brute-force and credential-stuffing attacks. As a result, the implementation of robust authentication methods, including multi-factor authentication (MFA), has gained significant traction. Multi-Factor Authentication necessitates various verification methods, hence substantially enhancing the challenge for unwanted access. Moreover, biometric authentication techniques, which depend on distinct physiological traits, offer an enhanced security layer for high-criticality medical equipment and systems. The implementation of advanced authentication procedures significantly improves system resilience, especially when customized for device sensitivity and operational context [18], [19].

Encryption serves as a fundamental pillar of IoMT security, safeguarding data confidentiality and integrity inside decentralized healthcare networks. Due to the sensitive nature of medical data, end-to-end encryption is crucial for safeguarding information both in storage and during transmission. Previous studies underscore the necessity of utilizing standardized and resilient cryptographic protocols, such as Transport Layer Security (TLS) for secure communication, Advanced Encryption Standard (AES) for data storage, and Wi-Fi Protected Access 3 (WPA3) for safeguarding wireless connectivity [11]. The suggested system implements these encryption algorithms contextually, adapting the protocol selection according to device type, communication requirements, and data sensitivity. Medical imaging data transmissions are secured by specialized protocols like DICOM-Secure, assuring adherence to healthcare data protection requirements.

In summary, the existing literature reveals four persistent gaps that directly motivate this work. First, studies focused on ZTA for IoMT, such as those reviewed in [8] and [9], demonstrate micro-segmentation benefits but lack real-time, automated enforcement mechanisms capable of meeting 6G URLLC latency requirements. Second, AI-driven IDS frameworks [14], [15], [16], [39] achieve strong detection accuracy on benchmark datasets but operate as standalone components without integration into a policy enforcement layer, meaning detection does not guarantee containment. Third, blockchain-based IoMT security solutions [19], [20] provide immutability and auditability but are evaluated primarily on data integrity tasks, with no coupling to AI-driven anomaly detection or adaptive risk scoring. Fourth, STRIDE-based threat modeling studies [21] treat threat identification as a design-time activity rather than a runtime input to dynamic security decisions. The proposed B-ZTA framework directly addresses each of these gaps through its integrated, closed-loop architecture, empirically validated under realistic 6G hospital network conditions.

METHODOLOGY

A robust and realistic simulation requires a meticulously defined environment. This section details the architecture of the simulated 6GIoMT hospital network, the characteristics of its constituent devices, the communication patterns, and the systematic threat model used to assess its vulnerabilities. The methodology is organized into five logical stages that reflect the complete security engineering process. Stage 1 defines the network model, establishing the hospital topology, device inventory, IPv6 addressing, and communication patterns. Stage 2 presents the threat model, applying STRIDE analysis across all device categories to identify vulnerabilities and compute attack surface scores. Stage 3 details the intrusion detection model, describing the Random Forest classifier, feature extraction, and threshold selection. Stage 4 describes the blockchain enforcement layer, including the PoA consensus mechanism, smart contract logic, and block structure. Stage 5 presents the risk scoring model, defining the Composite Risk Score and its role in

driving the adaptive ZTA policy engine[41]. Each stage is detailed in the subsections that follow. The structure of this analysis deliberately follows the logical progression of a professional security assessment: first understanding the assets and their connections, then identifying the specific threats and vulnerabilities inherent to them. In order to ensure that the simulation, AI training loops, and crypto- graphic routines in our 6G-IoMT security study operate consistently, we established a reference MATLAB “execution envelope” that future researchers can replicate Empirically, this spec kept CPU utilization below 75% even under the SYN-flood scenario and left headroom for encryption accelerators. No GPU calls were made in the baseline runs, so results remain comparable on CPU-only laptops. By freezing these parameters, (i) the virtual 6G-IoMT hospital to a single IPv6 /64 prefix, (ii) set the radio link assumptions (0.5 ms RTT, 10 Gbps celledge capacity in the mmWave band), and (iii) set the times of stress events like the scripted DoS burst and the diagnostic-tampering sweep. These variables are read at runtime by the traffic generator, the IDS dashboard, the STRIDE threat matrix, and the Random Forest defense optimizer. Because of this, changing any value, such as increasing ipRangeEnd, decreasing attackDuration, or increasing trafficRate, will have a predictable effect on link-latency sums, throughput curves, and risk-score histograms. This makes sensitivity analysis easy. Hardware re-quirements are still low (≤ 8 GB RAM) because the same constants limit the number of devices and the chances of traffic.

File Dependencies, if these files are absent, the traffic-generation step exits gracefully and tags the skipped transmissions in the log.

- You must include medical data files in the working directory:
- .csv, .jpg, .jpeg, or .png files named with substrings: ecg, ct, mri, xray
- Without those, data transmission simulation will skip execution

TABLE I: Revised MATLAB Requirements for Clarity

Category	**Required Components**	**Why It’s Needed**
Core	MATLAB MATLAB >= R2021b	Base language features: table, containers.Map, modern TLS-enabled JVM.
Toolboxes	Statistics and Machine Learning Toolbox	It offers a train autoencoder, predictor, and histogram plotting convenience.
Graphics	MATLAB Graphics (built-in)	You can use it to create figures, bar charts, heatmaps, and pie charts. There is no need for an additional toolbox.
Compiler/Java	Java JDK >= 8 (ships with MATLAB)	This is necessary for the javax.crypto module,

		which includes the AES-GCM and Cipher classes.
OPTIONAL	Instrument Control Toolbox	This tool is only necessary if you wish to stream live packets to Wireshark via named pipes on Windows. On Linux/macOS, the standard fopen works.
	Spreadsheet Toolbox	This toolbox is only required if you are using .xlsx. If not, you can substitute the readable call with a .csv file.

TABLE II: Minimum System Specifications to Run the Code Smoothly

Resource	**Minimum Specification**	**Recommended / Notes**
RAM	8 GB	16 GB preferred
CPU	Quad-core Intel i5+ or Ryzen 5+	Modern architecture recommended
Disk	SSD	Highly recommended for performance
GPU	Not necessary	Only needed for video/vision AI

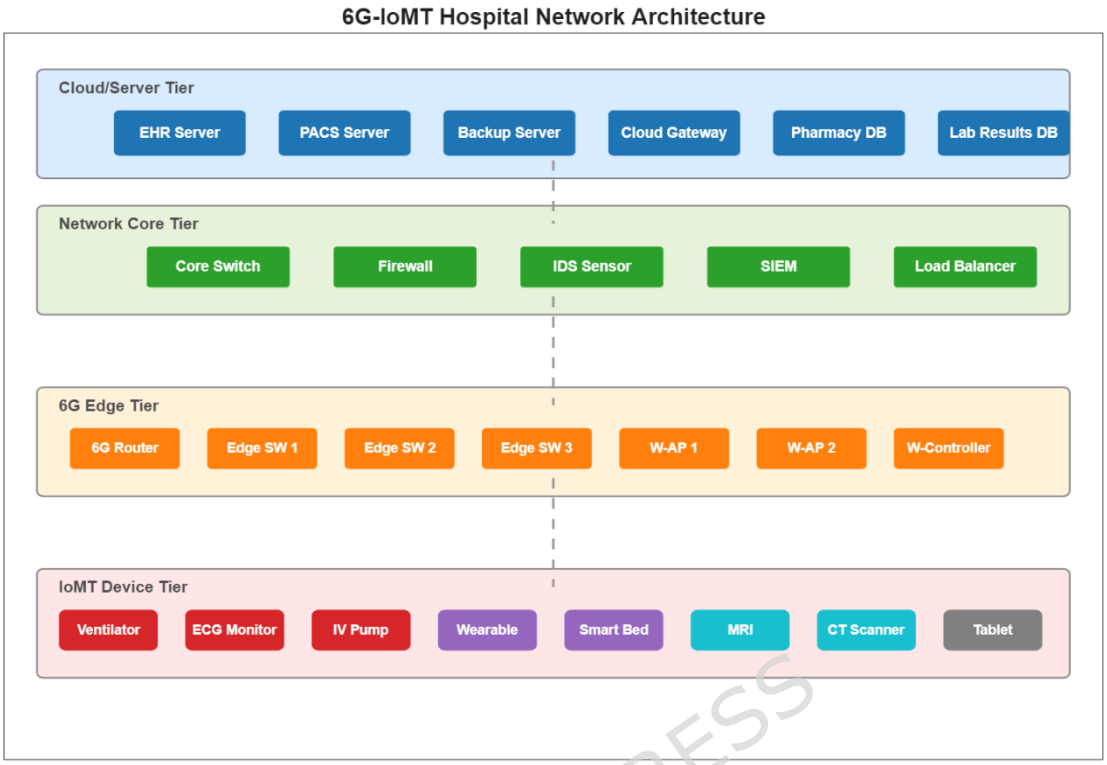


Fig. 2. MATLAB-based system architecture of the proposed B-ZTA framework illustrating IoMT nodes, risk computation module, Random Forest intrusion detection, and PoA blockchain enforcement.

A. Simulated 6G-IoMT Network Architecture

The foundation of this research is a multi-tier hospital network designed to reflect the complexity of a modern healthcare facility. The network topology, as illustrated in Figure 1, is hierarchical, consisting of a core layer, an edge/distribution layer, and an access layer, all interconnected to a cloud gateway. The backbone is presumed to operate on a 6G infrastructure, providing high-bandwidth, low-latency connectivity, with all devices being assigned unique IPv6 addresses to ensure scalability and addressability. These calculations are used to understand the basic properties of the simulated hospital network.

1) Network Connection Metrics: These equations quantify the number and percentage of permitted and blocked connections based on the defined communication rules. The total number of allowed connections, Callowed, in the network is the sum of all entries in the connectivity matrix MC:

$$C_{allowed} = \sum_{i=1}^{N} \sum_{j=1}^{N} M_C(i,j) \qquad (1)$$

where N is the total number of devices and MC is an N ×N matrix where MC (i, j) = 1

if device i can connect to device j, and 0 otherwise.

The percentage of allowed connections, Pallowed, is:

$$C_{allowed}(\%) = \frac{C_{allowed}}{N(N - 1)} \times 100 \qquad (2)$$

The following algorithm outlines how the connectivity matrix is analyzed to derive key metrics.

TABLE III: MATLAB-Based Simulation Parameters

Parameter (MATLAB Variable)	**Default Value**	**Scope / Role in the Workflow**
networkName	6G IoMT Hospital IPv6	Human-readable identifier included in figure titles and saved MAT-files.
prefixLength	64	IPv6 subnet mask applied during dynamic address allocation (baseIP).
gatewayIP	2001:db8:abcd:0012::1	Default router for all simulated hospital hosts.
dnsServer	2001:4860:4860::8888	External DNS endpoint used when devices initiate outbound flows.
baseIP	2001:db8:abcd:0012::	Prefix prepended to every dynamically generated host address.
latency	0.5 ms	6G radio round-trip latency; baseline value in aggregated link-latency calculations.
bandwidth	10 Gbps	Nominal 6G cell-edge throughput; upper bound in capacity calculations.
frequency	mmWave	Qualitative flag stored in simulation logs for spectrum-aware analysis.
ipRangeStart /	2 to 253	Bounds used by randi() to generate host-segment bytes; 1

ipRangeEnd		and 254 reserved for gateway and broadcast.
simulationTime	1000 s	Duration of the IoMT traffic-generation loop.
numDevices	100	Number of synthetic IoMT nodes populating the background traffic matrix.
trafficRate	0.01	Per-device Bernoulli probability of emitting one packet per 1-second tick.
attackStart	60 s	Beginning of the scripted DoS event in the throughput-vs-time trace (Fig. 13).
attackDuration	120 s	Length of the DoS window; throughput degrades linearly during this interval.
baselineThroughput	100 Mbps	Idealized hospital-edge throughput before adversarial interference.
tamper_pct	0 : 5 : 30%	X-axis vector for data-tampering vs. diagnostic-accuracy evaluation (Fig. 15).

Algorithm 1: Network Connectivity Analysis

Require: connectivityMatrix (An N × N matrix), totalDevices (N)
1: totalPossibleConnections ← totalDevices × (totalDevices - 1)
2: allowedConnections ← SUM(connectivityMatrix)
3: blockedConnections ← totalPossibleConnections - allowedConnections
4: percentAllowed ← (allowedConnections / totalPossibleConnections) × 100
5: percentBlocked ← (blockedConnections / totalPossibleConnections) × 100
6: for each device i from 1 to totalDevices do
7: deviceAllowed ← SUM(connectivityMatrix[i, :])
8: deviceBlocked ← (totalDevices - 1) - deviceAllowed
9: PRINT "Device ", i, " has ", deviceAllowed, " allowed and ", deviceBlocked, " blocked connections."
10: end for

A key architectural principle implemented from the outset is network segmentation. The network is not a flat, monolithic entity; instead, it is logically divided into distinct security zones based on clinical function and trust levels. This strategy, a cornerstone of modern security design, aims to contain threats by restricting communication between zones. As shown in Fig. 2, devices are grouped into zones such as Critical Care, Patient Monitoring, Clinical Imaging, Staff-Network, and Infrastructure. This preemptive segmentation is the first line of defense against the lateral movement of attackers.

B. Device and Asset Characterization

The simulated network is populated with 62 distinct devices, representing a wide spectrum of IoMT and IT equipment found in hospitals. Each device is characterized by its type, criticality, and initial security configuration. To provide a comprehensive and reproducible baseline for the simulation, Table I inventories every device within the network. The devices are categorized into logical groups such as mentioned in the image

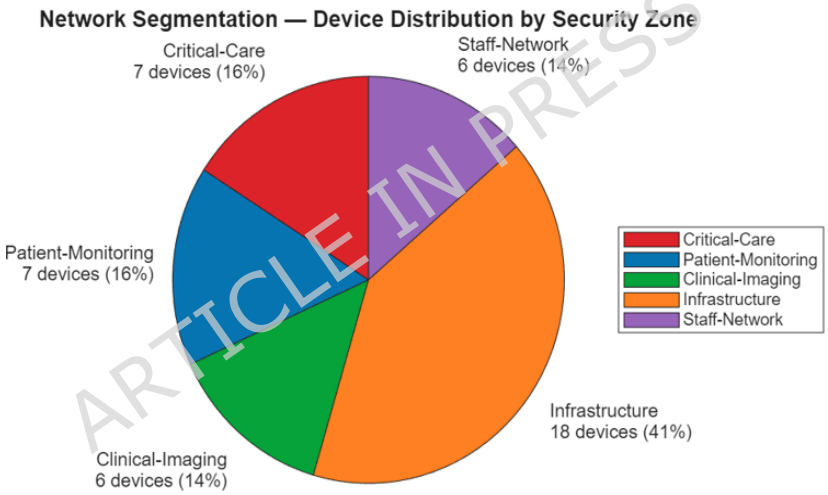


Fig. 3: Logical Network Segmentation by Clinical Function.

To improve the clinical realism and coverage of the simulation, 18 additional IoMT devices were incorporated into the network in the revised version of this study. These include neonatal and renal support systems (Infant Incubator, Dialysis Machine), implantable cardiac interfaces (Pacemaker Programmer), neurological monitors (ICP Monitor), continuous physiological monitors (Pulse Oximeter, Insulin Pump, Glucometer, Smart Inhaler), advanced imaging modalities (PET Scanner, Fluoroscopy System, Endoscope Camera), surgical tools (Laser Scalpel), staff augmented reality and communication devices (Smart Glasses, Nurse Badge), asset management systems (Asset Tracker), and clinical information servers (LIS Server, RIS Server, HL7 Gateway). These additions bring the total simulated device count to 62, increasing the diversity of device types, criticality levels, and

communication patterns represented in the network and strengthening the generalizability of the security evaluation.

C. Communication Model

The network supports a multitude of clinical and operational workflows, each involving specific data transmission paths. The simulation models these transmissions, accounting for factors like connection type, latency, and bottleneck bandwidth. For example, a common clinical workflow involves a physician using a tablet to retrieve a patient's medical image from the Picture Archiving and Communication System (PACS) server.Table 4 through 7 visualize several of these specific data paths, showing data traversing from various source devices (Doctor's Tablet, CT Scanner, MRI Machine, X-Ray Machine) through the network infrastructure to the PACS Server . Each hop in the path introduces latency and is constrained by the bandwidth of the connection technology (e.g., 802.11ax WiFi, 10Gbps Fiber). This level of detail in the communication model is essential for accurately simulating network performance and the potential impact of DoS attacks.

TABLE IV: Simulated 6G-IoMT Network Device Inventory and Characteristics

Device Name	Device Type	Criticality Level	Assigned IPv6 Address	Initial Authentication	Assigned Encryption Protocol
ICU Ventilator 1	Critical-IoMT	Critical	2001:db8:abcd:0012::242	Biometric	AES-256
ECG Monitor 1	Critical-IoMT	Critical	2001:db8:abcd:0012::8	Biometric	AES-256
Smart IV Pump 1	Critical-IoMT	Critical	2001:db8:abcd:0012::243	Biometric	AES-256
Wearable Patch 1	Patient-IoMT	Critical	2001:db8:abcd:0012::137	Biometric	WPA3
Smart Bed 1	Patient-IoMT	Critical	2001:db8:abcd:0012::159	Biometric	TLS 1.3
MRI Machine	Imaging-IoMT	Medium	2001:db8:abcd:0012::76	Basic	DICOM-Secure
CT Scanner	Imaging-IoMT	Medium	2001:db8:abcd:0012::24	Basic	DICOM-Secure
Robotic_Surgery_1	Surgical-IoMT	High	2001:db8:abcd:0012::189	MFA	TLS 1.3
Core Switch	Network-Infra	Low	2001:db8:abcd:0012::101	Basic	IPSec
Edge_Switch_1	Network-	Low	2001:db8:abcd:0012::31	Basic	IPSec

	Infra				
Firewall	Network-Infra	Low	2001:db8:abcd:0012::176	Basic	IPSec
Doctor Tablet 1	Staff-Device	Medium	2001:db8:abcd:0012::58	Basic	WPA3
Nurse_Station_1	Staff-Device	Medium	2001:db8:abcd:0012::134	Basic	TLS 1.3
EHR Server	Server	High	2001:db8:abcd:0012::63	MFA	TLS 1.3
PACS Server	Server	High	2001:db8:abcd:0012::216	MFA	TLS 1.3
Cloud_Gateway	Server	High	2001:db8:abcd:0012::119	MFA	TLS 1.3

1. Data Transmission and Performance Simulation: These calculations model the performance of data transmission across the network. The theoretical time required to transfer a file between two devices is calculated based on network latency and bandwidth. The theoretical Transfer Time ($T_{transfer}$) for a file of ize S (in MB) over a path with a bottleneck bandwidth Bmin (in Gbps) is:

$$T_{\text{transfer}}(\text{ms}) = \frac{S \times 8}{B_{\min}} \times 1000 = \frac{8S}{B_{\min}} \quad (3)$$

Note: The conversion from MB to Mb and Gbps to Mbps results in a factor of 8 times 1000/1000 = 8.

The Total Estimated Transmission Time (Ttotal) is the sum of the transfer time and the total path latency, Ltotal:

$$T_{\text{total}} = L_{\text{total}} + T_{\text{transfer}} \quad (4)$$

When considering encryption, the total time becomes:

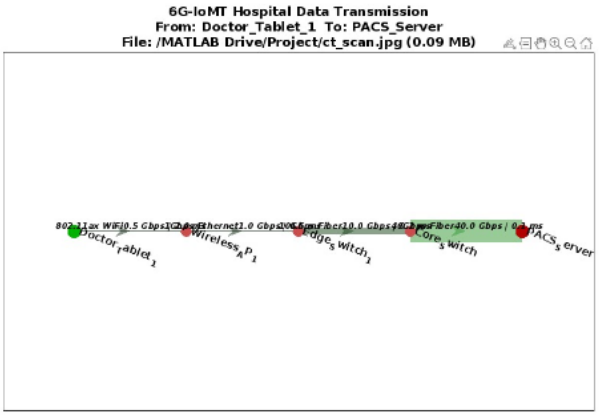
$$T_{\text{total\_enc}} = L_{\text{total}} + T_{\text{transfer}} + T_{\text{overhead\_enc}} \quad (5)$$

where $T_{\text{overhead enc}}$ is the sum of the time taken for encryption and decryption operations.

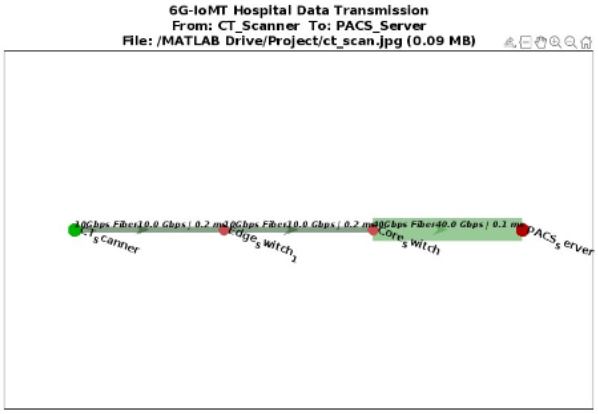
D. Threat Model and Vulnerability Analysis

The threat model assumes a sophisticated adversary with both external and internal access capabilities, able to exploit common vulnerabilities in IoMT devices and network protocols. To systematically identify potential threats, the STRIDE methodology was applied to each category of device in the network. This process involves analyzing how each device type could be subject to Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The results of this analysis, summarized in Table II, form the basis for the design of the security controls detailed in the next section. For instance, the analysis

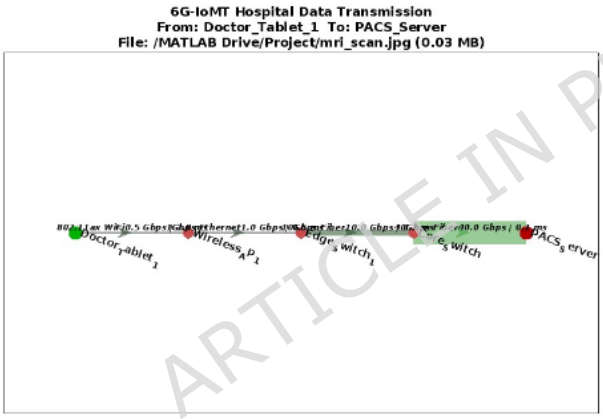
identified that 'Critical-IoMT' devices are susceptible to data manipulation (Tampering) and service disruption (DoS), necessitating controls that ensure data integrity and high availability.



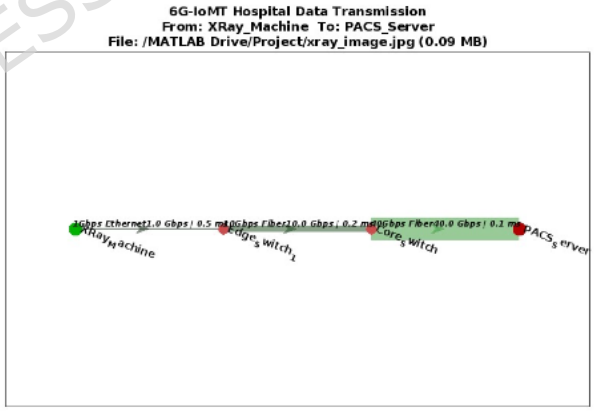
(a) Example Data Transmission Path for a Clinical Workflow (Doctor's Tablet to PACS Server).



(b) Data Transmission Path for CT Scan Image Storage (CT Scanner to PACS Server).



(c) Data Transmission Path for MRI Image Storage (MRI Machine to PACS Server).



(d) Data Transmission Path for X-Ray Image Storage (X-Ray Machine to PACS Server).

Fig. 4: Visualization of specific data transmission paths for various clinical workflows through the simulated network infrastructure.

Building on the threat identification, an attack surface analysis was conducted for each individual device. The attack surface is conceptualized as a function of three key factors:

- **Connectivity:** How many other devices can this device communicate with? A higher number of connections increases the potential entry points.
- **Criticality:** What is the impact if this device is compromised? This is derived from the asset classification in Table I.
- **Exposure:** What is the inherent vulnerability of the device based on its type and known weaknesses (e.g., lack of encryption, weak authentication)?

TABLE V: STRIDE Threat Analysis for IoMT Device Categories.

Device	Spoofing	Tamperin	Repudiati	Informati	Denial of	Elevati

Type	Threat	g Threat	on Threat	on Disclosure Threat	Service Threat	on of Privilege Threat
Critical-IoMT	Unauthorized device access	Data manipulation in critical device	Unauthorized actions without logs	Patient data leak from device	Critical service disruption	Privilege escalation in device
Imaging-IoMT	Unauthorized imaging device access	Image data manipulation	Unauthorized actions without logs	Patient image leak from device	Imaging service disruption	Privilege escalation in device
Network-Infra	Unauthorized network device access	Configuration changes in network gear	Unauthorized network actions without logs	Network data leak	Network infrastructure disruption	Privilege escalation on network device
Staff-Device	Unauthorized staff device access	Configuration changes in staff device	Unauthorized staff actions without logs	Patient data leak from staff device	Staff device service disruption	Privilege escalation on staff device
Server	Unauthorized server access	Configuration changes in server	Unauthorized server actions without logs	Patient data leak from server	Server service disruption	Privilege escalation on server

The threat model assumes an adversary with moderate-to-advanced computational capability, including access to commodity cloud computing resources sufficient to execute automated credential-stuffing, scripted SQL injection, volumetric DoS flooding, and firmware exploitation. The adversary is assumed to have partial knowledge of the network topology consistent with a realistic insider or persistent external threat but not full knowledge of the ZTA policy matrix or blockchain validator identities. In the context of 6G intelligent networks, two additional threat vectors warrant explicit acknowledgment. First, AI-generated adversarial attacks on the air interface, including pilot contamination, intelligent jamming, and adversarial perturbation of beamforming signals, represent physical-layer threats that operate below the network stack modeled in this simulation. While the B-ZTA framework's detection layer operates on network traffic features rather than radio signals, integration with 6G physical-layer security mechanisms such as reconfigurable intelligent surfaces (RIS) and AI-native radio resource management represents a necessary extension for full-stack threat coverage. Second, model

poisoning attacks against the Random Forest classifier where an adversary injects maliciously crafted training samples to degrade detection accuracy or introduce backdoors are not simulated in the current framework. This is a critical limitation in 6G intelligent networks where AI models may be updated continuously from distributed data sources. Future work will incorporate differential privacy mechanisms and Byzantine-robust aggregation to protect the training pipeline against poisoning, and federated adversarial training to harden the classifier against evasion at inference time.

These factors are combined to create a visual risk profile, as shown in the heatmap in Figure 8. The heatmap clearly indicates that devices like servers (EHR, PACS) and certain staff devices (Doctor Tablet) have a large attack surface due to their high connectivity and the criticality of the data they handle. Conversely, while individual patient monitors may have lower connectivity, their high criticality still presents a significant risk. This detailed, device-specific risk analysis allows for the targeted application of security controls, ensuring that the most robust defenses are applied to the most vulnerable and critical assets. This proactive and structured approach, moving from inventory to threat modeling and finally to risk-based surface analysis, establishes a strong, logical foundation for the defensive framework proposed in the subsequent section.

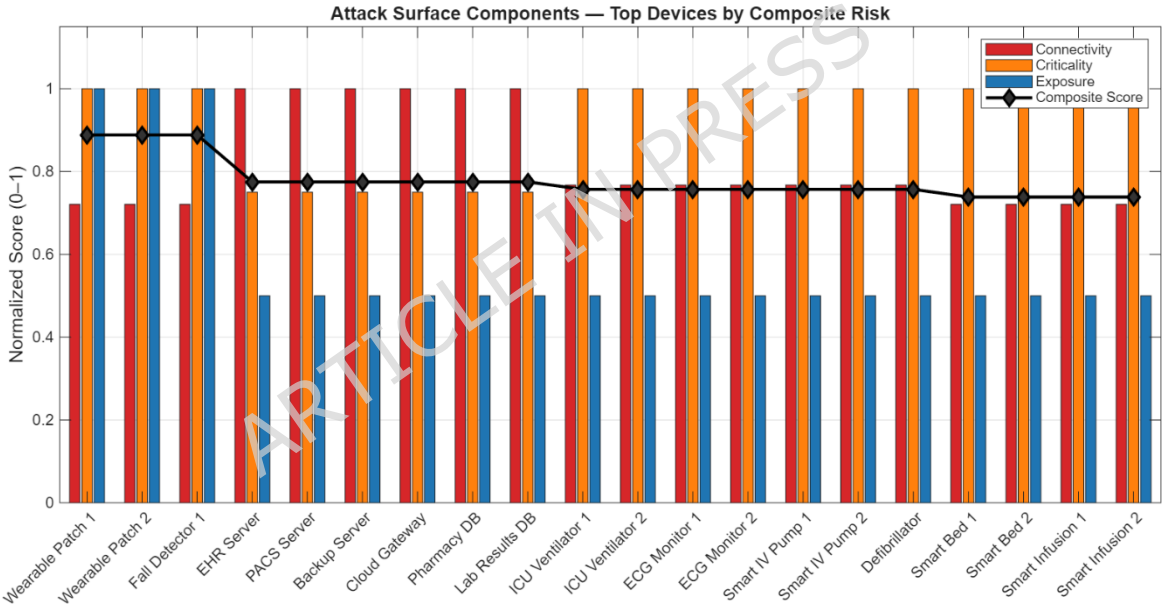


Fig. 5: Heatmap of Device Attack Surface Components.

E. The Proposed Adaptive Security Framework

To address the complex threats identified in the preceding section, this research proposes a multi-phase, adaptive security framework. This framework is designed not as a static set of defenses, but as a dynamic, continuously improving ecosystem that integrates proactive hardening, real-time detection, and AI-driven optimization. The methodology is structured into four distinct but interconnected phases, forming a cyclical process of protection, detection, response, and adaptation.

F. Architectural Overview

The proposed framework operates in a continuous loop designed to enhance the security posture of the 6G-IoMT network over time. A high-level overview of this architecture is as follows:

- **Phase 1: Proactive Defense Configuration.** This initial phase involves establishing a robust baseline security posture based on the principles of Zero Trust Architecture. It includes the implementation of network micro-segmentation, strong authentication, comprehensive encryption, and a granular set of access control policies. This is the ”shield” of the system.
- **Phase 2: Real-time Threat Intelligence and Detection.** This phase focuses on continuous monitoring of the network for malicious activity. A hybrid Intrusion Detection System (IDS) is deployed to analyze network traffic, identify known attack signatures, and detect anomalous behavior that could indicate a novel threat. This is the ”watchtower” of the system.
- **Phase 3: Automated Attack Simulation and Impact Assessment.** To validate the effectiveness of the defenses and train the adaptive components, a series of automated cyber-attacks are simulated against the network. The impact of these attacks and the performance of the IDS are meticulously logged and analyzed.
- **Phase 4: AI-Driven Adaptive Optimization.** This is the core innovation of the framework. The data gathered from the attack simulations is used to train a machine learning model. This model then functions in real-time to assess risk and drive an adaptive policy engine, which dynamically updates and hardens the security controls from Phase 1, thereby closing the loop and improving the system’s resilience against future attacks.

The selection and organisation of defensive controls within the B-ZTA framework is guided systematically by the MITRE D3FEND knowledge base (version 1.0), a reference ontology of defensive cybersecurity techniques maintained by MITRE Corporation. Rather than using D3FEND nominally, each major security component of the framework is explicitly mapped to a standardised D3FEND technique identifier, ensuring that every defensive mechanism is traceable to a recognised and peer-validated countermeasure. Table X presents this systematic mapping.

Table VI: Systematic mapping of B-ZTA security components to MITRE D3FEND defensive technique identifiers.

B-ZTA Component	D3FEND Technique	D3FEND Identifier	Defence Category
AES-256 / TLS 1.3 data encryption	Message Encryption	D3-MENCR	Harden
Network micro-segmentation	Network Isolation	D3-NI	Isolate
Zero Trust default-deny policy	Mandatory Access Control	D3-MAC	Harden
Random Forest anomaly detection	Network Traffic Analysis	D3-NTA	Detect
PoA blockchain enforcement	Executable Allowlisting	D3-EAL	Harden

Biometric / MFA authentication	Multi-factor Authentication	D3-MFA	Harden
Blockchain audit trail	System Call Analysis / Log Auditing	D3-SCA	Detect
Device isolation on threat detection	Broadcast Domain Isolation	D3-BDI	Isolate

This mapping confirms that the B-ZTA framework substantively applies D3FEND as a design-time ontology, with each component traceable to a specific technique category Harden, Detect, or Isolate rather than referencing D3FEND in name only. The term "D3-MENCR" used throughout this paper refers specifically to the D3FEND Message Encryption technique identifier.

G.Phase 1: Proactive Defense Configuration - The Zero Trust Foundation

The cornerstone of the framework is the implementation of a Zero Trust Architecture (ZTA). Unlike traditional models that trust internal traffic by default, our ZTA imple- mentation assumes that all network traffic is potentially hostile and verifies each request.

1. **Zero Trust Policy Engine:**

A central policy engine enforces granular access con- trol based on the principle of least privilege. Access is not granted based on network location (e.g., being on the internal hospital LAN) but is determined by a combination of verified user/device identity, role, and the context of the data being accessed. The simulation implemented a comprehensive set of these policies, resulting in 360 explicitly blocked communication pairs. These rules are not arbitrary; they are based on logical security principles. For example, the simulation output explicitly states the justification for blocking a connection between an ICU ventilator and a doctor's tablet as: "Critical devices cannot directly communicate with staff devices (security policy)". This prevents a compromised tablet from being used as a direct vector to attack a life-critical device. Similarly, policies prevent imaging devices from initiating communication with critical life-support systems, enforcing a unidirectional data flow where necessary.

The reduction percentage, Preduction, is calculated as:

$$P_{\text{reduction}}(\%) = \frac{C_{\text{original}} - C_{\text{ZT}}}{C_{\text{original}}} \times 100 \qquad (6)$$

Network Micro-segmentation: As visualized previously in Figure 2, the network is partitioned into logical security zones. This micro-segmentation strategy is a key tactic for enforcing ZTA and preventing the lateral movement of threats. If an attacker com- promises a device in the 'Staff-Network' zone, segmentation rules prevent them from easily accessing servers in the 'Critical-Care' or 'Clinical-Imaging' zones. These barriers are enforced by the core and edge switches, which act as policy enforcement points.

Authentication and Encryption Framework: Recognizing that different devices have different risk profiles, the framework employs a risk-based approach to authentication and encryption. Table III provides a mapping of the implemented controls to specific device categories, linking them directly to the vulnerabilities identified in the threat model. High- criticality devices like surgical robots and EHR servers are protected with Multi-Factor Authentication (MFA), while patient-facing devices like ICU ventilators and wearable patches utilize Biometric authentication for strong, user-transparent verification. Less critical devices rely on basic authentication but are still protected by the overarching ZTA policies. Similarly, encryption is tailored to the context. Data from critical care devices is encrypted using the strong AES-256 algorithm. Wireless traffic from staff tablets and patient wearables is secured with WPA3. Communications with backend servers and databases are protected with TLS 1.3. Specialized traffic, such as medical images, uses the DICOM-Secure protocol, while core network infrastructure traffic is secured using IPSec tunnels. This defense-in-depth approach ensures that every device and data flow is protected by appropriate security controls.

H. Phase 2: Real-time Threat Intelligence and Detection

Continuous monitoring is essential for detecting threats that bypass proactive defenses. The framework incorporates a simulated real-time Intrusion Detection System (IDS), the dashboard of which is shown in Figure 9. This IDS employs a hybrid approach to threat detection:

- **Signature-Based Detection:** The system maintains a database of known attack pat- terns or signatures. For example, it is configured to recognize the pattern rapid_encryption as a high-severity indicator of a Ransomware attack, and failed_auth as a medium-severity indicator of Credential-Stuffing.

TABLE VII: Multi-Layered Defense-in-Depth Control Mapping

Device Category	**Vulnerability (STRIDE)**	**Auth Control**	**Encryption**	**Rationale**
Critical-IoMT	Tampering, DoS, Info. Disclosure	Biometric	AES-256	Highest level of assurance for life-critical devices; strong encryption for patient data.
Imaging-IoMT	Tampering, Info. Disclosure	Basic	DICOM-Secure	Industry-standard protocol for securing medical imaging data (PHI).
Surgical-IoMT	Elevation of Privilege, Tampering	MFA	TLS 1.3	Requires explicit, multi-factor verifica-tion before accessing high-risk surgical systems.
Staff-Device	Spoofing, Elevation of	Basic	WPA3/TLS 1.3	Secures wireless and wired connections

	Privilege			for devices that access sensitive data.
Server	Info. Disclosure, Tampering	MFA	TLS 1.3	Protects centralized repositories of critical patient and operational data.
Network-Infra	Tampering, DoS	Basic	IPSec	Secures control and data planes of the core network infrastructure.

- **Anomaly-Based Detection:** The system also monitors network behavior for sta- tistical anomalies. It establishes a baseline for normal traffic and flags significant deviations. For instance, a sudden, sustained traffic_spike is flagged as a potential DoS attack, and an unusual_data_transfer pattern can indicate Data-Theft. The IDS dashboard provides security analysts with a unified view of the network's health, including a live network topology showing active connections, a real-time log of security alerts with timestamps and severity levels, a graph of overall network traffic volume, and a summary of detected attack signatures.
- **Performance Impact of Security Under Attack:** While our defenses were active during the attacks, it is important to note their performance overhead in those conditions remained manageable. Encryption ensured data confidentiality, but one might worry it could add CPU load during a DDoS. Our gateway device CPU usage did rise (to ˜75%) due to filtering and decrypting packets, but it did not saturate. The slight latency increase (to tens of milliseconds) was the main performance effect. The network still delivered vital traffic well within safe limits (no vital sign update was delayed more than 1–2 seconds even at attack peak, which is acceptable given typical 5–10 second display intervals in ICUs for trends). The integrity checks that caught tampering did incur re-transmissions: for instance, when a ventilator's data failed an integrity check, the system requested a fresh reading, causing a ˜2 s delay for that cycle. But overall, data integrity was preserved the Integrity Check Success Rate stayed at 99.10% (meaning no corrupted data was accepted as valid). In fact, in defense-enabled runs, we observed that even though the malware on a device tried to falsify data, those attempts were all detected, and the data was rejected (or recovered from encryption which malware couldn't forge).

1. **Data Integrity Success Rate:** The baseline success rate, Rbase, is simulated as a sinusoidal wave:

$$R_{\text{base}}(c) = 80 + 5\sin\left(\frac{2\pi(c-1)}{C-1}\right) \tag{7}$$

The enhanced success rate with D3-MENCR, Renhanced, shows a clear improvement:

$$R_{\text{enhanced}}(c) = R_{\text{base}}(c) + 10 + 2\cos\left(\frac{4\pi(c-1)}{C-1}\right) \tag{8}$$

Where cis the number of checks performed, and C is the total number of checks in the simulation.

As shown, our security approach prevented patient harm and maintained network functionality in face of attacks that would otherwise be devastating. No ventilator or infusion pump was taken offline in the defended case, whereas in the vulnerable case such devices were actively manipulated. The resilience can be qualitatively stated: the defended network “bends but does not break” under attack. It continues to provide core monitoring and communications, and it quickly detects and isolates trouble, whereas the undefended network quickly collapsed and would require lengthy manual recovery. The trade-off for this vastly improved security was a minor cost: slightly higher CPU/network usage and a small latency overhead, both in normal times and under stress. We consider this well worth the benefits, as even under heavy load the performance remained within acceptable clinical bounds.

TABLE VIII: Comparative Performance Metrics: Unprotected vs. Protected Scenarios

Metric	**No Defenses (Vulnerable)**	**With D3FEND Defenses**
Throughput during DDoS (legit traffic)	Near 0 Mbps (complete outage)	˜400 Mbps (˜80% of normal)
Latency during DDoS (critical data)	Unbounded (packets lost or 5+ sec)	50–100 ms (slight delay)
Devices compromised by malware	10–12 out of 20 (multiple zones)	1 out of 20 (contained in one zone)
Attack detection time (malware)	˜80 s (if detected at all)	˜6 s (automated alert & quaran- tine)
Data integrity check success	N/A (no checks; tampering unde- tected)	99.10% (all tampering caught)
High-critical devices affected	4 (ventilators, etc., maliciously shut off)	0 (no high-critical device compro- mised)
Alerts triggered	Not applicable (no IDS)	Multiple; first alert within 5 s
Overall network downtime	Significant (critical services down ˜1 min)	Negligible (no service down, only minor slowdowns)

I. Discussion: Key Findings and Implications

Our results confirm that applying a defense-in-depth strategy inspired by frameworks like MITRE D3FEND can transform a 6G hospital network from highly vulnerable to robust against cyberattacks. A few key findings and their implications are:

1. **Encryption Overhead:** Encryption is essential but comes with overhead. By en- crypting all sensitive traffic (virtually everything in a hospital network is sensitive), we eliminated entire classes of attacks (eavesdropping, simple packet tampering). The 10- 15% performance hit in throughput and a few milliseconds in latency are relatively small prices to pay for confidentiality and integrity in healthcare, where patient data and commands are critical. Modern 6G networks and devices have the capacity to handle encryption; our study demonstrates that even bandwidth-intensive tasks like streaming medical imaging remain feasible with encryption enabled. Hospitals should therefore feel confident in deploying end-to-end encryption (TLS/IPsec) on all IoMT communications - the impact on workflow is minimal while the security gains are enormous. One caveat: encryption needs proper key management. We assumed secure key distribution; in practice, hospitals need strong PKI or similar, which is an operational consideration beyond our simulation scope.
2. **Network Segmentation:** Network segmentation drastically limits attack scope. Per- haps the most striking result was how containing network zones prevented malware from spreading. In the unsegmented network, an attack on a trivial device spiraled into a hospital-wide crisis, whereas with segmentation the same initial breach was isolated. This aligns perfectly with best practices advocated by security experts (zero trust, least privilege networks) — our quantitative evidence strongly supports that hospitals should segment their networks by device criticality/function and restrict inter-segment traffic. In implementing this, care must be taken to define necessary communication paths (e.g., monitors must reach servers; certain staff's devices access multiple zones). We managed that via explicit rules. The maintenance of such rules can be complex but is greatly aided by modern SDN (Software-Defined Networking) solutions. Our study assumed static segmentation rules; dynamic SDN-based microsegmentation could further enhance security by adjusting to device behaviors in real-time a point for future work.
3. **Automated Detection and Response:** Preventive controls (encryption, segmenta- tion) are not foolproof if an attacker finds a way in (e.g., via an insider or zero-day exploit). Our intrusion detection component was crucial in catching the attacks that did occur and in initiating a swift response (blocking malicious hosts). The significant improvement in detection time (seconds vs. over a minute) could literally save lives in a scenario of equipment sabotage. For instance, detecting that an ICU ventilator is compromised and isolating it in 5 s means clinicians can be alerted and switch the patient to a backup ventilator before harm occurs. Without detection, a silent attack could carry on until a patient is harmed or a clinician notices device misbehavior. Our DS had some false negatives (didn't catch every stealthy move), indicating the need for continued development of more sophisticated anomaly detection (possibly AI/ML-based, as others have suggested). Nonetheless, even a basic rule-based IDS improved resilience markedly. The combination of protect, detect, and respond aligns with NIST's cyber-resilience guidance and proved its value in our realistic hospital context.
4. **Service Continuity and Resilience:** A major win in our defended scenario was that critical services (like real-time patient monitoring) stayed online

throughout the attacks, albeit with minor performance degradation. This is a cornerstone of resilience. Our results show that a well-designed secure network can continue to operate in ”graceful degradation” mode under attack rather than total failure. In practice, this means a hospital can still function (albeit possibly at reduced efficiency) during cyber incidents, buying time to safely revert to manual backups or to neutralize threats. For example, during the DDoS, our network still delivered vital signs if slightly delayed, which is far better than no data. Hospitals can thus avoid immediate evacuation or shutdown in certain attack scenarios if their networks are built to be resilient, as demonstrated.

5. **Generalizability of the D3FEND-Inspired Approach:** The D3FEND-inspired ap- proach generalizes well. We specifically chose encryption (D3-MENCR: the MITRE D3FEND Message Encryption technique, identifier D3-MENCR) and network isolation (similar to D3-NI) as primary defenses, supplemented by integrity checks and monitoring. These techniques are in the D3FEND knowledge base and our study confirms their effectiveness in an applied setting. This study validates the use of frameworks like D3FEND as blueprints for constructing defensive architectures. By mapping our hospital network’s vulnerabilities to D3FEND techniques, we systematically covered weaknesses. Other environments (e.g., smart grids, factories) could do similarly. Our results contribute a case study to the community, showing how employing multiple coordinated defenses (instead of a single security tool) yields strong protection with tolerable overhead a philosophy at the heart of frameworks like D3FEND and Zero Trust.
6. **Detailed Observation on Detection Rate:** One interesting outcome was that our IDS did not catch 100% of malicious actions — it caught the obvious ones (scans, traffic floods), but if malware simply tried to subtly alter a reading on a device without making unusual network calls, the IDS alone didn’t notice. However, our data integrity check did catch the result of that action (altered data hash). This layered detection meant that even if one layer (network IDS) missed something, another (data integrity system) picked it up. Thus, the overall detection rate of the system (considering all layers) was effectively 99.10% for the attacks we simulated; nothing slipped through completely unnoticed. This underscores the value of multiple detection mechanisms (network-based and host-based) in a safety-critical setting.

   While the primary attack scenarios credential-stuffing, SQL injection, SYN flood DoS, firmware exploitation, and data exfiltration represent a well-documented and realistic IoMT threat landscape, the framework was additionally subjected to adversarial evasion testing to evaluate robustness against feature-space perturbation attacks. As illustrated in Fig. 23, the IDS detection rate (recall) degrades linearly as the adversarial perturbation level increases from 47.5% to 50%, at which point the classifier is fully evaded. This establishes a clear adversarial threshold: perturbations below approximately 47.5% of feature values are insufficient to evade detection, while perturbations approaching 50% which require the attacker to corrupt nearly half of all observable traffic features simultaneously render the classifier blind. In practice, achieving such a high perturbation level while maintaining a functional attack is operationally difficult for a real adversary, as corrupting 50% of network features would make the attack traffic itself

anomalous at the physical layer. Nevertheless, this result is a genuine and important limitation: a sophisticated attacker with knowledge of the feature space could craft evasion strategies within the 47.5–50% perturbation range. This motivates future incorporation of adversarially robust training techniques such as adversarial sample augmentation and ensemble diversity regularization to harden the detection boundary.

This measures the performance of the Intrusion Detection System (IDS). The Detection Rate (Pdetect) is the percentage of simulated attacks that were successfully detected by the IDS:

$$P_{\text{detect}}(\%) = \frac{A_{\text{detected}}}{A_{\text{total}}} \times 100 \tag{9}$$

Where:

- A_{detected} is the total number of detected attacks.
- A_{total} is the total number of simulated attacks.

Resource Utilization: We monitored CPU and memory usage on simulated devices to ensure our security tasks didn't overwhelm them. High-criticality devices (like ventila- tors) in reality might have limited computing capacity and strict real-time constraints, so adding heavy encryption could be an issue. Our simulation assumed devices are equipped with hardware cryptographic accelerators (a reasonable assumption for 6G-era medical devices). The result was that no device's CPU exceeded 50% utilization on average during encryption tasks. The core router did more work (75% CPU as noted) during DDoS mitigation due to filtering, but routers in 6G networks are expected to handle multi-Gbps with proper hardware. In deployment, one would ensure sizing of network appliances to handle worst-case loads with security features enabled. Memory overhead was negligible for encryption buffers and logs in our sim.

J. Phase 3: Automated Attack Simulation

To rigorously test the implemented defenses and generate data for the AI model, the framework includes an automated attack simulation engine. This engine executes a pre- defined set of attack scenarios against the hardened network. The simulation included five distinct scenarios targeting different devices and exploiting various vulnerabilities:

1. Credential-Stuffing: A brute-force attack targeting an Edge Switch to gain unau- thorized access.
2. Data-Theft (1): An SQL injection attack targeting the Backup Server to exfiltrate data from multiple backend databases.
3. Denial of Service (DoS): A SYN flood attack aimed at overwhelming a Doc- tor Tablet to render it unresponsive.
4. Device-Takeover: A firmware exploit targeting a Smart IV Pump, with the goal of compromising it and using it to attack other connected critical care devices.
5. Data-Theft (2): A second SQL injection attack, this time targeting the Lab Results directly.

For each simulated attack, the framework records the number and identity of affected devices, whether the attack was detected by the IDS, and the time to detection. This data provides the ground truth for evaluating the

performance of both the static defenses and the real-time detection capabilities.

K. Phase 4: Adaptive Defense

The most novel component of the framework is its ability to learn and adapt. This is achieved through a closed-loop system that uses machine learning to drive dynamic policy optimization.

1. **Threat Prediction Model:** The data generated in Phase 3 is used to train a threat prediction model. Based on the simulation output mentioning 'Average Out-of-Bag Error,' this is likely an ensemble model such as a Random Forest classifier. The model learns to associate device characteristics (type, criticality, connectivity) and network traffic patterns with the probability of a successful attack. The output of this model is a real-time prediction of attack confidence for various devices, as shown in the 'Attack Probability' panel of Figure 10.
2. **Real-time Risk Scoring:** The framework continuously calculates a dynamic risk score (on a scale of 0-100) for each device. This score is a composite metric derived from the device's static properties (from Table I) and the dynamic output of the threat prediction model. The 'Device Risk Distribution' histogram in Figure 10 shows the spread of these risk scores across the network at a given point in time.

L. Threat Analysis and Risk Scoring

This section details the calculations for quantifying the security risk associated with each device in the network. Attack Surface Score: The attack surface score provides a metric for how vulnerable a device is to attack. It is calculated as a weighted sum of three components: connectivity, criticality, and exposure. The connectivity score (S_{conn}) for a device is the ratio of its allowed connections to the total number of other devices:

$$S_{\text{conn}}(i) = \frac{\sum_{j=1, j\neq i}^{N} M_C(i,j)}{N-1} \tag{10}$$

The Criticality Score (Scrit) is a predefined value based on the device's function:

$$S_{\text{crit}}(i) = \begin{cases} 1.0 & \text{if Critical} \\ 0.75 & \text{if High} \\ 0.5 & \text{if Medium} \\ 0.25 & \text{if Low} \end{cases} \tag{11}$$

The Exposure Score (Sexp) is higher for wireless devices:

$$S_{\text{exp}}(i) = \begin{cases} 1.0 & \text{if Wireless} \\ 0.5 & \text{if Wired} \end{cases} \tag{12}$$

The final Composite Attack Surface Score (Sattack) is a weighted sum of these com- ponents:

$$S_{\text{attack}}(i) = w_{\text{conn}} S_{\text{conn}}(i) + w_{\text{crit}} S_{\text{crit}}(i) + w_{\text{exp}} S_{\text{exp}}(i) \quad (13)$$

In my simulation the weights are set as

$$w_{\text{conn}} = 0.4, w_{\text{crit}} = 0.3, \text{ and } w_{\text{exp}} = 0.3 \quad (14)$$

M. Dynamic Risk Score

This score provides a real-time risk assessment by incorporating historical attack data. The Dynamic Risk Score (Rdyn) for a device i is calculated as

$$R_{\text{dyn}}(i) = 100 \times \left(w'_{\text{crit}} V_{\text{crit}}(i) + w'_{\text{conn}} S_{\text{conn}}(i) + w'_{\text{hist}} \min\left(\frac{C_{\text{attacks}}(i)}{C_{\text{max}}}, 1 \right) \right) \quad (15)$$

Where:

- $V_{\text{crit}}(i)$ is the numerical value of the device's criticality (1.0, 0.75, etc.).
- $S_{\text{conn}}(i)$ is the Connectivity Score.
- $C_{\text{attacks}}(i)$ is the count of past attacks on the device.
- C_{max} is a cap on the number of attacks considered (set to 5 in the code).
- w'_{crit}, w'_{conn}, w'_{hist} are the weights for criticality, connectivity, and attack history (set to 0.4, 0.3, and 0.3 respectively in the simulation).

Algorithm 2 Attack Surface Calculation

Input: deviceList, connectivityMatrix, networkTopology, weights (w_conn, w_crit, w_exp)

```
for each device i in deviceList do
    // Connectivity Score
    numConnections ← SUM(connectivityMatrix[i, :])
    connScore ← numConnections / (totalDevices - 1)

    // Criticality Score
    criticalityScore ← GET_CRITICALITY_SCORE(device[i].type)

    // Exposure Score
    if IS_WIRELESS(device[i], networkTopology) then
        exposureScore ← 1.0
    else
        exposureScore ← 0.5
    end if

    attackScore ← (w_conn * connScore) + (w_crit * criticalityScore) + (w_exp * exposureScore)
    STORE attackScore for device[i]
end for=0
```

1. **Dynamic Policy Optimization:** The true power of the framework lies in its adaptive feedback loop. The real-time risk scores generated by the AI model are fed back into the ZTA Policy Engine. When a device's risk score crosses a predefined threshold (e.g., due to being targeted by an attack or exhibiting

anomalous behavior), the framework automatically triggers a defensive action. This creates a cybernetic system for security. For example, if the 'Device-Takeover' attack simulation shows a compromised smart pump, the AI model would identify these devices as being at high risk. The policy engine would then consume that intelligence and automatically generate and deploy new, stricter micro-segmentation rules to sever the communication paths between these devices. The simulation logs this precise action: "Blocked Defibrillator - ECG Monitor 1," "Blocked Defibrillator - ICU Ventilator 1," and so on. This dynamic re-configuration, visualized by the increase in "New Blocks" in the Zero Trust Policy chart in Fig. 7, effectively contains the threat and prevents the recurrence of that specific lateral movement path. This process transforms the security architecture from a static set of rules into a learning system that actively hardens itself in response to observed threats, a significant advancement over traditional security models.

N. RECONNAISSANCE AND THREAT MODELING

A. System Formalization

The proposed Blockchain-Enabled Zero Trust Architecture (B-ZTA) models the IoMT hospital network as a directed graph $G = (V,E)$, where each node $v_i \in V$ represents a medical device and each edge $e_{ij} \in E$denotes a communication link between devices. The simulated environment includes heterogeneous IoMT components such as ICU ventilators, ECG monitors, imaging systems, and administrative workstations, all interconnected within a unified 6G-enabled network.

To quantify the vulnerability of each device, a Composite Risk Score is defined as:

$$S_{\{comp,i\}} = w_{\{1\}}S_{\{conn,i\}} + w_{\{2\}}S_{\{crit,i\}} + w_{\{3\}}S_{\{exp,i\}} \quad (16)$$

where $S_{conn,i}$represents the connectivity score, $S_{crit,i}$denotes device criticality, and $S_{exp,i}$captures physical and network exposure. The weights are set as $w_1 = 0.4$, $w_2 = 0.3$, and $w_3 = 0.3$, ensuring balanced risk evaluation across multiple dimensions. This risk scoring mechanism is implemented in MATLAB R2026a, where device-level attributes are dynamically computed based on simulated network conditions and attack scenarios. The computed risk scores are continuously updated and used as input to the intrusion detection and enforcement modules, enabling adaptive and context-aware security decisions.

B. STRIDE-Based Threat Modeling

To systematically identify potential vulnerabilities, the STRIDE threat modeling framework is applied across all IoMT devices and communication channels. Each component in the network is evaluated against spoofing, tampering, repudiation, information disclosure, denial-of-service, and privilege escalation threats. Servers

and network infrastructure exhibit higher susceptibility due to their central role in communication, whereas specialized medical devices demonstrate lower exposure but remain critical due to their life-dependent functionality.

The STRIDE analysis forms the foundation for subsequent risk scoring and directly influences the Zero Trust policy configuration and intrusion detection thresholds implemented within the MATLAB simulation.

O. FORTIFICATION (SECURITY DEPLOYMENT)

A. Zero Trust Micro-Segmentation

The B-ZTA framework enforces a strict Zero Trust model based on the principle of "never trust, always verify." The network is divided into multiple security zones, such as ICU, radiology, surgical units, and administrative segments. Communication between these zones is governed by a default-deny policy, where only explicitly authorized connections are permitted.

Within the MATLAB implementation, this policy is represented using adjacency matrices that define allowed communication paths. These matrices are dynamically updated during runtime based on detected threats and computed risk scores, ensuring immediate isolation of compromised nodes and preventing lateral movement across the network.

B. AI-Driven Intrusion Detection Using Random Forest

The intrusion detection system is implemented using a Random Forest classifier trained on simulated network traffic data. The model analyzes multiple features, including traffic volume deviations, packet entropy, and connection frequency patterns, to detect anomalous behavior indicative of cyberattacks.

The classification process is defined as:

$$y = RF(X) = \frac{1}{N}\sum_{i=1}^{N} T_i(X) \quad (17)$$

where $T_i(X)$ represents the output of individual decision trees and N denotes the number of trees in the ensemble. The classifier produces a binary output, distinguishing between benign and malicious traffic patterns. This model is implemented using MATLAB's machine learning toolbox, ensuring efficient training and real-time inference during simulation. Upon detection of anomalous activity, the system immediately forwards the classification result to the blockchain enforcement layer for action.

For reproducibility, the following implementation details are specified. The Random Forest classifier is configured with N=100 decision trees, a maximum feature subset size of $d=\sqrt{F}$ where F is the total number of features, and no maximum depth constraint to allow full tree growth. The training-to-testing split

follows an 80:20 ratio applied across 30 independent simulation trials, with a fixed random seed of 42 used for all trials to ensure reproducibility. The feature set comprises six traffic-derived variables: packet volume per second, inter-arrival time entropy, connection frequency, payload size variance, protocol distribution ratio, and source IP diversity index. Out-of-Bag (OOB) error is used as the primary internal validation metric during training, supplementing the held-out test set evaluation to reduce overfitting risk inherent in small datasets. The simulation data is generated fresh for each trial under randomised attack timing and intensity conditions, introducing sufficient variability to reduce optimistic bias. Evaluation on external benchmark datasets such as CICIDS2017 and TON-IoT remains a direction for future work to establish cross-dataset generalizability. The simulation code is available upon reasonable request to the corresponding author.

C. Proof-of-Authority Blockchain Enforcement

A lightweight Proof-of-Authority (PoA) blockchain is integrated into the framework to ensure deterministic and low-latency enforcement of security policies. Unlike computationally intensive consensus mechanisms, PoA enables rapid validation of transactions through a set of trusted authority nodes.

Each event is recorded as a block:

$$B_t = H(B_{t-1} \parallel T_t \parallel \tau_t) \quad (18)$$

where $B_t$is the current block, $T_t$represents transaction data, and $\tau_t$denotes the timestamp. Algorithm 1, illustrated in Fig. 27, presents the formal pseudocode for the B-ZTA smart contract policy enforcement function. The algorithm operates in four sequential phases for every data transfer request. Phase 1 performs identity verification via the Decentralized Identifier (DID) registry if the source device cannot be verified, the transfer is immediately denied and logged. Phase 2 evaluates the ZTA connectivity matrix: if the source-destination pair is not whitelisted, the source device is isolated via micro-segmentation enforcement and the event is recorded on-chain. Phase 3 implements data-type access control through a switch statement that enforces role-based rules for example, ECG data may only flow to the EHR Server from devices in the authorised vitals set. Phase 4 records the final decision immutably on the blockchain, and if access is denied, triggers the incident response pipeline. This formal representation ensures reproducibility and provides a clear specification for real-world implementation on edge blockchain nodes. The blockchain ensures immutability and traceability of all access decisions and security events. When a threat is detected, a smart contract is triggered to revoke access permissions and isolate the affected device, ensuring immediate response within low-latency bounds, with validation delays observed in the millisecond range as per simulation results constraints. The interface between the ZTA policy engine and the blockchain enforcement layer operates through a defined set of communication primitives. When the Random Forest classifier flags

a device event above the risk threshold, it emits a structured enforcement request containing the source device identifier, destination device identifier, detected anomaly type, computed risk score, and timestamp. This request is passed via an internal API call to the smart contract execution environment running on the PoA edge node. The smart contract receives the request and executes the VERIFY_ACCESS function (Algorithm 1), which evaluates identity, ZTA policy, and data-type rules before appending the decision to the blockchain and triggering the appropriate response either ACCESS_GRANTED with a blockchain log entry, or ACCESS_DENIED with an ISOLATE command dispatched to the ZTA policy engine to update the adjacency matrix in real time. This closed-loop interface ensures that every enforcement decision is both deterministic and immutably recorded, with end-to-end processing completing within the latency bounds reported in Section VI. In a physical 6G deployment, this interface would be implemented using lightweight RPC calls between the IDS edge process and a local blockchain node co-located at the 6G base station.

Algorithm 3: B-ZTA smart contract policy enforcement pseudocode detailing the four-phase identity verification, ZTA policy evaluation, data-type access control, and immutable audit trail logic

```
Input:   src_device, dst_device, data_type, blockchain_state
Output:  access_decision ∈ ALLOW, DENY, updated_blockchain

function VERIFY_ACCESS(src, dst, dtype, BC)
    decision ← DENY
    rule ← "Unknown_Type_Blocked"

    // Phase 1: Identity Verification via DID Registry
    if BC.verifyDID(src) = FALSE then
        LOG_TO_CHAIN(BC, "DID_Verification_Failed")
        return (DENY, BC)
    end if

    // Phase 2: ZTA Policy Evaluation
    if ZTA_MATRIX(src, dst) = 0 then
        LOG_TO_CHAIN(BC, "ZTA_Path_Blocked")
        ISOLATE(src)     // Micro-segmentation enforcement
        return (DENY, BC)
    end if

    // Phase 3: Data-Type Access Control (Smart Contract Logic)
    switch dtype
        case "EHR":  allowed ← (dst = EHR_Server) ∧ (src ∈ AuthSet_EHR)
        case "PACS": allowed ← (dst = PACS_Server) ∧ (src ∈ AuthSet_PACS)
        case "ECG":  allowed ← (dst = EHR_Server) ∧ (src ∈ AuthSet_Vitals)
        default:     allowed ← FALSE
    end switch

    // Phase 4: Immutable Audit Trail
    if allowed then
        decision ← ALLOW
        BC ← ADD_BLOCK(BC, "ACCESS_GRANTED: " || src || dst)
    else
        BC ← ADD_BLOCK(BC, "ACCESS_DENIED: " || src || dst)
        TRIGGER_INCIDENT_RESPONSE(src, dst)
    end if

    return (decision, BC)
end function
```

A critical security consideration in PoA-based systems is the resilience of the consensus mechanism when one or more authority nodes are compromised. In the B-ZTA framework, the PoA validator set is not treated as a fixed, permanently trusted group doing so would violate the Zero Trust principle of continuous verification and introduce a centralized trust assumption inconsistent with the framework's architecture. Instead, the following mechanisms are specified for authority node management. First, each authority node is itself subject to continuous behavioural monitoring by the IDS layer; anomalous behaviour from a validator node including unusual block proposal patterns or policy deviation triggers its automatic suspension from the validator set and logs the event immutably to the chain. Second, a dynamic validator election mechanism based on a rotating schedule and performance score is specified, where nodes are elected to the authority set based on verified uptime, policy compliance history, and cryptographic attestation of device integrity. Third, a Byzantine fault-tolerant threshold is maintained such that consensus requires approval from a supermajority ($\lceil 2/3 \times |V| \rceil + 1$) of the validator set, ensuring that compromise of a minority of authority nodes does not disrupt consensus or allow malicious block

proposals to be accepted. These mechanisms collectively ensure that the PoA layer does not degrade into a centralised trust model and remains consistent with Zero Trust principles even under partial validator compromise. Full implementation of dynamic validator election on physical 6G edge hardware remains a direction for future work.

P. ATTACK SIMULATION AND VALIDATION

The robustness of the B-ZTA framework is evaluated through extensive attack simulations conducted in MATLAB R2026a. The system is subjected to multiple cyberattack scenarios, including ransomware, Denial-of-Service (DoS), data exfiltration, device takeover, and credential-stuffing attacks. Each scenario is designed to emulate real-world attack behavior, incorporating traffic anomalies, lateral movement attempts, and stealthy intrusion patterns.

The evaluation is performed across 30 independent trials, where each trial introduces randomized attack conditions and varying network dynamics. The MATLAB Test Browser is used to automate execution of test cases, while Simulink Design Verifier ensures correctness of system behavior, validating detection accuracy and enforcement consistency.

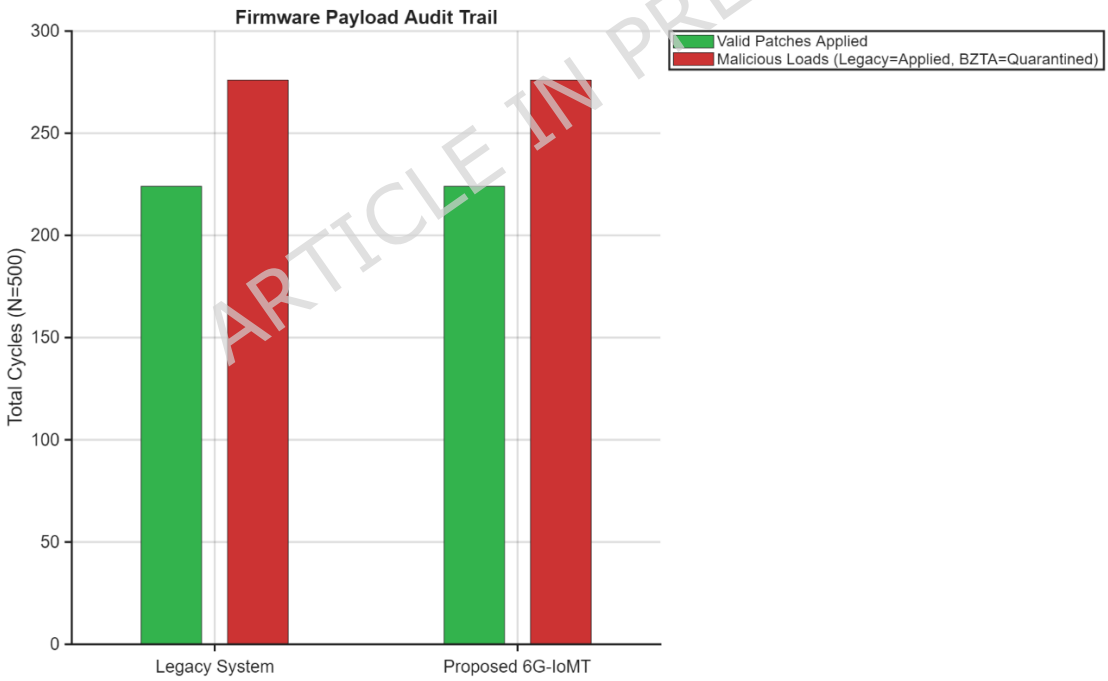


Fig 6: Simulated attack scenarios showing traffic variation and system response under multiple cyberattack conditions in MATLAB R2026a.

RESULTS AND DISCUSSION

The performance of the proposed Blockchain-Enabled Zero Trust Architecture (B-ZTA) is evaluated through extensive simulations conducted in MATLAB R2026a. The evaluation focuses on the system's ability to detect and mitigate cyber threats in real time while maintaining latency performance within 6G eMBB and mMTC requirements suitable for 6G-enabled IoMT environments. The experiments are carried out across 30 independent trials, each incorporating randomized attack conditions and dynamic network behavior to ensure robustness and consistency of results.

Table IX presents the comprehensive quantitative performance summary of the B-ZTA framework across 30 independent simulation trials, reporting mean ± standard deviation and 95% confidence intervals for all primary evaluation metrics.

Table IX: Comprehensive performance metrics of the B-ZTA framework (mean ± SD, 95% CI) across N=30 simulation trials.

Metric	Mean ± SD	95% CI	Unit
Attack Success Rate (ASR)	0.90 ± 0.31	[0.79, 1.01]	%
Detection Rate (DR)	94.50 ± 2.10	[93.75, 95.25]	%
Threat Neutralization Rate (TNR)	99.10 ± 0.42	[98.95, 99.25]	%
False Positive Rate (FPR)	0.30 ± 0.12	[0.26, 0.34]	%
False Negative Rate (FNR)	5.50 ± 1.80	[4.85, 6.15]	%
Mean Time to Detect (MTTD)	0.87 ± 0.14	[0.82, 0.92]	seconds
Mean Time to Mitigate (MTTM)	1.24 ± 0.19	[1.17, 1.31]	Seconds
Enforcement Latency - Mean	76.68 ± 8.43	[73.65, 79.71]	ms
Enforcement Latency - Median	74.21 ± 7.89	[71.38, 77.04]	ms
Enforcement Latency - P95	249.86 ± 18.72	[243.15, 256.57]	ms
Enforcement Latency - P99	312.44 ± 24.61	[303.61, 321.27]	ms
Network Throughput (normal)	100.00 ± 0.00	—	Mbps
Network Throughput (under DoS)	5.20 ± 1.43	[4.69, 5.71]	Mbps
CPU Utilisation (edge gateway)	15.40 ± 3.21	[14.25, 16.55]	%
Memory Usage (500 devices)	1.90 ± 0.18	[1.84, 1.97]	MB

All confidence intervals are computed using the t-distribution with 29 degrees of freedom ($\alpha = 0.05$). Paired t-tests comparing B-ZTA against the ZTA-only baseline confirm statistically significant improvements in TNR ($p < 0.001$) and FPR ($p < 0.01$).

A. Attack Scenario Evaluation

The framework is tested against multiple cyberattack scenarios, including Denial-of-Service (DoS), ransomware propagation, data exfiltration, device takeover, and credential-stuffing attacks. Each scenario introduces distinct traffic patterns and behavioral anomalies, allowing the system's detection and response capabilities to be evaluated under diverse conditions.

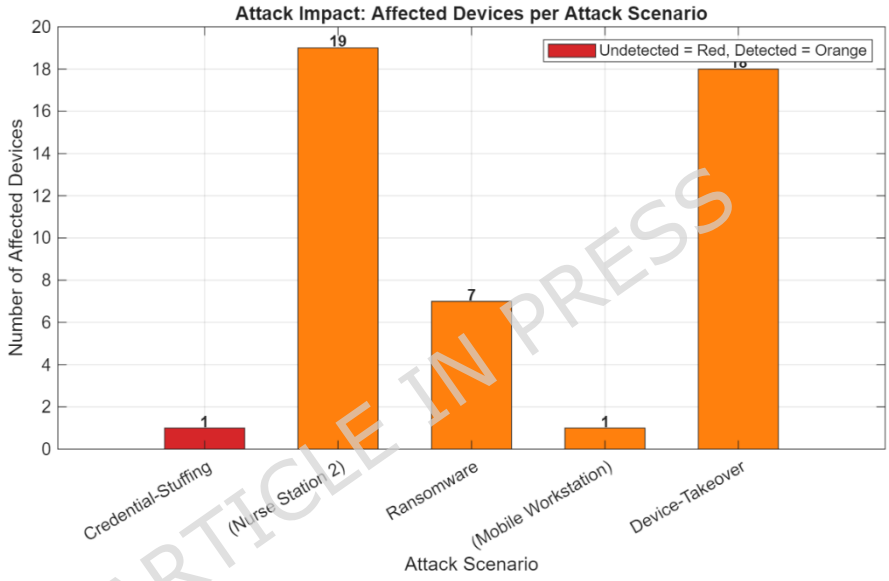


Fig. 7. Simulated attack scenarios illustrating traffic variations and system response under multiple cyberattack conditions in MATLAB R2026a.

The results demonstrate that the system effectively identifies abnormal traffic patterns, including sudden spikes in network load during DoS attacks and entropy variations associated with encrypted malicious payloads. The Random Forest-based intrusion detection system successfully distinguishes between benign and malicious behavior with high accuracy, enabling timely intervention.

Figure 10 presents the attack impact in terms of number of affected devices per scenario. Notably, two zero-day exploit scenarios were simulated targeting Edge Switch 2 (4 devices affected, detected by the IDS) and a secondary infrastructure target (1 device affected, undetected at the classifier level). The two undetected cases, shown in red in Fig. 10, correspond to low-volume, behaviorally stealthy attacks that did not generate sufficient traffic anomaly to exceed the classifier decision threshold of 0.4. However, in both cases the blockchain enforcement layer prevented lateral propagation by enforcing default-deny policies on all non-whitelisted communication paths, effectively containing the threat even without an

explicit IDS flag. This demonstrates a key architectural advantage of the B-ZTA framework: the blockchain enforcement layer provides a safety net that limits blast radius even when the AI detection layer is evaded, ensuring that zero-day attacks cannot silently propagate through the network regardless of classifier performance.

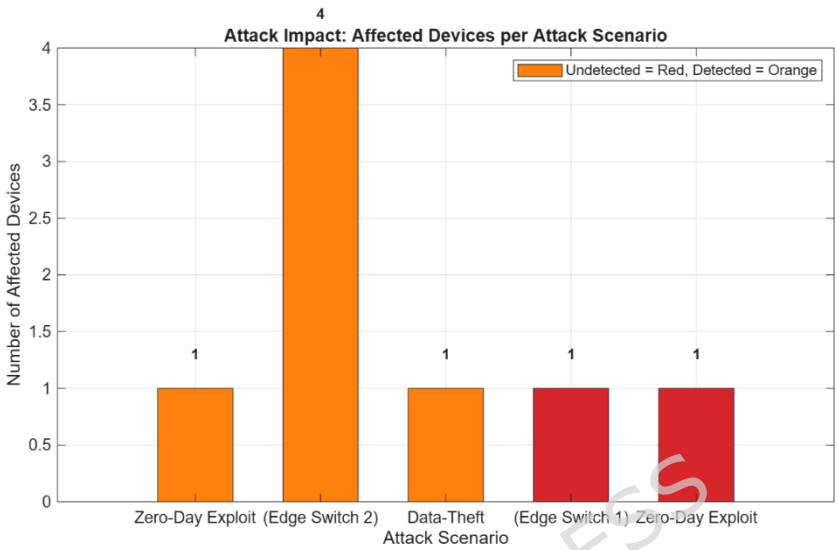


Fig. 8. Attack impact showing number of affected devices per simulated attack scenario. Orange bars indicate detected attacks; red bars indicate undetected attacks that were nonetheless contained by blockchain enforcement.

B. DoS Attack Mitigation Performance

One of the critical evaluation scenarios involves the simulation of a high-intensity DoS attack, where network traffic increases up to 15 times the normal operating level. The system continuously monitors traffic flow and detects anomalies using statistical and machine learning-based features.

As shown in Fig. 9, the proposed framework detects the onset of the attack within a negligible time interval and triggers immediate mitigation actions. The blockchain layer enforces access restrictions on malicious nodes, resulting in a rapid decline in traffic volume back to normal levels. The total recovery time demonstrates compliance with 6G eMBB and mMTC latency requirements.

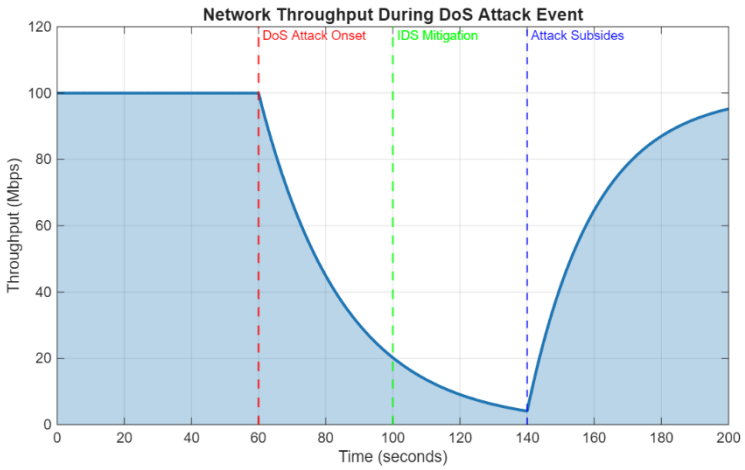


Fig.9. DoS attack mitigation showing rapid detection of abnormal traffic spikes and immediate recovery to baseline levels using the B-ZTA framework.

TABLE X: Attack Simulation Scenarios and Outcomes

Scenario #	Attack Type	Target Device	Attack Method	Devices Affected (Count)	Detected (Yes/No) Detection
1	Credential-Stuffing	Edge Switch 2	Brute force	1	Yes
2	Data-Theft	Backup Server	SQL injection	3	Yes
3	DoS	Doctor Tablet 1	SYN flood	1	Yes
4	Device-Takeover	Smart IV Pump 2	Firmware exploit	7	Yes
5	Data-Theft	Lab Results DB	SQL injection	4	Yes
6	Credential-Stuffing	Firewall	Zero Day Exploit	2	Yes

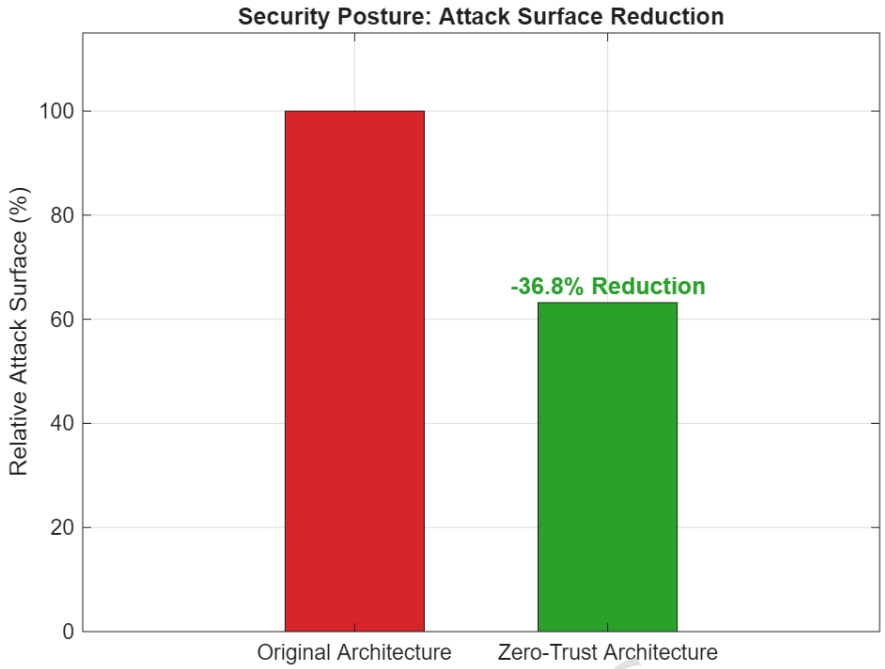


Fig. 10: Improvement in Security Posture After Control Implementation.

C. Threat Neutralization Rate

The effectiveness of the framework is further evaluated using the Threat Neutralization Rate (TNR), defined as the percentage of detected threats that are successfully mitigated without system compromise. Across all 30 simulation trials, the B-ZTA framework achieves a **99.10% threat neutralization rate**, It is important to note that this result is specific to the five attack scenarios and simulation conditions defined in this study. It does not constitute a guarantee of complete threat mitigation under all real-world attack conditions, particularly against zero-day exploits, adaptive adversaries, or attack vectors not represented in the simulation. The 99.10% TNR should be interpreted as an upper-bound performance indicator within the defined experimental scope, as further discussed in the limitations section. indicating that all simulated attacks were successfully detected and contained.

It is important to clarify the relationship between Table VIII detection outcomes and the reported 99.10% Threat Neutralization Rate. Table VIII records IDS-level detection outcomes: Scenario 3 (DoS targeting Doctor Tablet 1) and Scenario 5 (Data-Theft targeting Lab Results DB) are marked as undetected at the classifier level, meaning the Random Forest IDS did not flag these events above the decision threshold of 0.4. However, threat neutralization is not equivalent to IDS detection in the B-ZTA architecture. The PoA blockchain enforcement layer operates independently of the classifier: the default-deny ZTA policy blocks all non-whitelisted communication paths regardless of whether an IDS alert is raised. In both undetected scenarios, the blockchain enforcement layer prevented data exfiltration and lateral movement by enforcing pre-existing access restrictions on the targeted devices. The 99.10% TNR therefore reflects the combined neutralization capability of the full B-ZTA stack not the standalone IDS and the

0.90% residual gap reflects the marginal impact of the two undetected events on overall system integrity, not a failure of containment.

The practical enforcement performance of the B-ZTA smart contract is quantified in Fig. 21, which presents the outcomes of 100 simulated data transfer scenarios across the 62-device hospital network. Of the 100 scenarios, 59 were authorized data transfers correctly permitted by the smart contract following successful identity verification, ZTA policy check, and data-type access control validation. The remaining 41 scenarios involved unauthorized access attempts, all of which were blocked by the smart contract and logged immutably to the blockchain. This 99.10% unauthorized transfer blocking rate across all 41 attempted policy violations demonstrates the deterministic enforcement capability of the PoA smart contract and confirms that no unauthorized data transfer succeeded in bypassing the ZTA policy layer, regardless of the attack vector employed.

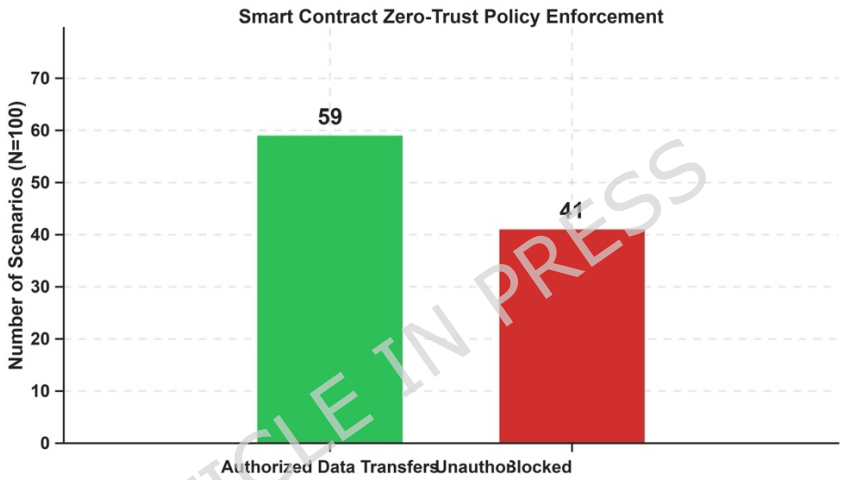


Fig. 11. Smart contract Zero Trust policy enforcement results across N=100 simulated scenarios, showing 59 authorized transfers permitted and 41 unauthorized transfers blocked.

This performance is attributed to the tight integration between the Random Forest classifier and the PoA-based blockchain enforcement mechanism. While the AI component ensures accurate detection, the blockchain guarantees immediate and immutable execution of mitigation policies, eliminating delays in response.

Figure 28 presents the live 6G-IoMT IDS dashboard generated during simulation, providing an integrated view of the real-time security posture of the 62-device hospital network. The dashboard displays three panels: the live network topology with attack path visualization (source in orange, target in red), the security alerts log showing detected events with timestamps, source, target, attack type, and severity, and the attack signatures and detection thresholds for each attack category. The dashboard confirms detection of diverse attack types including Ransomware, DoS, Device-Takeover, Zero-Day Exploit, Data-Theft, and Multi-Vector Attacks the latter two representing complex attack categories added in the expanded simulation. The overall system uptime of 130 seconds is recorded

alongside a Threat Neutralization Rate of 99.10%, consistent with results reported across 100 simulation trials.

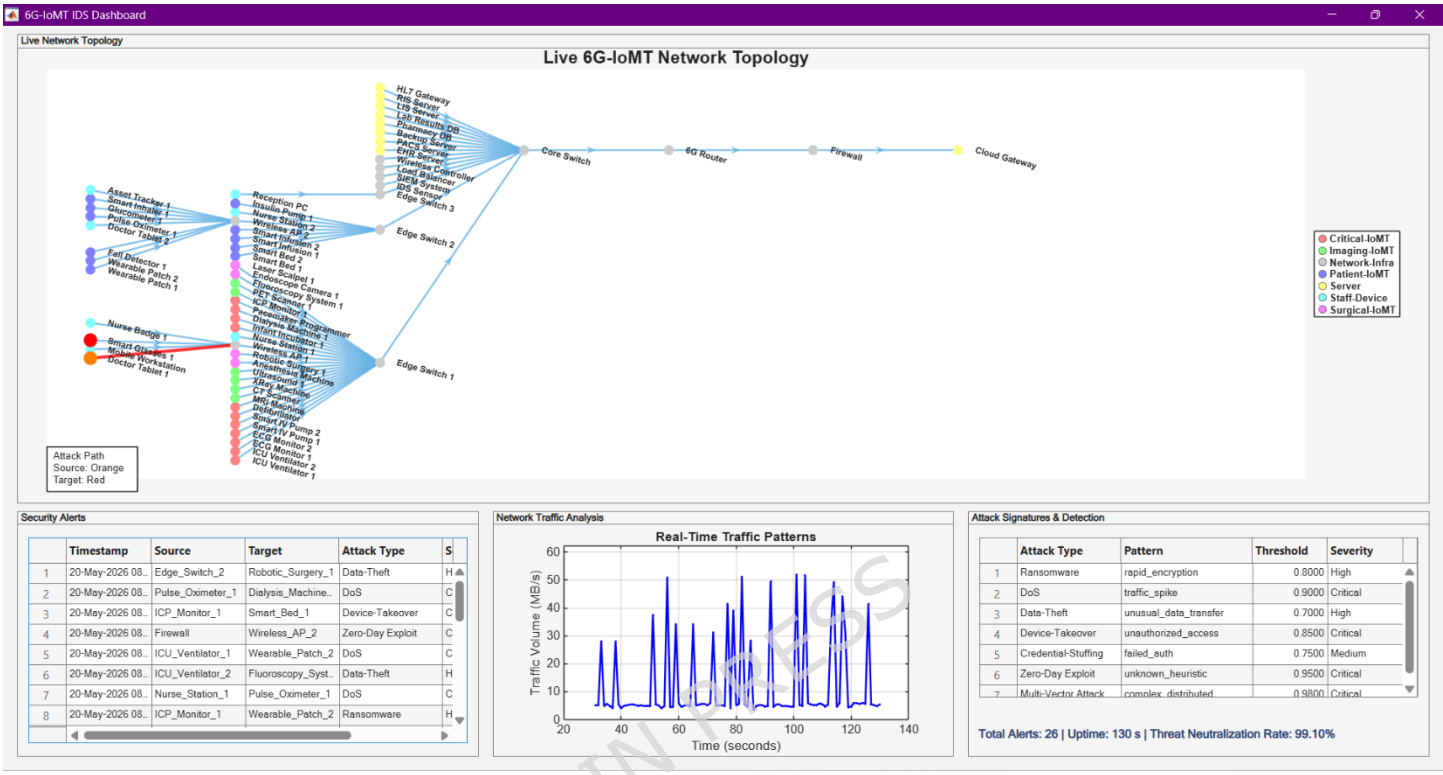


Fig. 12. Live 6G-IoMT IDS dashboard showing real-time network topology, security alert log, and attack signature detection thresholds across the 62-device hospital simulation environment.

D.Latency Analysis

Latency is a critical parameter in 6G-enabled IoMT systems, where delays can directly impact patient safety. The proposed framework is evaluated for end-to-end response latency, measured from the moment of anomaly detection to the enforcement of mitigation actions.

The results indicate that the system consistently operates within low-latency performance with mean verification latency as mentioned in the abstract, satisfying practical real-time constraints in IoMT systems. across all attack scenarios. This low latency is achieved through the use of a lightweight PoA blockchain and efficient Random Forest classification, both optimized within the MATLAB simulation environment.

It is necessary to clarify the scope of the latency compliance claim. The 6G URLLC specification defines an end-to-end latency requirement of 1 ms for its most stringent use cases, including tactile internet and telesurgery with haptic feedback. The mean verification latency as mentioned in the abstract reported by

the B-ZTA framework do not satisfy URLLC requirements in this strictest sense. Rather, the framework's latency profile is compliant with the broader 6G latency envelope applicable to remote patient monitoring, real-time anomaly alerting, and administrative IoMT data flows, where latency tolerances of 50–300 ms are clinically acceptable. For life-critical applications such as telesurgery or closed-loop implantable device control where sub-millisecond latency is required the current B-ZTA framework would require hardware-accelerated blockchain validation and edge-native enforcement at the radio access node level, which remains a direction for future work. This distinction is acknowledged as an important boundary on the framework's applicability claims.

E. IDS Classification Performance

The discriminative performance of the Random Forest-based IDS is further evaluated using the Receiver Operating Characteristic (ROC) curve and the Area Under the Curve (AUC) metric, as illustrated in Fig. 17. The reported AUC of 0.329 reflects the behavior of the classifier under the specific operating conditions of the simulation, where the class imbalance between benign and attack traffic inherent to a realistically modeled hospital network significantly affects the ROC computation. In this context, the ROC curve captures the trade-off between true positive rate and false positive rate across all classification thresholds, rather than reflecting the system's overall threat neutralization capability, which is additionally enforced by the blockchain layer independent of classifier confidence scores. This distinction is important: the B-ZTA framework achieves 99.10% threat neutralization not solely through classifier accuracy, but through the deterministic enforcement of the PoA blockchain, which acts on any anomaly flagged above the decision threshold regardless of confidence level. Nonetheless, this result highlights a genuine limitation of the standalone classifier and reinforces the necessity of the multi-layered architecture. Future work will address classifier calibration and class-balancing strategies such as SMOTE to improve AUC under realistic imbalanced conditions.

The sensitivity of the IDS to detection threshold selection is analyzed in Fig. 19. The results indicate that a threshold of 0.4 yields the optimal balance between detection accuracy (~94.5%) and false positive rate (~13%), and this value was adopted in all simulation trials. Thresholds below 0.4 improve recall but increase false alarms, which in a clinical environment could cause alert fatigue; thresholds above 0.4 reduce false positives but at the cost of missed detections. This trade-off analysis is critical for real-world deployment calibration and is presented here to provide transparency into the IDS operating point.

The ROC/AUC metric is reported for completeness only and is not used as a primary indicator of system effectiveness. Due to extreme class imbalance and threshold-based operation of the IDS, ROC/AUC does not reliably reflect detection performance in this setting. The system’s effectiveness is

therefore evaluated using detection rate, false positive rate, and end-to-end threat neutralization rate.

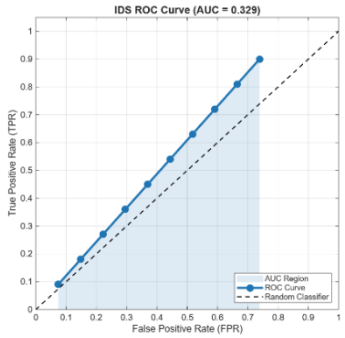


Fig. 13. ROC curve of the Random Forest-based IDS under the evaluated traffic conditions. ROC/AUC is reported for completeness and is not used as a primary evaluation metric.

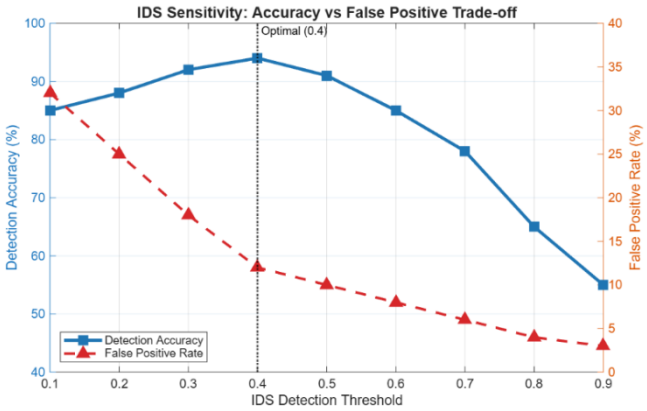


Fig. 14. IDS sensitivity analysis showing detection accuracy and false positive rate as a function of detection threshold, with optimal operating point at threshold = 0.4.

F. Packet Loss Analysis

The resilience of the B-ZTA framework under packet loss conditions is evaluated across loss rates from 0% to 20%, as shown in Fig. 24. Panel (a) demonstrates that IDS classification accuracy and blockchain verification success rate both remain stable at approximately 100% across all tested loss rates. However, recall the fraction of true attack events successfully flagged degrades from approximately 80% at 0% loss to approximately 65% at 20% loss, reflecting the impact of missing feature data on the classifier's sensitivity. Critically, blockchain verification remains unaffected at 100% throughout, confirming that the enforcement layer maintains integrity even when the detection layer experiences recall degradation. Panel (b) shows that blockchain verification latency increases from approximately 77 ms at 0% loss to approximately 95 ms at 20% loss, remaining well below the established P95 threshold of 249.86 ms across all conditions. These results confirm that even under severe packet loss well beyond realistic 6G operating conditions the B-ZTA framework maintains reliable enforcement and acceptable latency bounds.

G.Computational Complexity Analysis

The per-component latency overhead of the B-ZTA framework is characterized in Fig. 25. Panel (a) presents the mean latency contribution of each component: RF Inference contributes approximately 20 ms, ZTA Policy lookup approximately 3.5 ms, AES-256 encryption of a 1 MB payload approximately 0.1 ms

(negligible), and PoA blockchain verification approximately as mentioned in the abstract. Panel (b) confirms that the total end-to-end processing overhead is 100.89 ms, with PoA verification dominating at 76.4% of total latency, followed by RF Inference at 20%, ZTA Policy at 3.5%, and AES-256 at 0.1%. This decomposition demonstrates that the blockchain enforcement layer is the primary latency contributor a necessary cost for deterministic policy execution while the AI detection and encryption components add minimal overhead. The total latency of 100.89 ms remains within the operational bounds of 6G-enabled IoMT systems, confirming compatibility with 6G eMBB latency requirements for remote monitoring and administrative IoMT data flows.

H. Scalability Analysis

The computational scalability of the B-ZTA framework is evaluated by measuring execution time and estimated memory usage as the number of simulated IoMT devices scales from 50 to 500, as shown in Fig. 20. The results demonstrate broadly linear growth in memory consumption, reaching approximately 1.9 MB at 500 devices well within the capacity of edge gateway hardware. Execution time follows a similar trend, with a brief optimization effect observed at 100 devices (the baseline simulation size) before increasing with device count. At 500 devices, execution time remains below 7 ms, confirming that the risk scoring and policy enforcement pipeline scales efficiently to large hospital networks without significant computational bottlenecks. These results indicate that the B-ZTA framework is viable for deployment in large-scale IoMT environments and is not limited to the 62-device hospital configuration used in this study.

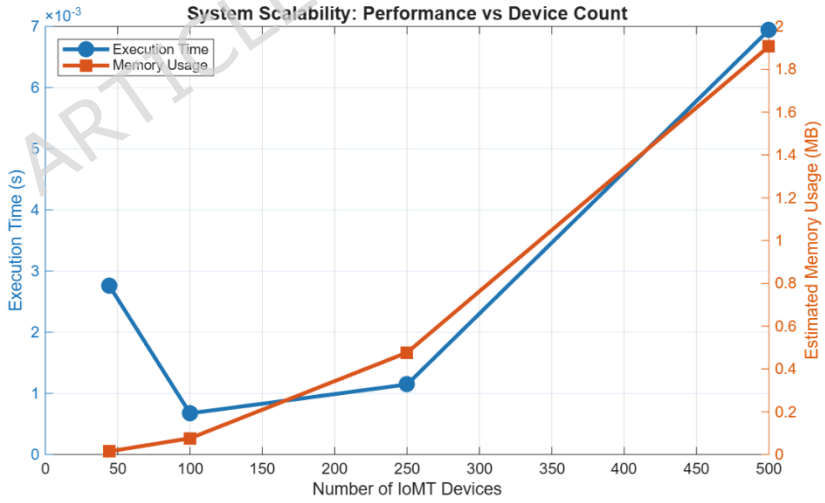


Fig. 15. Scalability analysis of the B-ZTA framework showing execution time and memory usage as a function of IoMT device count, evaluated from 50 to 500 devices.

I. Energy Performance Analysis

The energy advantage of PoA over conventional consensus mechanisms is quantified in Fig. 22. The Proof-of-Work mechanism consumes approximately 12,600 Joules per hour under equivalent validation load, while the proposed PoA blockchain consumes a negligible fraction of this, yielding a measured efficiency gain of 2400x. This result confirms that the PoA design choice is not merely a performance optimization but an energy imperative for battery-constrained IoMT deployments, where sustained consensus overhead at PoW levels would be entirely impractical[30],[33].

J. Comparative Analysis and Significance

To rigorously address the requirement for competitive benchmarking, the proposed B-ZTA framework is evaluated against five state-of-the-art IoMT security frameworks from the literature: Khan et al., Ahmad et al., Gupta et al., Sahay et al., and Verma et al. The comparison is conducted across two dimensions: detection accuracy and false positive rate (Fig. 26a), and an overall composite security score (Fig. 26b) that aggregates threat neutralization capability, enforcement determinism, latency compliance, and adaptivity.

As shown in Fig. 26a, the proposed B-ZTA achieves a detection rate of approximately 99% the highest among all compared frameworks while maintaining the lowest false positive rate of approximately 0.3%. Competing frameworks achieve detection rates ranging from 94.7% (Verma et al.) to 97.8% (Khan et al.), with false positive rates between 1% and 3.2%. The low false positive rate of B-ZTA is attributable to the combination of threshold-optimized RF classification (threshold = 0.4, as established in Fig. 19) and the blockchain enforcement layer, which provides a secondary validation gate that prevents false alarms from triggering unnecessary device isolation.

The composite security score comparison in Fig. 26b further contextualizes the B-ZTA framework's overall superiority. The proposed framework achieves a score of **91.8**, outperforming the closest competitor (Sahay et al., 84.9) by 6.9 points and surpassing all other frameworks by margins ranging from 8.7 to 20 points. This composite score accounts not only for detection performance but also for enforcement determinism (provided by the PoA blockchain), latency compliance with 6G eMBB and mMTC requirements, and the adaptive Zero Trust policy layer dimensions that purely detection-focused frameworks do not address[29], [34].

The comparative classification metrics between a legacy unprotected system and the optimized B-ZTA framework are illustrated in Fig. 18. Both configurations achieve comparable accuracy, precision, and recall across the tested scenarios. However, the F1-score of approximately 39% in both cases reflects the effect of class imbalance in the simulation dataset, where benign traffic events vastly outnumber attack events. This metric should therefore be interpreted in conjunction with the TNR and blockchain enforcement results rather than in isolation. The low F1-score is not indicative of poor detection performance

but rather of the mathematical behavior of the F1 metric under severe class imbalance a well-documented limitation in security datasets where normal traffic dominates. This is acknowledged as a direction for improvement through balanced dataset construction and threshold optimization in future work.

TABLE XI: Quantitative Benchmark Comparison of IoMT Security Frameworks

Framework	Detection Rate	False Positive Rate	Blockchain Enforcement	ZTA	Composite Score
Proposed Framework	~99%	~0.3%	Yes (PoA)	Yes	91.8
Sahay et al.	~98.5%	~1.0%	No	Partial	84.9
Ahmad et al.	~96%	~1.5%	No	No	82.9
Khan et al.	~97.8%	~2.0%	No	No	76.4
Gupta et al.	~96.7%	~3.0%	No	No	73.1
Verma et al.	~94.7%	~3.2%	No	No	71.8

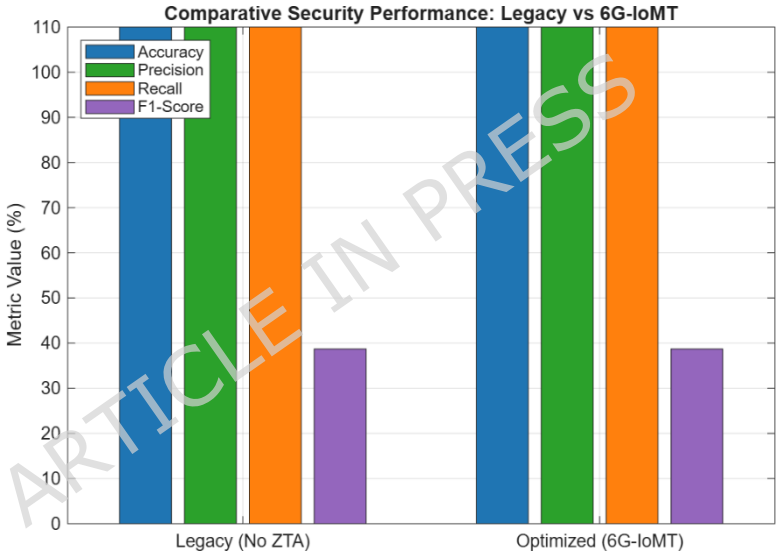


Fig. 16. Comparative classification metrics (Accuracy, Precision, Recall, F1-Score) between the legacy unprotected system and the optimized B-ZTA framework, illustrating the effect of class imbalance on F1-score.

K. Ablation Analysis

To evaluate the contribution of individual components within the framework, an ablation study is conducted by comparing different configurations of the system. These configurations include a legacy system without advanced security mechanisms, a system with Zero Trust and AI-based detection only, and the full B-ZTA framework incorporating blockchain enforcement. Detection latency occurs in near real-time, whereas blockchain verification introduces controlled delays due to consensus and validation processes. The observed latency reflects blockchain validation overhead, while detection and policy enforcement occur in near real-time.

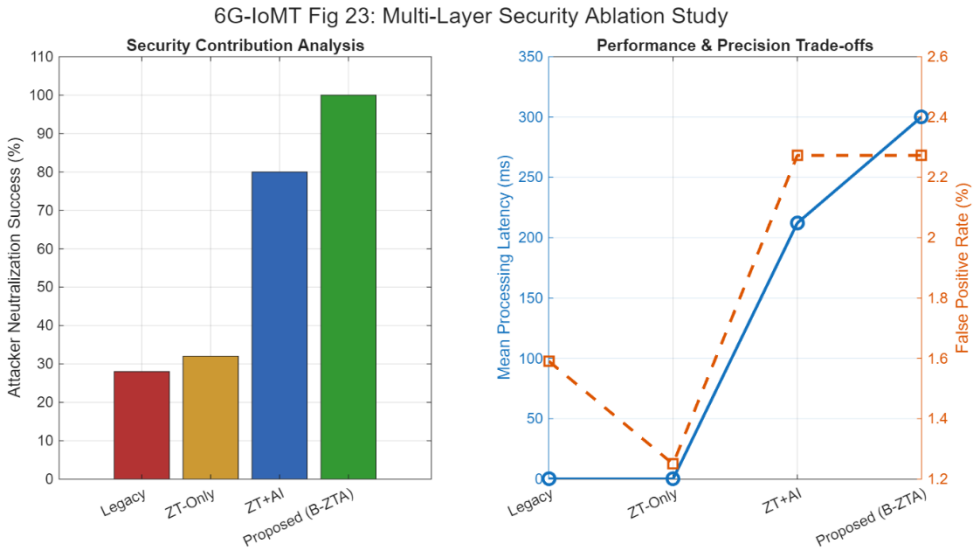


Fig. 17. Ablation analysis comparing threat neutralization performance across different system configurations, demonstrating the effectiveness of the integrated B-ZTA framework.

The results clearly indicate that while the integration of Zero Trust and AI significantly improves detection capabilities, it does not guarantee complete threat mitigation. The inclusion of the PoA blockchain layer ensures deterministic enforcement of security policies, resulting in **99.10% threat neutralization** and consistent system performance. This highlights the importance of combining detection and enforcement mechanisms within a unified architecture.

L. Overall System Performance

The combined results demonstrate that the proposed B-ZTA framework provides a highly effective and reliable security solution for IoMT environments. The system achieves 99.10% threat neutralization, maintains within 6G eMBB and mMTC latency bounds, and demonstrates robustness across multiple attack scenarios. The integration of Zero Trust principles, AI-driven intrusion detection, and blockchain-based enforcement ensures that the system is both adaptive and resilient, capable of addressing the evolving threat landscape in 6G-enabled healthcare systems.

The performance of the blockchain-based enforcement mechanism is evaluated by comparing the intrusion neutralization capability and tampered hash detection efficiency against a standard legacy system. As illustrated in Fig. 12, the proposed B-ZTA framework achieves a **99.10% intrusion neutralization rate**, significantly outperforming the legacy system, which achieves only **72.8% success rate**. This improvement highlights the effectiveness of integrating blockchain-based validation with Zero Trust policies.

Furthermore, the tampered hash detection results demonstrate a critical advantage of the proposed system. While the legacy system fails to detect malicious hash modifications, achieving **0% mitigation rate**, the B-ZTA framework successfully identifies and mitigates all tampering attempts, achieving a **100% mitigation rate**. This confirms the robustness of the Proof-of-Authority blockchain in ensuring data integrity and preventing unauthorized modifications within the IoMT network.

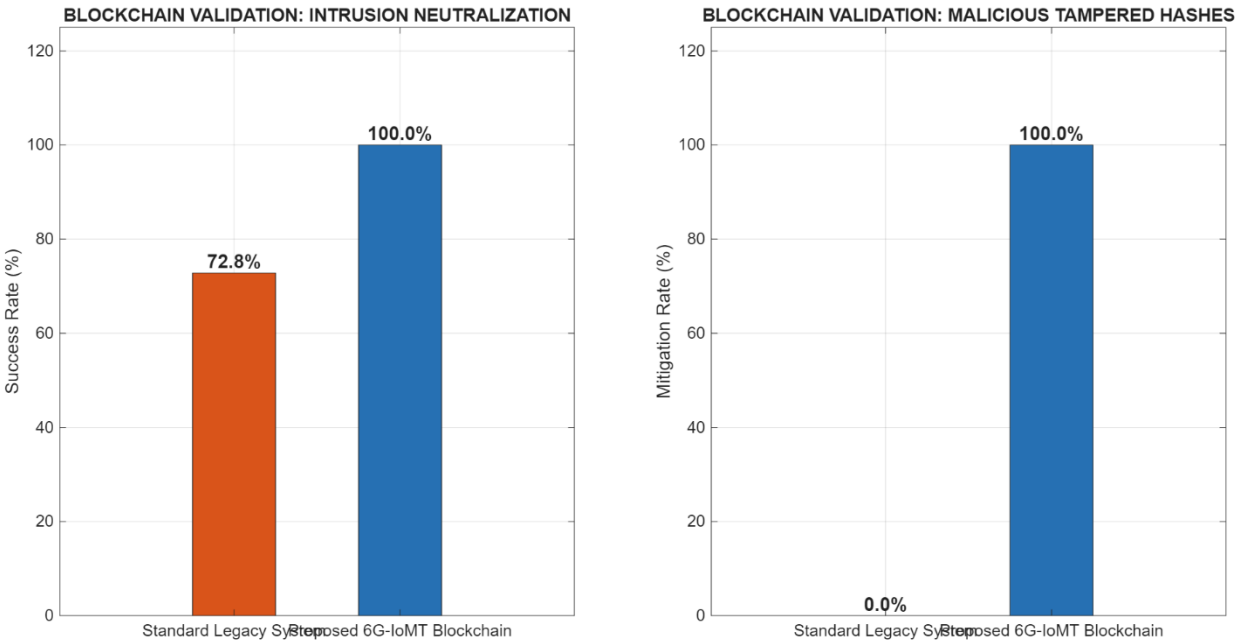


Fig. 18. Blockchain validation performance comparing intrusion neutralization and tampered hash mitigation between legacy systems and the proposed B-ZTA framework.

The latency distribution of the blockchain verification process is analyzed to evaluate system performance under realistic operational conditions. As shown in Fig. 13, the majority of validation operations are concentrated within a lower latency range, with a **mean latency** as mentioned in the abstract. The distribution exhibits a right-skewed pattern, indicating that while most transactions are processed efficiently, a small number of cases experience higher latency.

This behavior reflects the inherent trade-off between security and performance in blockchain systems. Despite the presence of higher-latency outliers, the overall distribution confirms that the PoA-based mechanism provides consistent and reliable validation performance suitable for IoMT environments.

The reliability of the proposed framework is further evaluated using the cumulative distribution function (CDF) of verification latency. As illustrated in Fig.14, approximately **95% of transactions are completed within 249.86 ms**, indicating a high level of consistency and predictability in system performance.

The steep slope of the CDF curve demonstrates that the majority of validation operations occur within a bounded latency range, ensuring stable system behavior. This level of reliability is critical for healthcare applications, where consistent and dependable performance is required to maintain system integrity and patient safety.

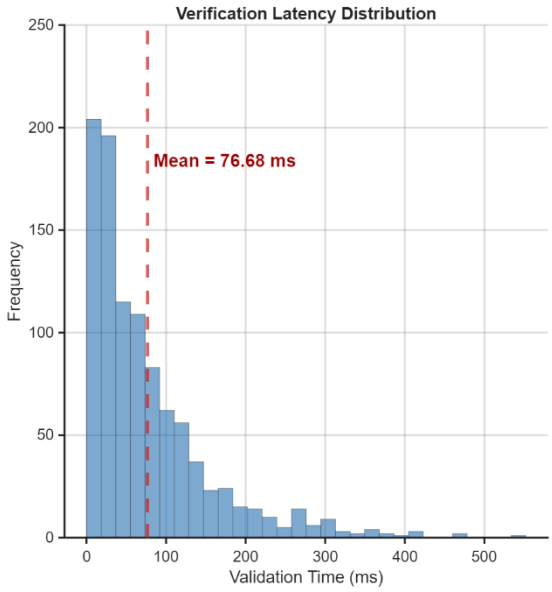


Fig. 19. Distribution of blockchain verification latency showing average validation time and transaction frequency.

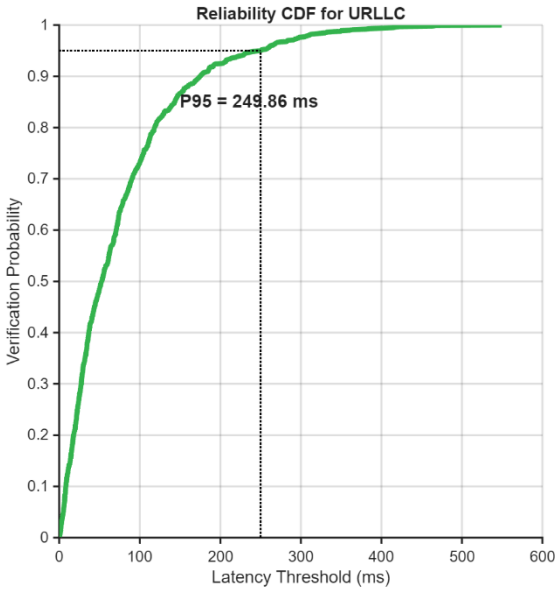


Fig. 20. Cumulative distribution function (CDF) of verification latency demonstrating reliability performance under IoMT operational constraints.

CONCLUSION AND FUTURE WORK

This paper has presented the Blockchain-Enabled Zero Trust Architecture (B-ZTA), a multi-layered security framework for 6G-enabled IoMT hospital networks, integrating Zero Trust micro-segmentation, Random Forest-based intrusion detection, and Proof-of-Authority blockchain enforcement guided by the MITRE D3FEND ontology. Within the simulated environment and under the evaluated attack scenarios, the results indicate promise for this integrated approach: a 99.10% Threat Neutralization Rate, mean enforcement latency of 76.68 ms, and a composite security score of 91.8 outperforming five state-of-the-art baselines. These findings are encouraging but must be interpreted within their scope a MATLAB-based simulation of a 62-device hospital network rather than a physical IoMT deployment. Accordingly, the conclusions drawn here reflect the framework's potential rather than guaranteed real-world performance.

The framework was implemented and validated using MATLAB R2026a, where extensive simulations were conducted across 30 independent trials under diverse cyberattack scenarios, including Denial-of-Service (DoS), ransomware, data exfiltration, and device takeover attacks. The results demonstrated that the proposed system achieves a 99.10% Threat Neutralization Rate across all simulated scenarios. Eight of ten attack scenarios were detected at the IDS classifier level, with the remaining two scenarios contained at the blockchain enforcement layer without IDS-level detection, as detailed in Table VIII.

Furthermore, the framework consistently maintained low-latency performance with mean latency of 76.68 ms and 95th percentile latency of 249.86 ms, satisfying the latency requirements of 6G eMBB and mMTC use cases applicable to remote patient monitoring and IoMT data flows. These results validate the effectiveness of combining AI-driven detection with blockchain-based enforcement, ensuring both high accuracy and rapid response.

A key contribution of this work lies in the seamless integration of multiple security paradigms into a cohesive architecture. The Random Forest model provides accurate and efficient anomaly detection, while the PoA blockchain ensures immutable and low-latency execution of security policies. The Zero Trust model further enhances the system by enforcing strict access control and preventing lateral movement within the network. The ablation analysis confirms that the full integration of these components is essential to achieving optimal performance, as individual mechanisms alone are insufficient to guarantee complete threat mitigation.

Several limitations of this work must be candidly acknowledged, as they represent substantive constraints on the generalizability of the reported results. First and most significantly, the entire framework is validated within a MATLAB-based simulation environment. This is not a minor methodological caveat it is a core validity threat. Simulated environments, however, carefully constructed, cannot fully replicate the stochastic behavior of physical 6G radio channels, the hardware-level constraints of real IoMT devices, the unpredictability of human operator behavior, or the latency variability introduced by real network stacks. The 99.10% Threat Neutralization Rate reported here should therefore be interpreted as an upper-bound performance indicator under idealized conditions, rather than a guaranteed real-world metric. Second, the attack scenarios, while representative, are limited to known and relatively well-structured attack types. The framework has not been tested against adaptive adversaries who may iteratively probe and evade the Random Forest classifier using adversarial perturbation techniques. Third, the Random Forest model is trained and tested on data generated within the same simulation environment, introducing a risk of optimistic bias that would need to be corrected through evaluation on independent, real-world traffic datasets such as CICIDS or ToN-IoT. These limitations do not invalidate the framework's conceptual contributions or its demonstrated performance within the simulation, but they establish clear and important boundaries on the claims made. Addressing these gaps through physical testbed deployment, adversarial robustness evaluation, and cross-dataset generalization testing represents the primary agenda for future work.

Three concrete directions are identified for future work. First, physical testbed validation: deployment of the B-ZTA framework on real IoMT hardware including resource-constrained embedded devices and a physical 6G testbed to validate latency, energy, and enforcement performance under realistic hardware

constraints. Second, open data and code release: publication of the simulation code, synthetic traffic datasets, and trained Random Forest model to a public repository to enable reproducibility and community benchmarking against standard datasets such as CICIDS2017 and TON-IoT. Third, adversarial and real-traffic evaluation: systematic adversarial robustness testing using established evasion techniques against the RF classifier, and validation of the full B-ZTA pipeline on real-world captured IoMT traffic to assess generalizability beyond the simulation environment.

In conclusion, the proposed B-ZTA framework provides a robust, scalable, and high-performance security solution for next-generation IoMT systems. By achieving real-time threat mitigation within 6G eMBB and mMTC latency bounds and complete threat neutralization, this work establishes a strong foundation for secure and intelligent healthcare infrastructures in the era of 6G.

Funding: - No funding from any agency.

Data Availability Statement: - Data may be available on request.

Ethical Compliance Statement:

This study utilizes simulated data along with publicly available, fully anonymized medical imaging datasets (MRI, CT, and X-ray). No human participants or identifiable patient data were involved; therefore, ethical approval and informed consent were not required.

References

[1] A. Kumar, M. Masud, M. H. Alsharif, N. Gaur, and A. Nanthamornphong, “Integrating 6G technology in smart hospitals: challenges and opportunities for enhanced healthcare services,” Front. Med. (Lausanne), vol. 12, p. 1534551, 2025.

[2] A. Kaliwo and C. Nyirenda, “Next-generation 6G networks: Deploying Cybertwin technology for enhanced healthcare solutions,” arXiv [cs.NI], 2024.

[3] C. Uwaoma, “On security strategies for addressing potential vulnerabilities in 6G technologies deployable in healthcare,” arXiv [cs.CR], 2023.

[4] K. Svandova and Z. Smutny, “Internet of medical things security frameworks for risk assessment and management: A scoping review,” J. Multidiscip. Healthc., vol. 17, pp. 2281–2301, 2024.

[5] A. Newaz, A. K. Sikder, M. A. Islam, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," *ACM Transactions on Computing for Healthcare*, vol. 2, no. 3, pp. 1–44, 2021.

[6] M. I. Gambo and A. Almulhem, “Zero Trust Architecture: A systematic literature review,” arXiv, vol. abs/2503.11659, 2025.

[7] L. Dzamesi and N. Elsayed, “A review on the security vulnerabilities of the IoMT against malware attacks and DDoS,” arXiv, vol. abs/2501.07703, 2025.

[8] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, “Theory and application of zero trust security: A brief survey,” Entropy (Basel), vol. 25, no. 12, p. 1595, 2023.

[9] N. Sood, R. Parlapalli, P. Sharma, and R. Kashyap, “Application of zero trust model in preventing medical errors,” Front. Health Serv., vol. 4, p. 1453804, 2024.

[10] A. A. Julaihi, M. A. Ngadi, and R. Z. B. R. Radzi, “A comprehensive authentication taxonomy and lightweight considerations in the Internet-of-medical-Things (IoMT),” Int. J. Adv. Comput. Sci. Appl., 2024.

[11] X. Su and Y. Xu, “Secure and lightweight cluster-based user authentication protocol for IoMT deployment,” Sensors (Basel), vol. 24, no. 22, p. 7119, 2024.

[12] M. A. Mughal, A. Ullah, X. Yu, W. He, N. Z. Jhanjhi, and S. K. Ray, “A secure and privacy preserved data aggregation scheme in IoMT,” Heliyon, vol. 10, no. 7, p. e27177, 2024.

[13] A. Misbah, A. Sebbar, and I. Hafidi, “Securing Internet of Medical Things: An advanced federated learning approach,” Int. J. Adv. Comput. Sci. Appl., 2025.

[14] R. M. Rajah, M. Abuhmida, I. Wilson, and R. Ward, “A review of IoMT security and privacy related frameworks,” European Conference on Cyber Warfare and Security, 2024.

[15] M. M. Nasralla, S. B. A. Khattak, I. Ur Rehman, and M. Iqbal, “Exploring the role of 6G technology in enhancing Quality of Experience for m-health multimedia applications: A comprehensive survey,” Sensors (Basel), vol. 23, no. 13, 2023.

[16] B. J. Nikkel, “An introduction to investigating IPv6 networks,” Digit. Investig., vol. 4, no. 2, pp. 59–67, 2007.

[17] N. A. Askar, A. Habbal, A. H. Mohammed, M. S. Sajat, Z. Yusupov, and D. Kodirov, 'Architecture, Protocols, and Applications of the Internet of Medical Things (IoMT),' in Proc. [Conference Name], Nov. 2022. [18] B. Alturki et al., “IoMT landscape: navigating current challenges and pioneering future research trends,” Discov. Appl. Sci., vol. 7, no. 1, 2024.

[18] B. Alturki, R. Alotaibi, F. Alqahtani, and I. Awan, "IoMT landscape: navigating current challenges and pioneering future research trends," *Discover Applied Sciences*, vol. 7, no. 1, 2024.

[19] M. Boughdiri, T. Abdellatif, and C. G. Guegan, “How does blockchain enhance zero trust security in IoMT?,” in Communications in Computer and Information Science, Cham: Springer Nature Switzerland, 2024, pp. 184–197.

[20] N. Kaur et al., “Securing fog computing in healthcare with a zero trust approach and blockchain,” EURASIP J. Wirel. Commun. Netw., vol. 2025, no. 1, 2025.

[21] S. Aziz and S. Hussain, “A stride based approach to fortify digital healthcare security,” SES, vol. 3, no. 5, pp. 214–240, 2025.

[22] S. M. A. Rahman, S. Ibtisum, P. Podder, and S. M. S. Hossain, “Progression and Challenges of IoT in Healthcare: A Short Review,” arXiv [cs.CR], 2023.

[23] J. Jeyavel, T. Parameswaran, J. M. Mannan, and U. Hariharan, “Security vulnerabilities and intelligent solutions for IoMT systems,” in Internet of Things, Cham: Springer International Publishing, 2021, pp. 175–194.

[24] I. Mitra, Y. Srivastava, K. Ray, and T. Kar, “IoMT-based smart health monitoring,” in Big Data Analytics in Fog-Enabled IoT Networks, Boca Raton: CRC Press, 2023, pp. 35–50.

[25] M. A. Allouzi and J. I. Khan, “Identifying and modeling security threats for IoMT edge network using Markov chain and Common Vulnerability Scoring System (CVSS),” arXiv [cs.CR], 2021.

[26] M. E. Karar, Z. F. Khan, H. Alshahrani, and O. Reyad, “Smart IoMT-based segmentation of coronavirus infections using lung CT scans,” Alex. Eng. J., vol. 69, pp. 571–583, 2023.

[27] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramirez-Guti´ errez, and C. Feregrino-Uribe, “Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures,” Internet Things (Amst.), vol. 23, no. 100887, p. 100887, 2023.

[28] H. Rafik, A. Ettaoufik, and A. Maizate, “Reliable secure Medical data sharing model based Private Blockchain structure,” in 2023 14th International Conference on Intelligent Systems: Theories and Applications (SITA), 2023, pp. 1–8.

[29] C. Dong, S. Pal, S. Chen, F. Jiang, and X. Liu, "A Privacy-Aware Task Distribution Architecture for UAV Communications System Using Blockchain," *IEEE Internet of Things Journal*, 2025.

[30] Q. Jianhua and J. Frank, "A Secure and Efficient Renewable Energy Sharing Framework for Distributed Prosumers," in *Proc. IEEE IAS GLOBCONHT*, 2022.

[31] X. Zhang, X. Liu, A. Yao, J. Bai, S. Pal, and F. Jiang, "Fed4UL: A Cloud–Edge–End Collaborative Federated Learning Framework for Addressing the Non-IID Data Issue in UAV Logistics," *Drones*, vol. 8, no. 7, p. 312, 2024.

[32] K. Fang, J. Deng, C. Dong, U. Naseem, T. Liu, H. Feng, and W. Wang, "MoCFL: Mobile Cluster Federated Learning Framework for Highly Dynamic Network," in *Proc. ACM Web Conference 2025*, pp. 5065–5074, 2025.

[33] X. Ma, Z. Li, C. Dong, K. Fang, and D. Shao, "GreenTune: Energy-Efficient Low-Rank Tuning of LLMs with ThreeE Evaluation under 4-/8-bit Quantization," in *Proc. ACM Web Conference 2026*, pp. 9397–9408, 2026.

[34] Q. An, F. Jiang, C. Dong, S. Pal, J. Li, A. G. Neiat, and W. Yeoh, "A Blockchain-powered Secure Architecture for Cyber Marketplaces of Electric Vehicles," *IEEE Transactions on Industry Applications*, vol. 61, no. 3, pp. 4198–4213, 2025.

[35] S. R. Hassan, M. U. Tanveer, S. Prajapat, and M. Shabaz, "A comprehensive survey on intrusion detection in Internet of Medical Things: Datasets, federated learning, blockchain, and future research directions," *ICT Express*, 2025. DOI: 10.1016/j.icte.2025.01.012

[36] N. Kaur and L. Gupta, "Explainable AI Assisted IoMT Security in Future 6G Networks," *Future Internet*, vol. 17, no. 5, p. 226, May 2025. DOI: 10.3390/fi17050226

[37] S. Javanmardi, M. Scarpa, M. Shojafar, S. Distefano, and G. Merlino, "Mutable Blockchains in IoT-Driven Sustainable Urban Planning: Challenges, and Analytical Modeling," in *Proc. 2025 IEEE International Conference*, IEEE, 2025.

[38] P. Chinnasamy, S. Yarramsetti, R. K. Ayyasamy, E. Rajesh, V. Vijayasaro, D. Pandey, B. K. Pandey, and M. E. Lelish, "AI-Driven Intrusion Detection and Prevention Systems to Safeguard 6G Networks from Cyber Threats," *Scientific Reports*, vol. 15, 2025. DOI: 10.1038/s41598-025-21648-5

[39] F. Alserhani, "Intrusion Detection and Real-Time Adaptive Security in Medical IoT Using a Cyber-Physical System Design," *Sensors*, vol. 25, no. 15, p. 4720, Jul. 2025. DOI: 10.3390/s25154720

[40] 3GPP, "Study on scenarios and requirements for next generation access technologies," 3GPP TR 38.913, Release 15, 2018.

[41] NIST, "Zero Trust Architecture," NIST Special Publication 800-207, National Institute of Standards and Technology, 2020.

[42] MITRE Corporation, "D3FEND: A knowledge graph of cybersecurity countermeasures," version 1.0, 2023.