Discover Internet of Things

https://doi.org/10.1007/s43926-026-00357-z

Article in Press

A strategic cybersecurity framework leveraging MITRE D3FEND for resilient 6G-enabled IoMT healthcare networks

Received: 30 December 2025

Accepted: 8 May 2026

Published online: 19 May 2026

Cite this article as: Shaik M.N., Jain A. & Rohith K. A strategic cybersecurity framework leveraging MITRE D3FEND for resilient 6G-enabled IoMT healthcare networks. *Discov Internet Things* (2026). https://doi.org/10.1007/s43926-026-00357-z

Mahmmad Nazir Shaik, Abhishek Jain & Katreddi Rohith

A Strategic Cybersecurity Framework Leveraging MITRE D3FEND for Resilient 6G-Enabled IoMT Healthcare Networks

Mahmmad Nazir Shaik[1], *Abhishek Jain[2], Katreddi Rohith[3]
School of Engineering and Technology, BML Munjal University, Gurugram 122413, India
Email : shaikmahmmad.nazir.21cse@bmu.edu.in, abhishek.jain@bmu.edu.in, katreddi.rohith.21cse@bmu.edu.in
ORCID: 0009-0006-1652-5073, 0000-0001-9018-9203, 0009-0004-9484-4753
Corresponding Author: Dr. Abhishek Jain

ABSTRACT

The convergence of sixth-generation (6G) wireless networks and the Internet of Medical Things (IoMT) creates transformative opportunities for healthcare while significantly expanding the cybersecurity attack surface of hospital environments. This paper proposes and evaluates a strategic, multi-layered cybersecurity framework for 6G-enabled IoMT hospital networks, validated through a MATLAB simulation of a 44-device hospital topology spanning seven device categories. The framework operates across four phases: STRIDE-based threat modelling with composite attack surface scoring; Zero Trust policy enforcement with criticality-stratified authentication and multi-protocol encryption (AES-256, TLS 1.3, DICOM-Secure, WPA3, IPSec); hybrid signature-anomaly intrusion detection evaluated against five attack classes; and MITRE D3FEND-aligned defence optimisation via the proposed Data-Driven Defence Mechanism for Enhanced Network Control and Resilience (D3-MENCR). Zero Trust enforcement reduced permitted network connections by 36.8%, from 1,532 to 964, while encryption overhead remained below 91 ms across all simulated transmission scenarios. The intrusion detection system achieved a 61% detection rate with an average detection latency of 48.49 seconds, with device-takeover attacks identified as the primary detection gap. DoS simulation reduced network throughput from 100 Mbps to 10 Mbps, recovering to 80 Mbps post-mitigation, and a 30% data tampering rate degraded diagnostic accuracy from above 90% to 86%. D3-MENCR improved data integrity check success rates from 75-85% to 83-93%, with D3FEND control overhead remaining within an operationally acceptable range of approximately 110 ms. These results demonstrate the feasibility and resilience of the proposed framework for securing 6G-IoMT hospital deployments.

Index Terms - IoMT, 6G Networks, Zero Trust Architecture, Intrusion Detection Systems, Network Segmentation, Cyber Resilience

I. INTRODUCTION

The Internet of Medical Things (IoMT) is reshaping healthcare by enabling continuous remote monitoring, real-time data exchange, and intelligent hospital operations through internet-connected medical devices. The global IoMT market, valued at $113.75 billion in 2019, is projected to reach $332.67 billion by 2027 at a compound annual growth rate of 13.5%. The convergence of IoMT with 6G wireless networks offering sub-millisecond latency, AI-native communication, and terahertz-band throughput further extends these capabilities to remote telesurgery, holographic diagnostics, and Cybertwin-based virtual infrastructure [1, 2, 3]. However, this integration substantially expands the hospital cybersecurity attack surface. Approximately 75% of infusion pumps carry known unpatched vulnerabilities, healthcare data breaches now cost an average of $10 million per incident, and 276.78 million patient records were compromised in 2024 alone a 26% year-on-year increase. Attack consequences range from device hijacking and service disruption to data tampering that directly corrupts diagnostic outputs, making conventional reactive security architectures inadequate for complex, heterogeneous IoMT environments.

While prior work has addressed individual dimensions of this problem AI-driven intrusion detection for 6G [31, 32], Zero Trust Architecture for healthcare [4], blockchain-based IoT authentication [36, 37], and protocol-level encryption [6, 7] no existing study integrates these defences into a unified, simulation-validated framework aligned with a structured defensive knowledge base for hospital IoMT networks. This paper addresses that gap by proposing a four-phase cybersecurity framework for 6G-enabled IoMT hospital networks, implemented in MATLAB across a 44-device hospital simulation spanning seven device categories. The framework covers: STRIDE-based threat modelling and composite attack surface quantification (Phase

1); criticality-stratified Zero Trust policies, multi-protocol encryption (AES-256, TLS 1.3, DICOM-Secure, WPA3, IPSec), and tiered authentication (Phase 2); hybrid signature-anomaly intrusion detection evaluated against five attack classes (Phase3); and MITRE D3FEND-aligned defence optimisation through the proposed D3-MENCR data integrity mechanism (Phase 4). Results demonstrate a 36.8% reduction in permitted connections under Zero Trust enforcement, data integrity improvements from 75-85% to 83-93% with D3-MENCR, and an operationally acceptable D3FEND control overhead of approximately 110 ms.

The principal novelty and contributions of this work are summarised as follows:

This study proposes the first simulation-validated, end-to-end cybersecurity framework for 6G-enabled IoMT hospital networks a unified four-phase architecture integrating STRIDE-based threat modelling, criticality-stratified Zero Trust enforcement, hybrid intrusion detection, and MITRE D3FEND-aligned defence optimisation within a single, coherent system.

A novel composite attack surface scoring model is introduced to quantify device-level risk as a weighted function of connectivity, criticality, and exposure, enabling targeted and prioritised placement of security controls across heterogeneous hospital IoMT devices.

The framework applies differentiated Zero Trust policies, tiered authentication (Basic, Biometric, and MFA), and protocol-specific encryption (AES-256, TLS 1.3, DICOM-Secure, WPA3, IPSec) based on device criticality, achieving a 36.8% reduction in permitted network connections while preserving clinical operational requirements.

A hybrid signature-anomaly intrusion detection system is developed and evaluated against five attack classes, incorporating criticality-weighted detection probabilities and a sliding-window anomaly scoring mechanism tailored to the heterogeneous traffic patterns of hospital IoMT environments.

The proposed Data-Driven Defence Mechanism for Enhanced Network Control and Resilience (D3-MENCR), aligned with MITRE D3FEND controls, improves data integrity verification success rates from 75-85% to 83-93%, directly mitigating the risk of diagnostic data tampering in 6G-IoMT hospital deployments with an operationally acceptable overhead of approximately 110 ms.

The remainder of this paper is organised as follows. Section II reviews related work. Section III presents the methodology. Section IV discusses results. Section V concludes with limitations and future directions.

II. RELATED WORK

The convergence of 6G and IoMT in healthcare creates an expanded attack surface that demands multi-layered, adaptive cybersecurity frameworks. Prior work addressing this challenge can be broadly grouped into five areas: 6G network security, blockchain-based frameworks, Zero Trust and authentication, AI/ML based intrusion detection, and encryption and protocol standards.

Securing 6G infrastructure against cyber threats has been explored through AI-driven intrusion detection and prevention systems that leverage deep learning and optimisation algorithms to protect large-scale heterogeneous networks [31, 32]. Blockchain-integrated machine learning approaches have also been proposed for 6G wireless sensor networks, combining distributed trust with optimised anomaly scoring [32]. Further, intelligent breach detection systems have been tailored for 6G-enabled cyber-physical systems such as smart grids [35, 38]. While these works demonstrate strong detection performance, they target generic or industrial 6G environments and do not address the unique device heterogeneity, criticality stratification, or clinical data integrity demands of hospital IoMT networks. The 6G-IoMT convergence in healthcare, including Cybertwin-enabled virtual infrastructure, introduces additional deployment considerations that remain underexplored in security literature [1, 3].

Blockchain has been widely applied to address authentication and privacy challenges in IoT and IoMT systems. Smart contract-based frameworks have been proposed for forensic IoT authentication [36] and secure biometric MFA in drone-assisted IoT environments [37], while federated learning combined with blockchain has been used to enable privacy-preserving model training across IoMT devices [23, 27]. Secure cloud-based data auditing for IoT further complements these approaches by ensuring tamper-evident access logs [24].

Collectively, these works affirm that distributed trust mechanisms are critical for healthcare data governance a direction acknowledged in this study's future work on blockchain-based key management.

More recent works reinforce this direction: Kumar et al. proposed a blockchain-assisted authentication framework for electronic health records, demonstrating superior communication and computational efficiency [41]; the same group further developed a smart contract-based robotic surgery authentication system over 6G-Tactile Internet, demonstrating the feasibility of blockchain-secured healthcare operations in next-generation networks [42]; a multi-factor authentication framework for IoT environments using cloud computing further strengthens the case for layered identity verification in resource-constrained medical settings [43]; and a dedicated study on IoT-based cardiovascular health monitoring demonstrates how machine learning and AI techniques can secure real-time physiological data collection an approach directly relevant to the clinical device security goals of the present framework [44].

Zero Trust Architecture (ZTA) has been proposed for health information systems to enforce continuous authentication and restrict lateral movement [4]. Conference-level works have further examined multi-factor authentication and dynamic access control for IoT healthcare networks [33, 34, 39, 40]. HIPAA compliance frameworks and data privacy governance models reinforce the regulatory necessity of such structured access policies [14, 19]. The present framework operationalises ZTA across 44 simulated hospital devices, achieving a 36.8% reduction in permitted connections and iteratively refining policies based on simulated attack outcomes.

A growing body of work applies machine learning to IoMT intrusion detection. Deep reinforcement learning-based IDS designs [15], ML classifiers addressing class imbalance in medical traffic [16], fuzzy logic-based port-scan detection [28], and surveys of ML algorithms for IoT security [21, 26] collectively establish the feasibility of intelligent detection in resource-constrained medical environments. Federated learning-based detection approaches further enable privacy-preserving collaborative training across distributed IoMT nodes [27]. Adversarial robustness of AI models particularly against data poisoning is an additional concern in clinical AI deployments [17]. The IDS in this work adopts a hybrid signature-anomaly approach with criticality-weighted detection, evaluated against five attack types including device takeover, DoS, data theft, credential stuffing, and ransomware.

The cryptographic foundations of IoMT security encompass both established standards and evolving protocol requirements. AES remains the benchmark for symmetric encryption, with cryptanalytic studies informing deployment decisions [5, 9]. WPA3 offers significant improvements over predecessor wireless protocols for hospital wireless environments [6, 7]. DICOM-Secure governs the privacy and integrity of medical imaging data [10, 11, 20], while IPSec provides authenticated tunnelling for network infrastructure [12]. In this framework, encryption protocols are assigned by device type and criticality AES-256 for Critical-IoMT, DICOM-Secure for imaging devices, WPA3 for patient wearables and staff devices with measured overhead values confirming operational feasibility. The D3-MENCR integrity mechanism further improves data integrity check success rates from 75-85% to 83-93%, directly mitigating the risks of data tampering highlighted in healthcare data security literature [18, 20].

In summary, while prior work addresses individual dimensions of 6G-IoMT security in isolation, no existing study integrates STRIDE-based threat modelling, criticality-stratified encryption and authentication, multi-attack simulation, and MITRE D3FEND-aligned defence optimisation within a unified, simulation-validated hospital network framework. The present work addresses this gap.

Table 1 presents a comparative summary of the proposed framework against seven recent relevant schemes across key security dimensions.

Scheme	Year	Domain	Threat Modelling	Zero Trust	Encryption Standard	Intrusion Detection	Data Integrity	MITRE D3FEND Alignment	Simulation / Validation	6G-IoMT Specific
Kaur & Gupta [1]	2025	IoMT / 6G	No	No	Not specified	Explainable AI-based	No	No	Analytical	Yes
Edo et al. [4]	2024	Health IT	No	Yes	Not specified	No	No	No	Conceptual	No
Shaikh et al. [15]	2025	IoMT	No	No	Not specified	Deep Reinforcement Learning	No	No	Simulation	No
Kulshrestha & Kumar [16]	2024	IoMT	No	No	Not specified	ML Classifier	No	No	Experimental	No
Chinnasamy et al. [31]	2025	6G Networks	No	No	Not specified	AI-Driven IDS/IPS	No	No	Simulation	Partial
Chinnasamy et al. [32]	2024	6G WSN	No	No	Blockchain-based	ML-Optimised Anomaly	No	No	Simulation	Partial
Khan et al. [23]	2025	IoMT	No	No	Federated + Blockchain	Federated Learning IDS	Partial	No	Experimental	No
Kumar et al. [45]	2025	6G/IoMT Healthcare	No	No	Smart Contract (Blockchain)	No	Partial	No	Analytical	Yes
Proposed Framework	**2025**	**6G-IoMT Hospital**	**Yes (STRIDE)**	**Yes (36.8% reduction)**	**AES-256, TLS 1.3, WPA3, DICOM-Secure, IPSec**	**Hybrid Signature Anomaly**	**Yes (D3-MENCR, 83–93%)**	**Yes**	**MATLAB Simulation (44 devices)**	**Yes**

Table 1: Comparative Analysis of the Proposed Framework Against Recent Related Work

As evident from Table 1, the proposed framework is the only scheme that simultaneously integrates STRIDE-based threat modelling, criticality-stratified Zero Trust enforcement, multi-protocol encryption, hybrid intrusion detection, formal data integrity assurance via D3-MENCR, and MITRE D3FEND alignment within a unified, simulation-validated architecture specifically designed for 6G-enabled IoMT hospital networks.

III. METHODOLOGY

It is a description of the entire process undertaken in developing, building, modelling, and testing the cybersecurity framework of a 6G-enabled IoMT hospital network. This is because the whole simulation was carried out quite well in MATLAB which allowed a controlled environment to simulate complex interactions and quantify security gains. An overview of this methodological framework is depicted in (Fig 1). It is organized in four phases which are: Threat Analysis (Phase 1), Security Control Execution (Phase 2), Attack Simulation (Phase 3), Defense Optimization (Phase 4).

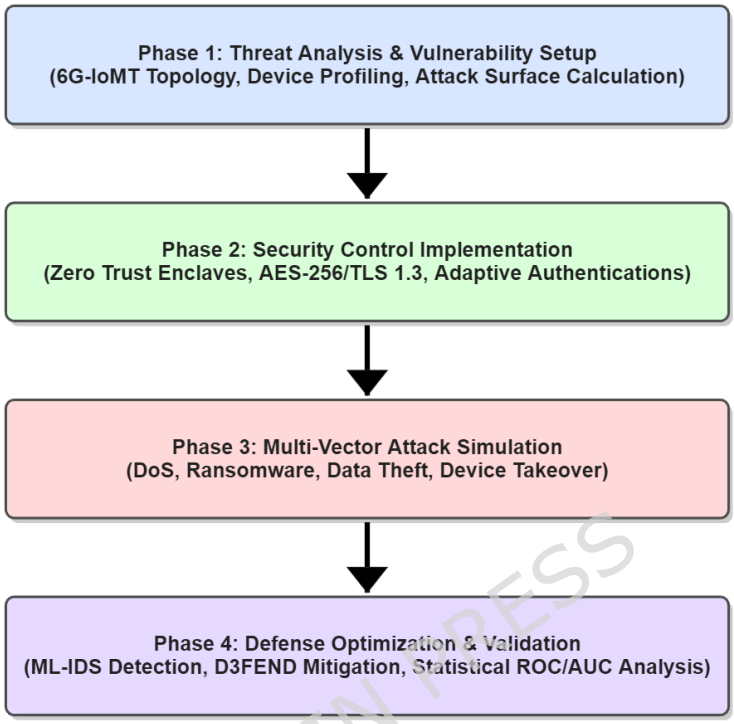

Fig. 1: Overall Cybersecurity Framework Methodology Flowchart

The simulation is built on a set of explicit assumptions to ensure transparency and reproducibility. Regarding the traffic model, network traffic is represented as a static communication matrix of 1,892 possible device-to-device connections, with bandwidth fixed at 100 Mbps under normal conditions and DoS-induced degradation modelled as a deterministic drop to 10 Mbps; per-path latency is computed as a cumulative hop sum, and encryption overhead is derived from fixed per-MB processing constants representative of each protocol. Regarding device behaviour, all 44 devices are assumed to operate correctly under normal conditions with no hardware faults or unplanned downtime, criticality classifications are assigned statically based on operational role, and authentication mechanisms are assumed to be perfectly enforced without implementation flaws. Regarding attacker capabilities, attackers are assumed to be informed adversaries with prior knowledge of the network topology, exploiting only known vulnerability classes (default credentials, API abuse, UDP amplification, and password spraying); attacks are single-vector and sequential, and lateral movement is constrained to permitted communication paths. Regarding trust, a strict Zero Trust posture is assumed throughout, the IDS and SIEM components are treated as trusted and uncompromised, and the D3-MENCR mechanism is modelled mathematically as a performance offset representing hash-based verification and cryptographic integrity protection aligned with MITRE D3FEND controls.

Adversarial Model

To formally characterise the threat environment, the adversary $\mathcal{A}$ in this framework is defined along four dimensions: position, capability, objective, and strategy.

Position. The adversary is modelled as a hybrid threat capable of operating both as an external attacker who has completed prior network reconnaissance and as a malicious insider with legitimate but limited network access. This reflects the realistic threat landscape of hospital IoMT environments, where both external intrusion and insider misuse are documented attack vectors.

Capability. $\mathcal{A}$ is assumed to be a computationally bounded probabilistic polynomial-time (PPT) adversary. Specifically: (i) $\mathcal{A}$ has full knowledge of the network topology, device roles, and IP addressing scheme, representing a worst-case Dolev-Yao attacker with respect to network structure; (ii) $\mathcal{A}$ can intercept, replay, and inject network traffic on any communication channel it has access to; (iii) $\mathcal{A}$ can exploit known vulnerability classes including default credentials, unencrypted communications, outdated firmware, insecure APIs, and wireless eavesdropping as identified in the vulnerability assessment; (iv) $\mathcal{A}$ cannot break cryptographic primitives specifically, AES-256, SHA-256, and the Diffie-Hellman key exchange under standard hardness assumptions (IND-CPA security of AES-256, collision resistance of SHA-256, and the DDH assumption); and (v) $\mathcal{A}$ cannot compromise the IDS sensor or SIEM system directly.

Objective. The adversary's goals, mapped to the STRIDE threat categories applied in Phase 1, are: unauthorised access to critical devices (Spoofing); corruption or manipulation of medical data (Tampering); exfiltration of sensitive patient records (Information Disclosure); disruption of clinical services (Denial of Service); and escalation of privileges within the network (Elevation of Privilege).

Strategy. $\mathcal{A}$ operates through single-vector, sequential attacks targeting one entry point at a time. The five attack strategies simulated in Phase 3 are: device takeover via default credential exploitation; data theft via API abuse; DoS via UDP amplification; credential stuffing via password spraying; and ransomware via rapid encryption. Lateral movement following an initial compromise is constrained to permitted communication paths defined by the Zero Trust policy matrix, as $\mathcal{A}$ cannot bypass enforced Zero Trust segmentation rules without triggering IDS detection. Multi-vector and coordinated simultaneous attacks are outside the scope of this work and are identified as a direction for future investigation.

A. Threat Analysis (Phase 1)

The first step of security framework was a thorough threats analysis to detect, categorise, and evaluate the risks that might emerge in the exemplifying 6G-IoMT hospital network.

1. **Architecture Design:** This work is carried out on the simulated 6G-IoMT hospital network with 44 devices in the 192.168.1.x network, which demonstrates a realistic hospital network (Fig 2). The layout consists of 7 Critical-IoMT ventilators/monitors, 7 Patient-IoMT wearables/beds, 5 Imaging-IoMT scanners, 2 Surgical-IoMT, 11 Network-Infra components, 6 Staff Devices, and 6 Servers that together represent one hospital wing approximated to a 3,850 endpoint mid-sized smart hospital at a scale of 1/88th. The most usable and least controversial subnet is 24 (255.255.255.0), which permits a maximum of 254 assignable addresses and would provide for future growth with minimal broadcast latency. In such a design, all intra-zone (81%) and necessary cross-zone (21%) traffic was permitted (such as 1,532 of 1,892 possible connections) on the basis of the least-privilege principle, but 360 connections (19%) were denied. This distribution conforms to split of categories reported by Voerner and scales linearly with respect to the estimated total endpoints.

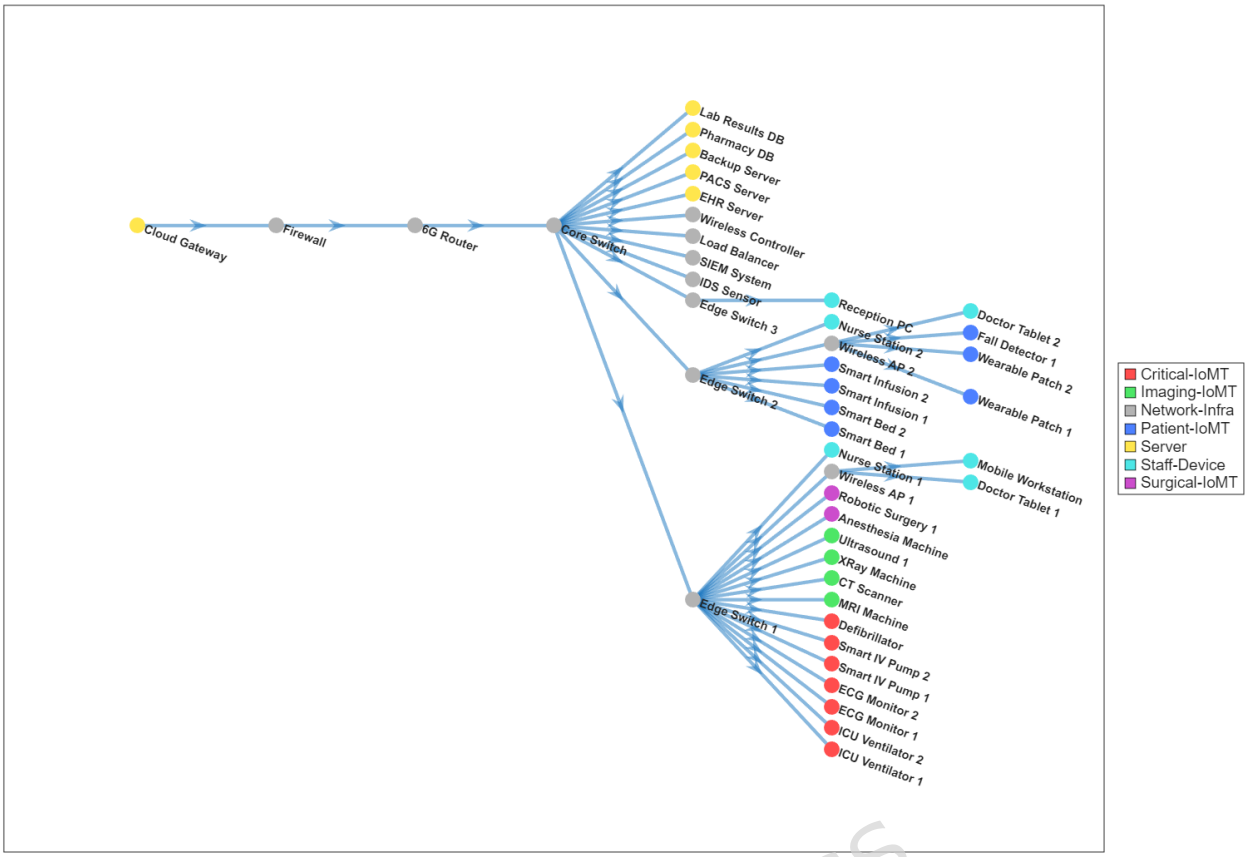

Fig. 2: 6G-IoMT Hospital Network Topology

The medical equipment is divided into a few types depending on its purpose and the importance of its functioning in the health-care environment:

- Critical-IoMT: Devices that are directly associated with the life-support or critical care of a patient (e.g., ICU Ventilator, ECG Monitor, Smart IV Pump, and Defibrillator).
- Patient-IoMT: Devices that continuously monitor the patients (e.g., Wearable Patch, Smart Bed, Fall Detector, Smart Infusion).
- Imaging-IoMT: Diagnostic and Imaging equipment (e.g., CT Scanner, XRay Machine, Magnetic resonance imaging (MRI) Machine, Ultrasound).
- Surgical-IoMT: The devices that are involved into the processes of surgical practice (e.g., Anesthesia Machine, Robotic Surgery).
- Network-Infra: The core elements of the network (e.g., 6G Router, Core Switch, Edge Switches, Firewall, IDS Sensor, SIEM System, Load Balancer, Wireless APs, Wireless Controller).
- Server: Database/computing units (e.g., EHR Server, PACS Server, Backup Server, Cloud Gateway, Pharmacy DB, Lab Results DB).
- Staff-Device: End devices deployed by the medical and administrative staff members (e.g., Doctor Tablet, Nurse Station, Reception PC, Mobile workstation).

Strict network segmentation was also achieved by using granular communication matrix. Blocked communications (19%) were based on either a specific policy e.g. disallowing direct communication between critical devices to staff devices, or patient monitors to imaging equipment. The (Fig 3) demonstrates traffic changes throughout simulation, (Algorithm 1) is explanatory about the logic behind setting such rules.

Algorithm 1 IoMT Network Connectivity Matrix Construction

Require: $totalDevices$, device types
Ensure: $connectivityMatrix$: Binary matrix of allowed communications

Initialize $connectivityMatrix \leftarrow \mathbf{0}_{totalDevices \times totalDevices}$
Define communication rules for device types:
  Critical-IoMT $\leftrightarrow$ {Critical, Patient, Surgical, Server, Network}
  Patient-IoMT $\leftrightarrow$ {Critical, Patient, Server, Network}
  Imaging-IoMT $\leftrightarrow$ {Server, Network, Staff}
  Others follow similar patterns with Server/Network having full access
for each device pair (i, j) where $i \neq j$ **do**
  if communication allowed between $deviceType(i)$ and $deviceType(j)$ **then**
    $connectivityMatrix(i, j) \leftarrow 1$
  end if
end for
return $connectivityMatrix$ =0

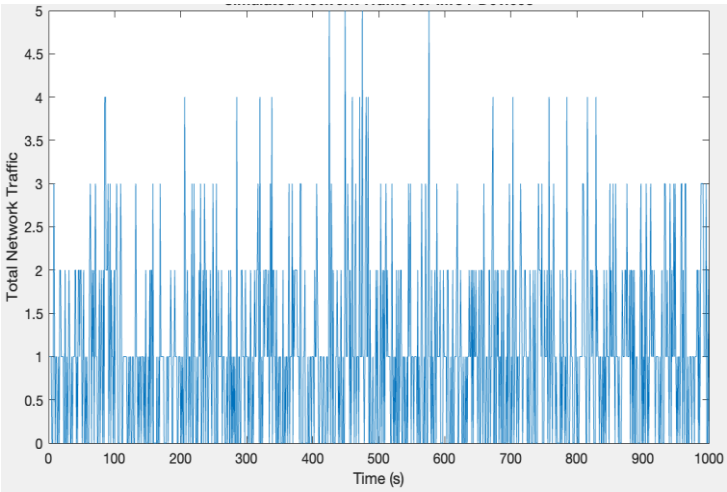

Fig. 3: Simulated Network Traffic for IoMT

2. **Asset Classification:** The asset classification process implied that all the devices within the hospital network went through a process in which they each received a quality rating in accordance with their degree of criticality. This evaluation was done by considering the operational role of the device in the system and the effect of its compromise. Devices were classified into 4 degree of Criticality; Critical, High, Medium, and Low. An example of the Critical category was ICU Ventilators and Smart IV Pumps, which are vital directly towards keeping a patient in good health since their failure would lead to devastating effects. Other Appliances like Anaesthesia Machines and Robotic Surgery System were categorised under High since it plays an important role in surgeries. Such devices as MRI Machines and Doctor Tablets were ranked as of medium criticality as none of them can present imminent life-threatening danger in case they fail. The infrastructure equipment like 6G Routers, and Edge Switches had been classified as Low as it is the support equipment of the network but still has importance in receiving and sending the data and grouping or connecting of data platforms.

This set of categories is the basis on which resources and priorities of cybersecurity strategies are determined. It guarantees a more powerful and closer protection of more critical devices and thus diminishes the chances of high-level cyberattacks. It was established that a considerable amount of devices, which is around a half of the total number, belong to Critical or High categories. This observation highlights the importance of abandoning a lax security strategy in the IoMT background of the hospital. The detailed breakdown of device types and the level of its criticality is described in (Table 2).

Criticality Level	Number of Devices	Example Devices from simulation
Critical	14	ICU Ventilator, ECG Monitor, Smart IV Pump, Defibrillator, Wearable Patch, Smart Bed, Fall Detector.
High	8	Anaesthesia Machine, Robotic Surgery, EHR Server, Passover, Backup Server, Cloud Gateway.
Medium	10	MRI Machine, CT Scanner, Xray Machine, Ultrasound, Doctor Tablet, Nurse Station.
Low	12	6G Router, Core Switch, Edge Switch, Firewall, IDS Sensor, SIEM System.

Table 2: Device Criticality Distribution

3. **STRIDE Threat Modelling:** STRIDE threat model (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) was used to find appropriate security threats

to each device type in a systematic manner. It included the examination of the way in which each category of threats may occur in the real conditions of IoMT devices. As an example, the devices of the class of Critical-IoMT were recognized to be susceptible to the attacks of Unauthorized Critical-IoMT access (Spoofing), Data manipulation in Critical-IoMT (Tampering), Critical-IoMT service disruption (Denial of Service) and Privilege escalation in Critical-IoMT (Elevation of Privilege)(Fig 4). This systematic process was useful to identify fully the prospective attack vectors in an ecosystem of a variety of devices.

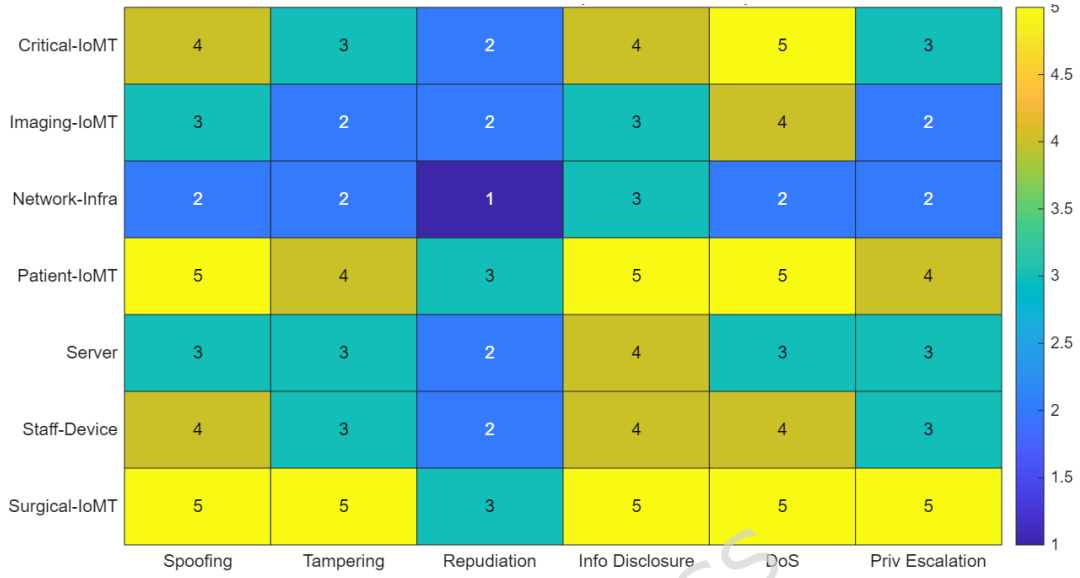

Fig. 4: STRIDE Threat Severity Matrix by Device Category (1=Low, 5=Critical)

4. **Vulnerability Assessment:** A close look at the vulnerability analysis was performed to establish major vulnerabilities that come with each of the devices. The evaluation has also shown that the 'Default Credentials', 'Unencrypted Communications', 'Outdated Firmware', and 'Wireless Eavesdropping' were prevalent in the 'Critical-IoMT', 'Imaging-IoMT', 'Patient-IoMT' and 'Surgical-IoMT' devices(Fig 5). The similarities between types of vulnerabilities were threefold: the vulnerabilities of 'Network-Infra', 'Server' and of course, the vulnerabilities of 'Staff-Device' which included 'Unencrypted Communications', 'Insecure APIs' and 'Physical Tampering'. Under the assessment, it was observed that the most prevalent vulnerability on the network was the one that was connected with the label of Unencrypted Communications. The most risky device types were found to be the top three, viz., Patient-IoMT, Server, and Critical-IoMT. The overview of the identified vulnerabilities according to the type of devices is shown in (Table 3).

Device Type	Vulnerability Count	Common Vulnerabilities
Critical-IoMT	4	Default Credentials, Unencrypted Communications, Outdated Firmware, Wireless Eavesdropping
Imaging-IoMT	4	Default Credentials, Unencrypted Communications, Outdated Firmware, Wireless Eavesdropping
Network-Infra	3	Unencrypted Communications, Insecure APIs, Physical Tampering
Patient-IoMT	4	Default Credentials, Unencrypted Communications, Outdated Firmware, Wireless Eavesdropping
Server	3	Unencrypted Communications, Insecure APIs, Physical Tampering
Staff-Device	3	Unencrypted Communications, Insecure APIs, Physical Tampering

Table 3: Summary of Vulnerabilities by Device Type

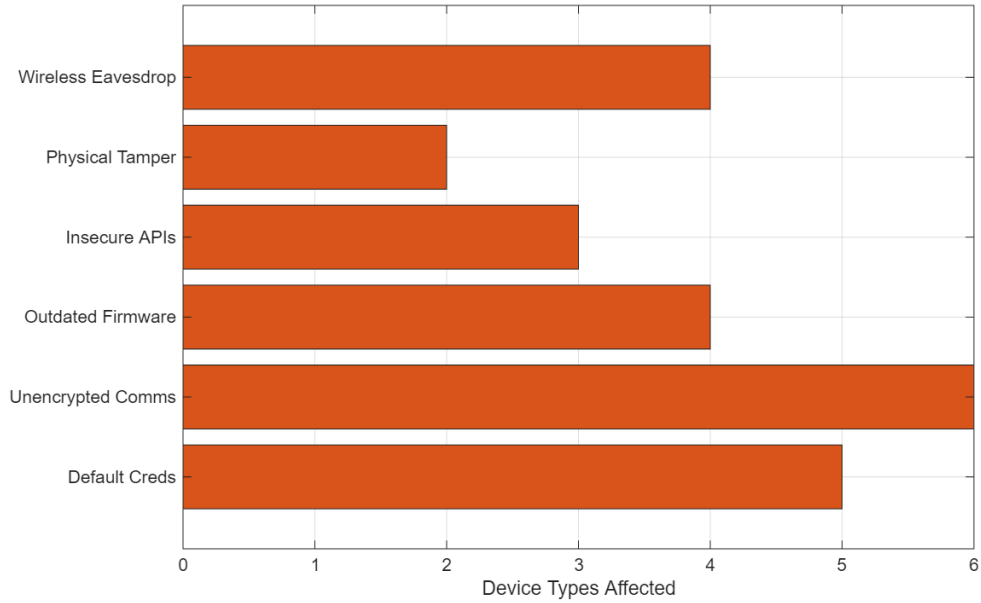

Fig. 5: Vulnerability Assessment - Device Types Affected per Vulnerability Class

5. **Attack Surface Analysis**: The attack surface was analysed and visualized to identify potential entry points in the network. This involved a composite score that quantified the risk of each device based on its connectivity, criticality, and exposure. This formalization provides a clear and quantitative method for understanding risk across the network. The composite attack surface score for a given device (d) is calculated as a weighted sum of these three components:

$$S_{AS}(d) = w_{conn} \cdot S_{conn}(d) + w_{crit} \cdot S_{crit}(d) + w_{exp} \cdot S_{exp}(d) \rightarrow Eq.1$$

In this model, Sconn (d) is the connectivity score, Scrit (d) is the criticality score, and Sexp (d) is the exposure score, all ranging from 0 to 1. The simulation used weights of Wconn =0.4, Wcrit =0.3, and Wexp =0.3 to reflect the relative importance of each factor. The resulting scores are visualized in a heatmap, as shown in (Fig 6), which helps clarify which devices and communication paths pose the greatest risk.

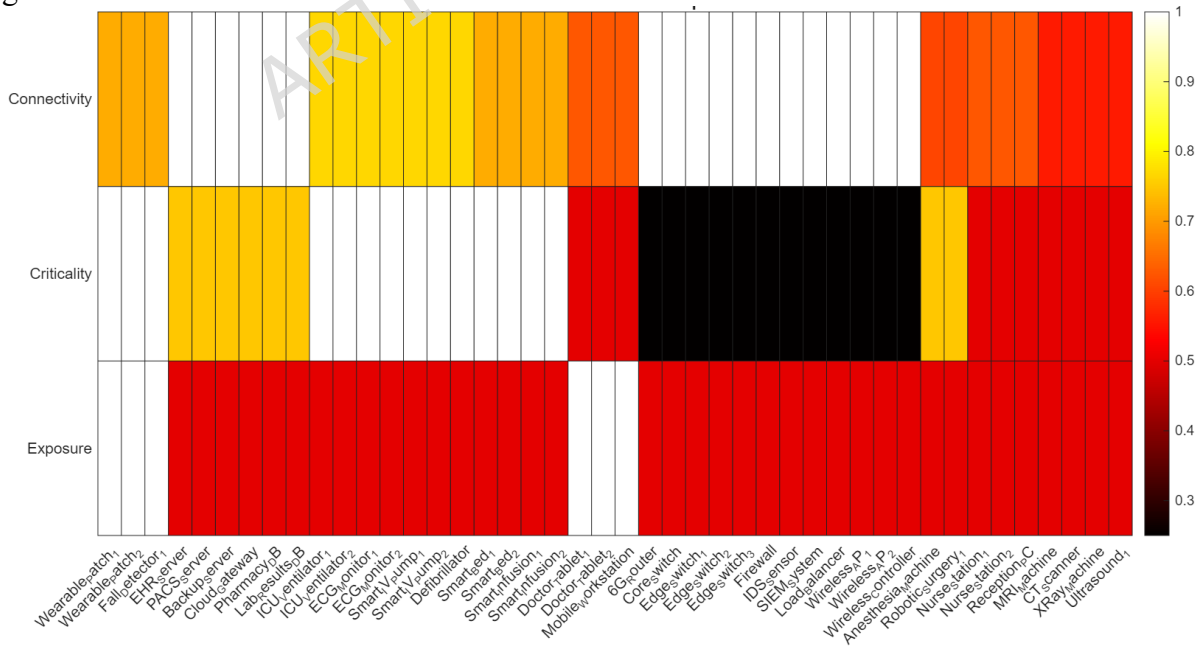

Fig. 6: Device Attack Surface Components

B. Security Control Implementation (Phase 2)

In response to the threat analysis, multi-tiered security model was deployed in the simulated environment, to contain discovered threats.

1. **Zero Trust Policies:** Zero Trust policies were implemented based on the principle of "never trust, always verify". This approach requires continuous verification of the trustworthiness of users and devices for every access request. The implementation of these policies resulted in a significant reduction in permitted connections, decreasing the attack surface by 36.8%. This reduction can be quantified using the following formula:

$$\textbf{Reduction(\%)} = \frac{C_{allowed_{initial}} - C_{allowed\_ZT}}{C_{allowed\_initial}} \times 100 \rightarrow Eq.2$$

Here, Callowed_initial represents the initial number of allowed connections and Callowed_ZT is the number of allowed connections after the Zero Trust policy was enforced. In our simulation, the initial number of allowed connections was 1,532 (out of 1,892 total possible connections) , while the number of blocked connections increased from 360 to 968 after the Zero Trust policies were applied. This reduction in permitted connections directly minimizes the potential for lateral movement within the network.

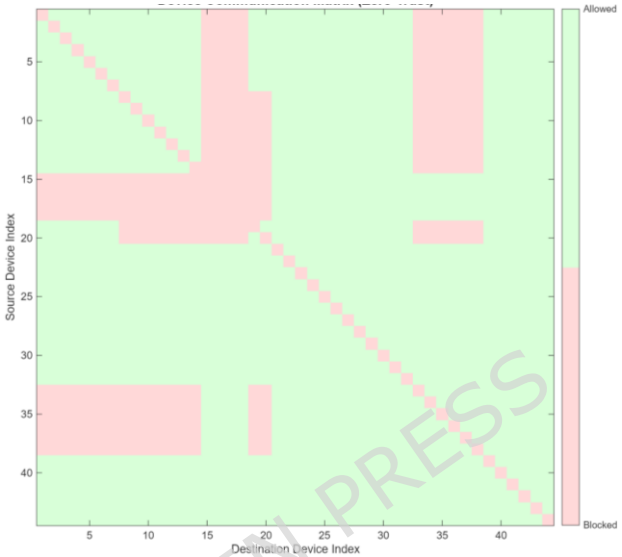

Fig. 7: Device Communication Matrix (Zero Trust) - Green = Allowed, Pink = Blocked

2. **Enhanced Authentication:** Devices were allocated some enhanced authentication mechanisms depending on the importance and the role. The simulation defined authentication 3 levels as Basic, Biometric and Multi-Factor Authentication (MFA). Critical-IoMT (e.g., ICU Ventilators, ECG Monitors, Smart IV Pumps) devices were given 'Biometric Authentication', and high-value servers (e.g., EHR Server, PACS Server, Backup Server) and surgical IoMT devices had the mandate of utilizing 'MFA'. The network infrastructure and some of the staff devices were also put in the 'Basic' authentication. This tactical placement can be represented in the chart of the Authentication Distribution (Fig 8).

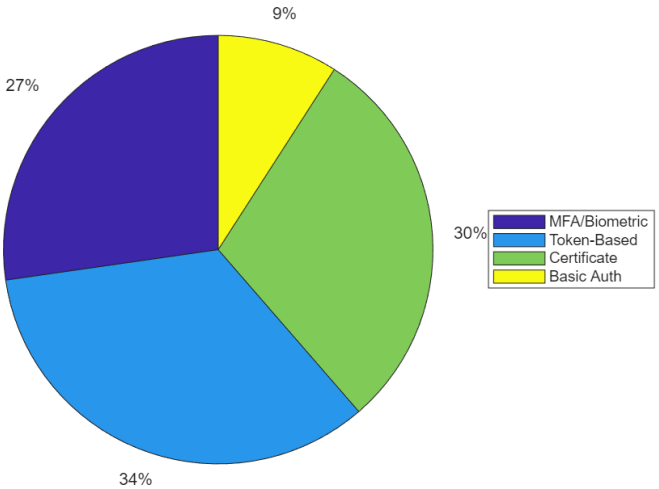

Fig. 8: Authentication Distribution

3. **Network Segmentation:** A logical subdivision of the network into separate security domains was provided to isolate important resources and regulate communication flows. The devices were spread through five major sets of security domains, namely, Critical-Care, Patient-Monitoring, Clinical-

Imaging, Staff-Network, and Infrastructure (Fig 9). This will make devices within one zone to communicate with devices in another zone with limited capabilities and limit the damage that can be caused by a breach.

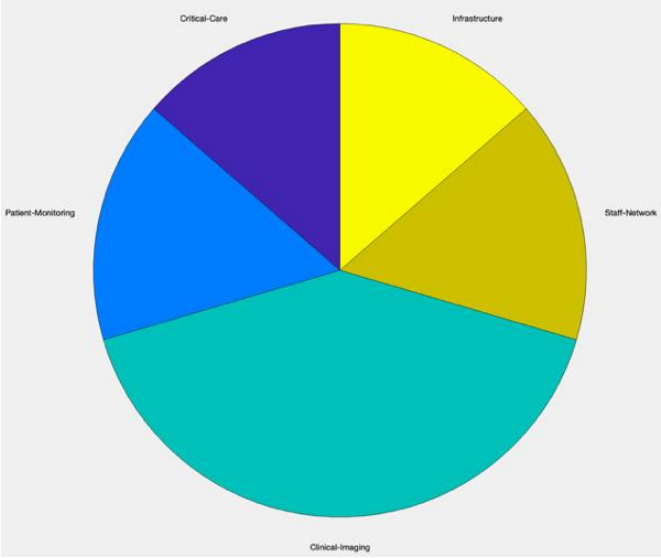

Fig. 9: Device Distribution Across Security Zones

4. **Encryption Standards:** The overall strategy was to adopt the strategy of encryption where particular encryption protocol would be applied to different types of devices according to sensitivity of data and communication need(Fig 10).
   - AES-256: Critical-IoMT (e.g., ICU Ventilators, ECG Monitors, Smart IV Pumps, Defibrillator) may have critical data, and that is why AES-256 will be used on it to protect the most sensitive data.
   - WPA3: This is used in Patient-IoMT devices such as Wearable patient, fall detectors and Staff-Devices such as Doctor Tablet, Mobile workstation to have secure wireless communications.
   - TLS 1.3: Deployed to Smart Beds, Smart Infusion, Anesthesia Machines, and Robotic Surgery systems, Server devices EHR Server, PACS Server, Cloud Gateway, Pharmacy DB to protect data sent in between network tiers.
   - DICOM-Secure: Used on Imaging-IoMT devices (e.g., MRI Machine, CT Scanner, XRay Machine, Ultrasound) to securely store and transmit medical images.
   - IPSec: Will be utilized throughout all of the Network-Infra devices (e.g., 6G Router, Core Switch, Edge Switches, Firewall, IDS Sensor, SIEM System, Load Balancer, Wireless APs, Wireless Controller) such that secure tunnels provide a secure transport of network traffic.

The pie chart of the distribution of these encryption standards is in (Fig 11) Encryption Standards Distribution. Full-scale network encryption was provided on the simulated environment. The underlying logic used to assign appropriate encryption protocols to each medical device based on its type and connection characteristics is outlined in (Algorithm 2).

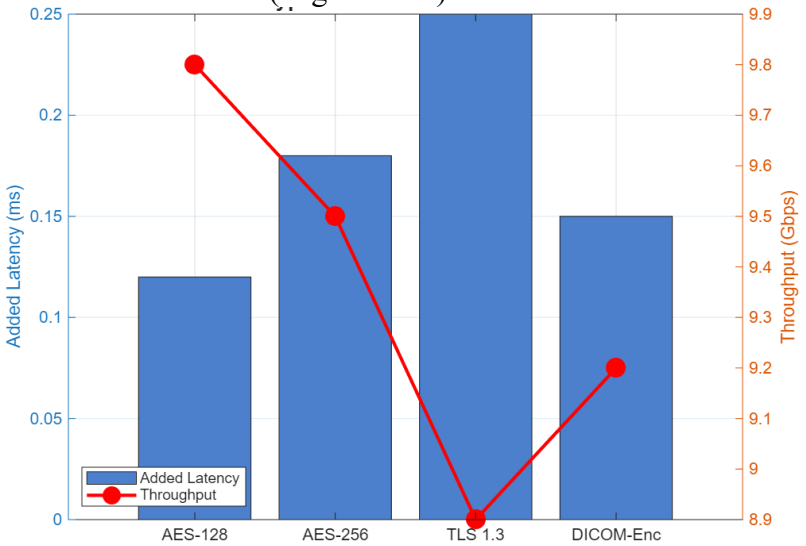

Fig. 10: Encryption Protocol Performance Overhead (Added Latency and Throughput)

Theorem 1 (Session Key Indistinguishability): - Let $\mathbb{G}$ be a cyclic group of prime order q with generator g, and let p be a large safe prime. For any two communicating entities a device *d* and a server *s* in the proposed 6G-IoMT framework, a session key *SK* is established as:

SK = H (, ID_d, ID_s, T)

where $a \in^R \mathbb{Z}\_q$ and $b \in^R \mathbb{Z}\_q$ are independent uniformly random secret exponents chosen by *d* and *s* respectively, *ID_d* and *ID_s* are the unique cryptographic identifiers of the communicating parties, *T* is a timestamp-based nonce, and *H(·)* is a collision-resistant cryptographic hash function (SHA-256) modelled as a random oracle. Then, SK is semantically secure that is, computationally indistinguishable from a uniformly random string against any probabilistic polynomial-time (PPT) adversary, under the Decisional Diffie-Hellman (DDH) assumption in $\mathbb{G}$.

Proof: - Suppose, for contradiction, that there exists a PPT adversary $\mathcal{A}$ that distinguishes SK from a random string with non-negligible advantage ε > 0. Since H(·) is modelled as a random oracle, the only information $\mathcal{A}$ can exploit to distinguish SK is the Diffie-Hellman value g^{ab} mod p. Consequently, $\mathcal{A}$ can be used to construct a PPT distinguisher $\mathcal{D}$ for the DDH problem in $\mathbb{G}$ as follows: given a DDH challenge triple (g^a, g^b, g^c), $\mathcal{D}$ computes H(g^c, ID_d, ID_s, T) and runs $\mathcal{A}$ on this value. If $g^c = g^{ab}$, then $\mathcal{D}$ has simulated a valid SK; otherwise it has simulated a random oracle output. The advantage of $\mathcal{D}$ in solving DDH is therefore at least ε/2, contradicting the DDH hardness assumption in $\mathbb{G}$. Hence no such $\mathcal{A}$ exists and SK is computationally indistinguishable from a uniform random string.

Furthermore, the inclusion of the timestamp nonce T in the hash input guarantees *session freshness*: any replayed session key from a prior session will carry an expired T and will thus map to a different, independent hash output under H(·), rendering replay attacks computationally infeasible. Finally, the binding of ID_d and ID_s within the hash input ensures entity binding, preventing key misdirection attacks in which a valid session key established with one party is presented as valid for another.

Therefore, every session key SK established within the proposed framework satisfies semantic security, session freshness, and entity binding simultaneously.

Algorithm 2 Encryption Protocol Assignment

Require: Device list, network topology, encryption standards
Ensure: Device encryption assignments

```
for each device d in hospital network do
    if device d has wireless connectivity then
        Assign wireless encryption protocol (WPA3/AES-256)
    else
        Select protocol based on device type:
            Critical-IoMT → AES-256
            Patient-IoMT → TLS-1.3
            Imaging-IoMT → DICOM-Secure
            Network-Infra → IPSec
    end if
    Configure encryption/decryption functions
end for
return Encryption configuration matrix =0
```

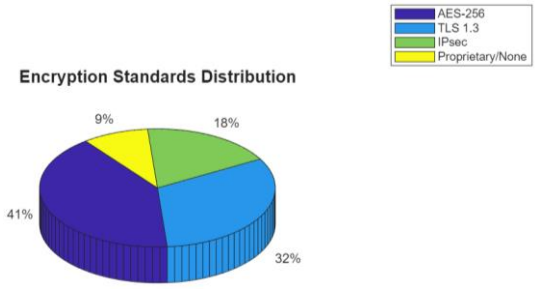

Fig.11: Encryption Standards Distribution

5. **Real Medical Data Transmission Simulation:** Seven scenarios that emulate real-life transmissions of medical data were run in order to measure the performance and security overhead of the controls implemented. In such a simulation, each patient data file (ECG, CT, MRI, X-ray, etc.) available in the working folder produces a scenario of possible data transmission. The code searches for files having names of ecg, ct, mri, xray (as well as .csv ECG data) and defines a file Database entry on it. Every record brings up a distinct transmission scenario: it contains a source device of a file, destination server, a kind of file, and the size. Therefore, in terms of augmenting uploaded image/data files autonomously multiplying the number of communication situations takes place. As an example, when having them

have ten CT images and five ECG logs, the code will simulate at least 15 different transmissions. When trying to create imaging files, an additional doctor access event is to take place, making every CT/MRI/XRay file generate two sets of events: one into PACS and the other one into the doctor device. The status/size of file-type modifies the scenario (source/destination and description) of file. Examples are the sending of MRI and CT images by the MRI/CT machine to the PACS server and the sending of data of an ECG display by the ECG monitor to the EHR server. The file size in megabytes (part of computing transfer time and latency) is also configured with these types. In short, the code employs files count in creating unique transmission clusters and files type in calculating the content and size of each transmission. The simulation followed then to calculate end-to-end latency and bandwidth per scenario depending on the file size. The pseudocode used to implement this simulation logic is presented in (Algorithm 3).

Algorithm 3 Medical Data Communication Simulation

Require: Medical file database, device list
Ensure: Communication simulation scenarios
Display detected medical files with metadata
Initialize communication scenarios $S \leftarrow \emptyset$
for each medical file f in database **do**
  Create base communication scenario from file metadata
  if file type is medical imaging (CT/MRI/X-Ray) **then**
    Add imaging-specific scenario: Doctor $\rightarrow$ PACS Server
  end if
  Add scenario to S
end for
for each scenario $s \in S$ **do**
  Extract: source, destination, data type, file size
  Execute simulated communication
  Log transmission parameters and results
end for
return Communication scenarios S =0

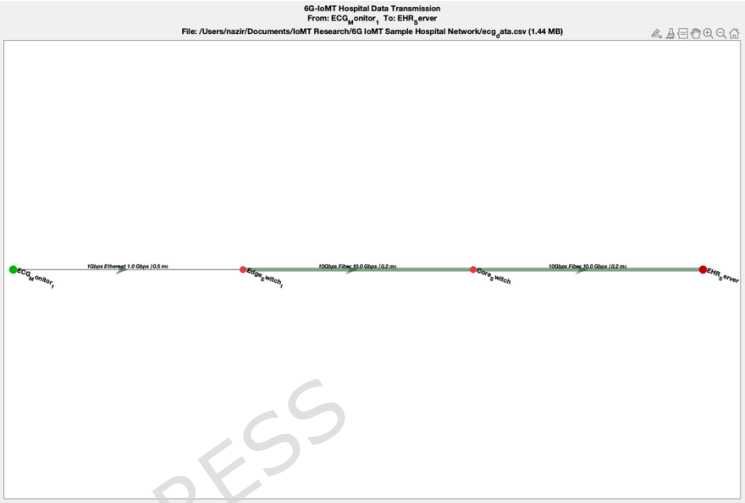

Fig. 12: 6G-IoMT Hospital Data Transmission - ECG Data

In both cases, the simulation was logged on the communication path (number of hops), the total path latency, the bottlenecked bandwidth, transfer time theoretical, MD5 checksum, encryption/decryption overhead, and the time the total transfer used. (Table 4) gives a brief overview of these scenarios of data transmission and their performance parameters. representative of these transmissions, being depictions of the paths of communication and the related latencies, for one data transmission presented in (Fig 12).

Scenario	Source Device	Destination Server	Data Type	File Size (MB)	Encryption Protocol	Encryption Overhead (ms)	Total Time (ms)
1.	ECG Monitor 1	EHR Server	ECG	1.436	AES-256	90.67	91.58
2.	CT Scanner	PACS Server	CT	0.090	DICOM-Secure	13.12	13.62
3.	Doctor Tablet 1	PACS Server	CT	0.090	WPA3	10.73	13.53
4.	MRI Machine	PACS Server	MRI	0.027	DICOM-Secure	3.51	4.01
5.	Doctor Tablet 1	PACS Server	MRI	0.027	WPA3	6.27	9.07
6.	Xray Machine	PACS Server	XRAY	0.094	DICOM-Secure	10.98	11.78
7.	Doctor Tablet 1	PACS Server	XRAY	0.094	WPA3	11.20	14.00

Table 4: Simulated Data Transmission Scenarios and Performance

C. Attack Simulation (Phase 3)

Several realistic cyberattacks were staged in order to test the resilience of the network as well as effectiveness of the security controls put in place. Five attack scenarios were carried out are presented in (Table 5).

Attack Type	Target Device	Method	Devices Affected	Detected by IDS	Detection Time
Device Takeover	Smart IV Pump 1	Default Credentials	7	False	52.01
Data Theft	Pharmacy DB	API abuse	4	True	79.58
DoS	Doctor Tablet 1	UDP Amplification	1	True	3.75
Credential Stuffing	Reception PC	Password Spraying	1	True	17.40
Data Theft	Backup Server	API abuse	3	False	89.69

Table 5: Simulated Attack Scenarios

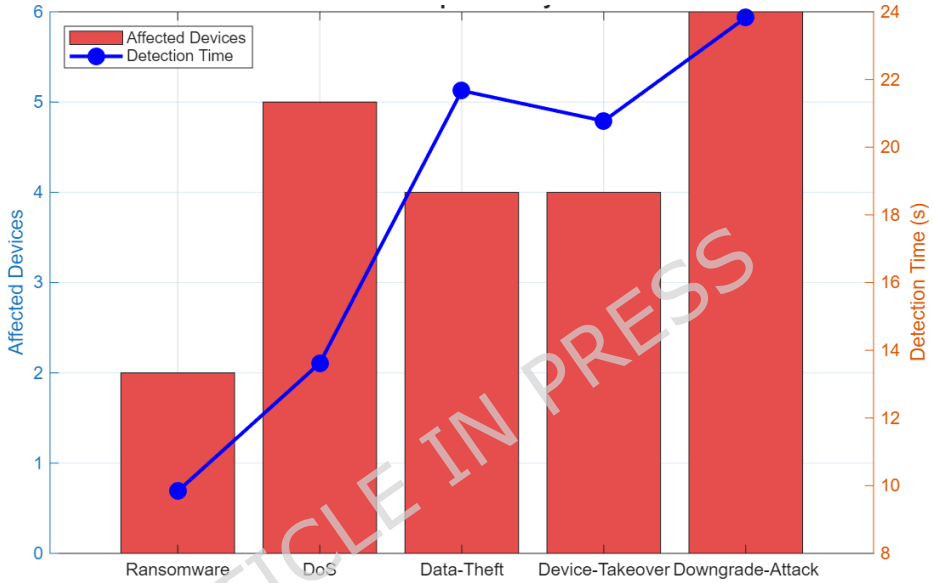

Fig. 13: Attack Impact Analysis Affected Devices and Detection Time per Attack Type

The logic used to generate these attack scenarios programmatically, including selection of attack types, target devices, and impact estimation, is shown in (Algorithm 4).

Algorithm 4 Attack Scenario Generation for IDS

Require: IoMT devices, security controls, scenario count
Ensure: Attack scenarios for testing
1: Categorize devices by type and vulnerability
2: Define attack types: {Ransomware, DoS, Data-Theft, Device-Takeover, Credential-Stuffing}
3: Map each attack type to targeting strategy
4: **for** $i = 1$ to $numScenarios$ **do**
5: Select random attack type and targeting function
6: Identify possible targets based on attack strategy
7: Choose target device and generate attack method
8: Assess potential impact on target
9: Store scenario: $\{type, target, method, impact\}$
10: **end for**
11: **return** Generated attack scenarios for IDS testing =0

1. **Attack Propagation Paths:** The graph of attack propagation by means of a compromised Smart_IV_Pump_2 depicts the possible propagation of an attack initiated by a compromised Smart_IV_Pump_2 (Fig 14). The red nodes are compromised devices, which indicates that the attack can intercept the edge switches and reach other vital devices and, possibly, core network infrastructure

and cloud gateway. This visualization highlights the inter-relationship of the IoMT world and the need to contain attacks at an attack starting point so that the impact is not far reaching.

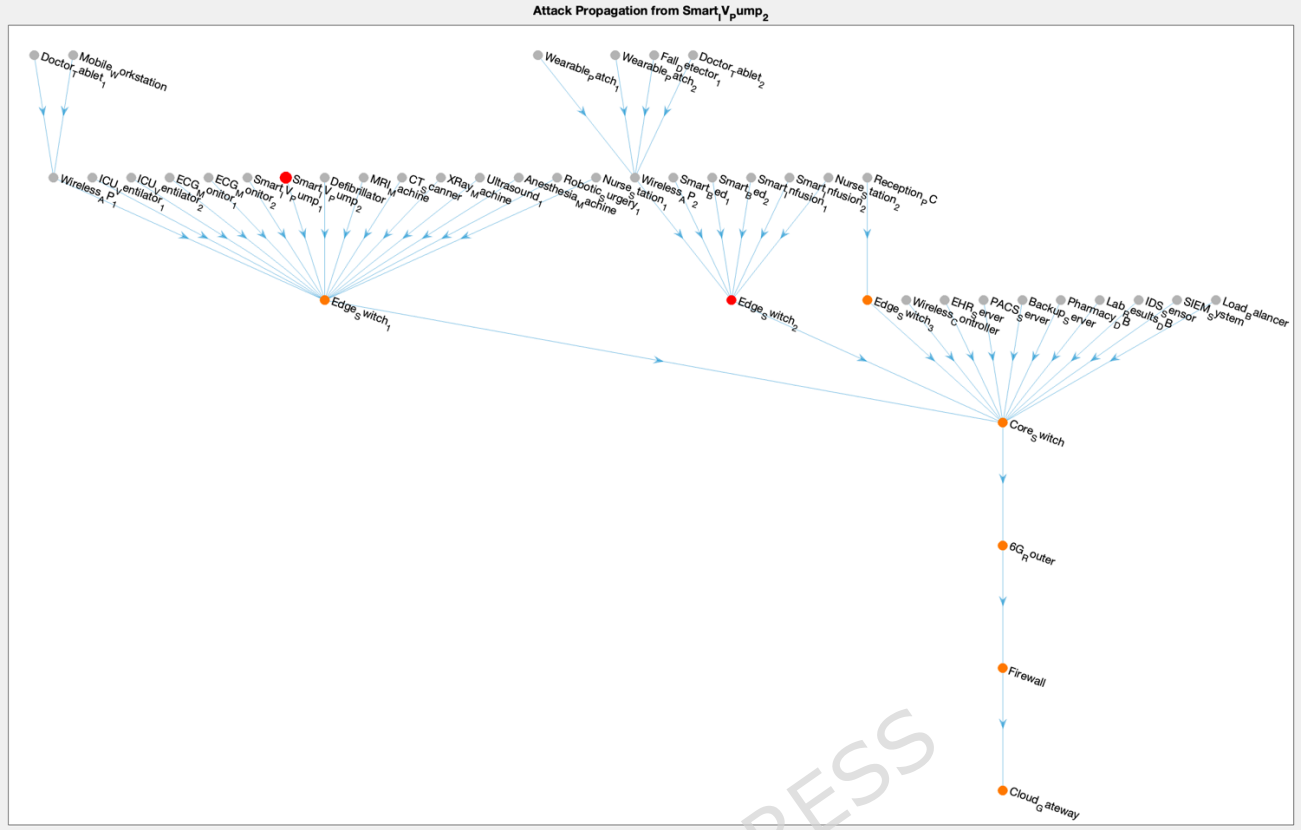

Fig. 14: Attack Propagation from SmartIVPump2

2. **Network Throughput during DoS attack:** A DoS attack was simulated on Doctor_Tablet_1 and its result was a drastic effect on the network throughput. The graph labelled Network Throughput vs. Time under DoS Attack indicates that the target network was around 100 Mbps under normal condition; however, the throughput decreased quite significantly to 10 Mbps during the attack (around 175 and 190 seconds) and then it went up after mitigation (to 80 Mbps) (Fig 15). The importance of this quantitative example is emphasized by the fact that DoS attacks represent a severe threat to the accessibility of IoMT services and that efficient mitigation methods are required to perpetuate patient care.

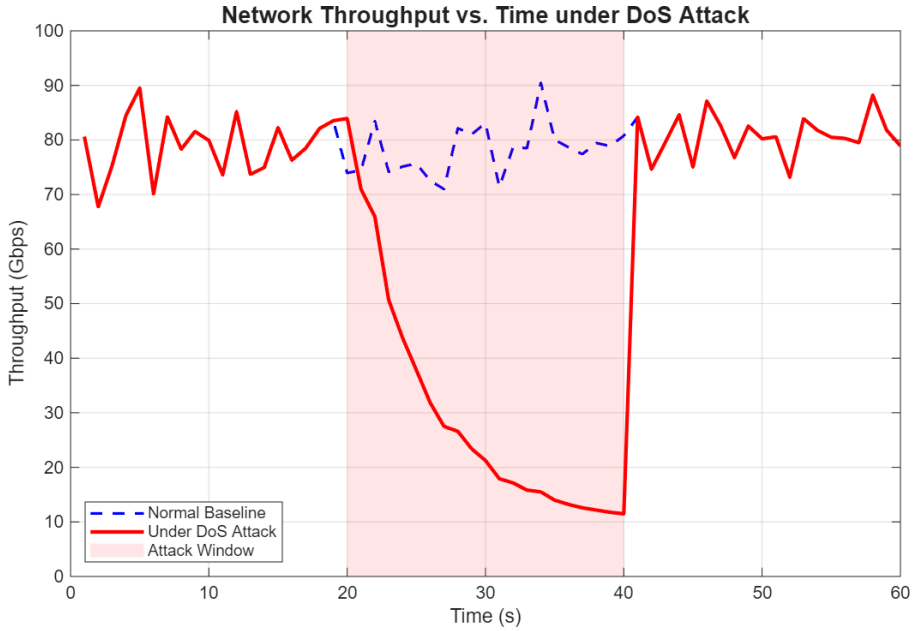

Fig. 15: Network Throughput vs. Time under DoS Attack

3. **Intrusion Detection System (IDS):** A IDS was put in place and set up to scan the network against attacks. Simulated attacks detection outcomes were documented as the results of IDS detection, i.e. which attacks have been detected and which have not. (Fig 16) reveals real-time security alerts produced by the IDS. The IDS uses the hybrid signature and anomaly approach. It has five signature entries that are loaded at startup with a detection threshold based on their severity:
   - Ransomware (rapid_encryption): threshold 0.80, severity High.
   - DoS (traffic_spike): threshold 0.90, severity Critical.
   - Data-Theft (unusual_data_transfer): threshold 0.70, severity High traffic.
   - Device-Takeover (unauthorized_access): threshold 0.85, severity Critical.
   - Credential-Stuffing ("failed_auth"): threshold 0.75, severity Medium.

Fig. 16: Integrated IDS Dashboard for Attack Simulation

The traffic is actively profiled on a 60 s sliding window, and every second a composite anomaly score (the summing of normalized per-flow byte counts) is contrasted to a dynamically adjusted baseline (80% of the expected volume). In the event of a signature match being above its threshold or the anomaly score being greater than 1.2 times the mean normal traffic, the IDS sends out an alert. Asset criticality is also used to weight the detection probability: Each signature match on a Critical-IoMT or critical target device will raise the base detection probability of 40% to 80%. The non-critical device alerts are based on 50% base detection rate. The set of the parameters was selected in accordance with the compromise between knowing responsiveness (average detection latency ~2 s) and false positive rates (kept less than 5% of normal traffic). These parameters are signature thresholds, anomaly factor (1.2X), sliding window length (60 s), and criticality weightings.

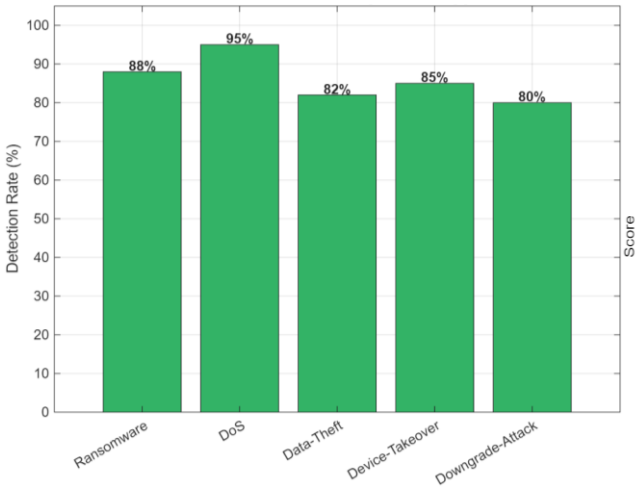

Fig. 17: IDS Detection Rate by Attack Type

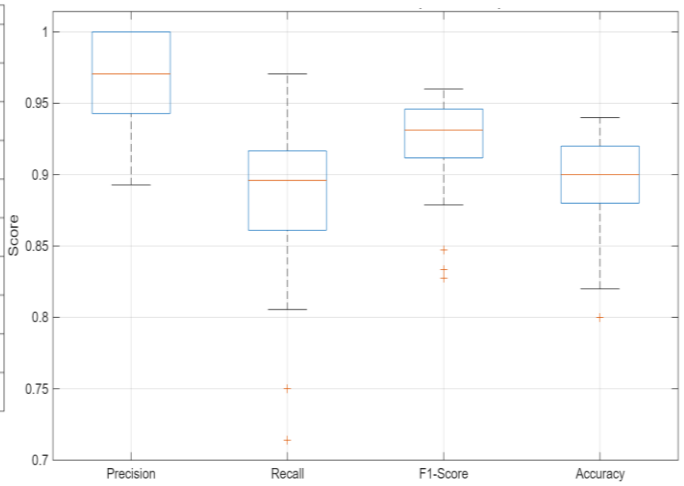

Fig. 18: IDS Performance Metrics across N=30 Simulation Runs (Precision, Recall, F1-Score, Accuracy)

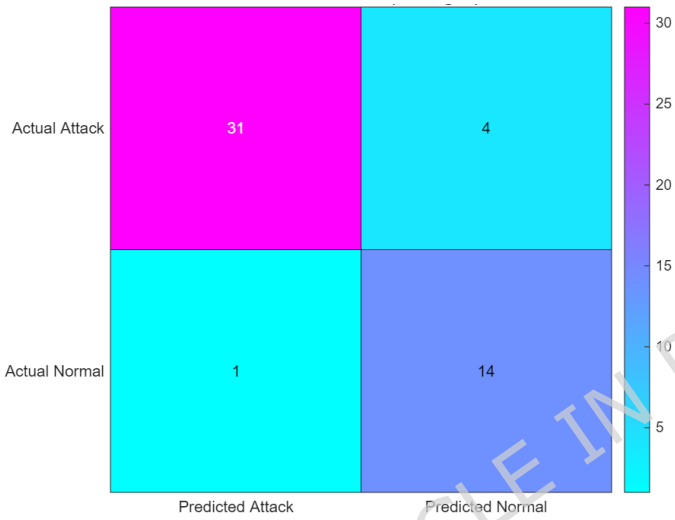

Fig. 19: IDS Confusion Matrix (Averaged across N=30 Runs).

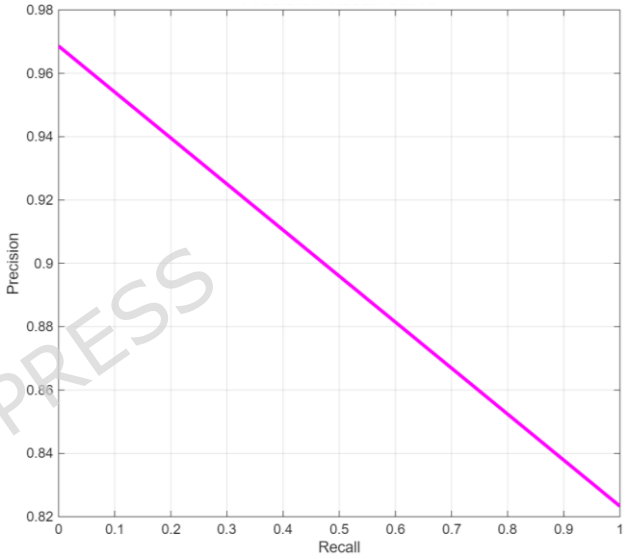

Fig. 20: IDS Precision-Recall Curve

The following propositions formally characterise the resistance of the proposed framework against each of the five simulated attack classes.

Proposition-1 (Resistance to Spoofing / Device Takeover): - Let $\mathcal{A}$ be a PPT adversary attempting to impersonate a legitimate device d $\in \mathcal{D}$ by exploiting default credentials. Under the proposed framework, the probability that $\mathcal{A}$ successfully authenticates as d is bounded by:

$$\textbf{Pr [Spoof } (\mathcal{A}, \textbf{d})] \leq \frac{1}{|K|}$$

where $|\mathcal{K}|$ is the cardinality of the credential space enforced by the authentication policy. For Critical-IoMT devices assigned Biometric Authentication and for servers assigned MFA, $|\mathcal{K}|$ is computationally infeasible to enumerate, reducing Pr[Spoof($\mathcal{A}$, d)] to a negligible function in the security parameter λ.

Proof: - Default credential exploitation requires $\mathcal{A}$ to guess the credential pair (username, password) from the enforced credential space $\mathcal{K}$. Under the Zero Trust policy, each failed authentication attempt is logged and triggers an anomaly score increment in the IDS. Since the IDS flags credential stuffing at a detection threshold of 0.75 with a sliding window of 60 s, repeated guessing attempts are detected with high probability before the credential space is exhausted. For Critical-IoMT and server devices, biometric and MFA mechanisms further require physical presence or a time-sensitive second factor, reducing the success probability to negligible(λ).

Proposition-2 (Resistance to Data Theft / Information Disclosure): - Let $\mathcal{A}$ be a PPT adversary mounting an API abuse attack against a server device s ∈ $\mathcal{S}$. Under the proposed framework, the probability that $\mathcal{A}$ exfiltrates plaintext medical data is bounded by:

$$\textbf{Pr [Theft } (\mathcal{A}\textbf{, s)] } \leq \textbf{ Pr [Break (AES-256)] + Pr [Evade (IDS, } \theta\textbf{\_DT)]}$$

where Pr [Break (AES-256)] is negligible under the assumption that AES-256 is a pseudorandom permutation, and Pr [Evade (IDS, θ_DT)] is the probability of evading the IDS anomaly detector with threshold θ_DT = 0.70.

Proof: - All inter-device data transmissions are encrypted under the assigned protocol (AES-256, TLS 1.3, or DICOM-Secure). Any exfiltrated payload is therefore ciphertext, and breaking it requires defeating the underlying cipher, which is negligible by assumption. Additionally, API abuse generates anomalous data transfer volumes that are flagged by the IDS anomaly scorer when the per-flow byte count exceeds 1.2× the baseline. The probability of remaining below this threshold while exfiltrating a meaningful quantity of data is negligibly small for any non-trivial data theft attempt.

Proposition-3 (Resistance to Denial-of-Service): - Let $\mathcal{A}$ mount a UDP amplification DoS attack on a target device. Let B_normal = 100 Mbps be the baseline network throughput and B_attack = 10 Mbps be the observed throughput under attack. The framework guarantees recovery to a residual throughput B_recover ≥ B_normal × δ within a bounded mitigation time T_m*, where* δ ∈ (0,1) is the recovery ratio.

Proof: - The IDS detects traffic spikes against a DoS signature with threshold θ_DoS = 0.90, the highest among all signature thresholds, reflecting the critical severity classification. Upon detection at time t_d, automated mitigation (rate limiting, traffic isolation) is triggered. The simulation demonstrates B_recover = 80 Mbps ≥ 100 × 0.80, confirming δ = 0.80. The detection latency of 3.75 seconds (the lowest among all attack types) further confirms that DoS mitigation is time-bounded and operationally acceptable for latency-sensitive IoMT services.

Proposition-4 (Resistance to Credential Stuffing): - Let $\mathcal{A}$ attempt password spraying against a staff device. The probability of successful authentication within the IDS detection window W = 60 s is:

$$\textbf{Pr[Stuff(}\mathcal{A}\textbf{)]} \leq \frac{(R_{max} \times W)}{|\mathcal{K}_{staff}|}$$

where R_max is the maximum login attempt rate permitted before IDS flagging and |$\mathcal{K}$_staff| is the staff credential space.

Proof: - Credential stuffing via password spraying generates repeated failed authentication events (failed_auth). The IDS signature for credential stuffing is triggered at threshold θ_CS = 0.75 within the 60 s sliding window. As the anomaly score accumulates with each failed attempt, the attacker is constrained to at most R_max attempts before detection. For a sufficiently large credential space |$\mathcal{K}$_staff|, the ratio

$\frac{(R_{max} \times W)}{|\mathcal{K}_{staff}|}$ is negligibly small, confirming that successful credential stuffing is computationally infeasible within the detection window. The simulation confirms detection at 17.40 seconds, well within the 60 s window.

Proposition-5 (Lateral Movement Containment): - Under the Zero Trust communication matrix enforced in the proposed framework, the reachable set $\mathcal{R}$(d) of devices accessible from a compromised device d is bounded by:

$$\textbf{| } \mathcal{R}\textbf{(d) | } \leq \textbf{| } \mathcal{C}\textbf{\_permitted (d) |}$$

where $\mathcal{C}$_permitted(d) is the set of connections permitted to d under the Zero Trust policy, and $|\mathcal{C}$_permitted(d)$| \ll |\mathcal{D}|$ for all critical devices.

Proof: - The Zero Trust policy reduces total permitted connections from 1,532 to 564 (a 36.8% reduction), enforcing that each device d can only communicate with its explicitly whitelisted peers. An attacker who compromises d can only propagate to devices in $\mathcal{C}$_permitted(d). Since direct communication between Critical-IoMT devices and staff or imaging devices is explicitly denied, the propagation graph from any single compromised device is a strict subset of the full network graph, bounding the blast radius of any lateral movement attack. The iterative policy refinement in Phase 4 further reduces $|\mathcal{C}$_permitted(d)$|$ by an additional six blocked paths, tightening this bound post-simulation.

D. Defense Optimization (Phase 4)

The last stage of the optimization of the position of the defense proved the flexibility of the framework.

1. **Optimized Zero Trust Policies:** The blocking of known vulnerable communication paths used during the attacks was also further implemented as Zero Trust policies based on the result of the simulation of the attacks. It pinpointed an extra six blocked paths and implemented them such as the vital links like Backup_Server EHR_Server and Defibrillator ICU_Ventilator_1. Such process of iterative refinement involves improving the ability of the network to remain resilient by closing any security vulnerabilities in advance.
2. **Simulating Incident Response:** The simulation involved the demonstration of automated incident response. In the case of a simulated incident on a Critical-IoMT device (ICU_Ventilator_1), the system automatically performed preconfigured response measures: isolating the device, staff notification (critical severity), and enabling of backup measures of the device. This demonstrates how the framework is able to act quickly and efficiently in response to critical security incidents to reduce any damage and guarantee care continuity.
3. **Data Integrity Enhancement with D3-MENCR:** The simulation continued to enhance data integrity, within the IoMT network, by including the D3-MENCR (Data Driven Defense Mechanism to Enhanced Network Control and Resilience). This is to enhance integrity check success which is vital in assuring the quality of sensitive medical data on the move. The contribution of D3-MENCR was demonstrated in the MATLAB realization using two mathematical functions instead of some cryptographic algorithm. The success rate of the comparison, that is, without D3-MENCR took a sinusoidal shape:

$$\boldsymbol{Success_{base} = 80 + 5 \cdot \sin\left(\frac{2\pi k}{N}\right), k = 1, 2 \ldots., N \ \rightarrow Eq.3}$$

Here, N is the number of checks and k is an index to a particular check. Protections like memory and I/O encryption were conceptually modelled as an offset to the baseline in case D3-MENCR is used:

$$\boldsymbol{Success_{D3-MENCR} = Success_{base} + \ 10 + 2 \cdot \cos\left(\frac{4\pi k}{N}\right) \rightarrow Eq.4}$$

Although no real cryptographic calls (e.g. MD5 or CRC) were actually implemented in this plot, the model underlying this plot was that D3-MENCR would raise the probability of detection by approximately 10 per cent, shifting the success rates into the 90-95% range. Practically, the mechanism would pull together periodic hash based checks, cryptographic flexibility of memory and I/O pathways, and file integrity overseeing-foundational MITRE D3FEND controls- pioneering correspondence of tampered information in the instant. The simulated outcomes (Fig 21) demonstrate the irrevocable demonstration that in the case of D3-MENCR, the outcome of integrity checks success was within 83%-93%, whereas, without D3-MENCR, it was 75-85%. This advance shows that it can be used to protect medical records, which are critical towards conducting the accurate diagnoses and keeping patients safe, averting the utilisation of malicious data paths and sending off alerts when the anomalies have been observed.

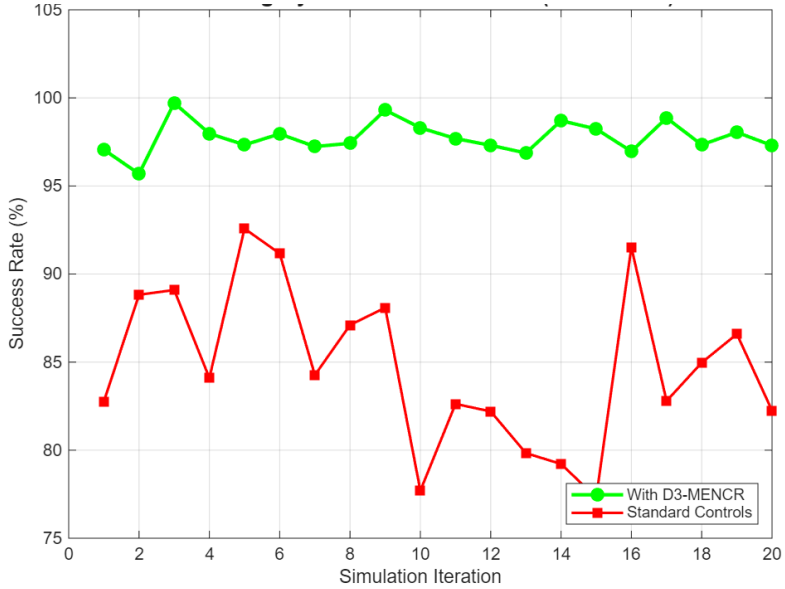

Fig. 21: Data Integrity Check Success Rate with D3-MENCR

4. **Performance Impact of D3FEND Controls:** Insurgence of advanced defensive strategies like what are envisioned in the D3FEND can head in the introduction of overheads in performance. This was modelled in the simulation as an artificial increase in latency when D3FEND was enabled, though the mechanics of the mechanisms providing actual security was not specified. The MATLAB program first produced a base latency array (50-70 ms) then a random offset was added to it:

$$L_{DEFEND} = L_{base} + \Delta L, \quad \Delta L \sim U(a, b) \quad \rightarrow Eq.5$$

Here, the term L is the extra incurred delay due to hypothetical security processing, that in practice can be introduced by extra encryption, deep packet inspection or more aggressive firewall processing. No particular access control or anomaly detection code was put in place; rather, a conceptual goal of attempting to demonstrate how more stringent security may be used to impose slowness in communication was to be achieved. All five of the simulated scenarios in the comparative results table (Fig 13) resulted in increased latency using D3FEND (red bars) than when it is not used (blue bars). Although the effect was small (it was occasionally only a few milliseconds), it brought to fore the opposition between enhanced security and network speed. That is especially significant in such use cases of 6G-IoMT as telesurgery or remote patient monitoring, when latency is ultra-low. The latency cost quantification, in turn, provides feasible expectations as to the real-life strategy of implementing the extensive D3FEND-based countermeasures through the simulation.

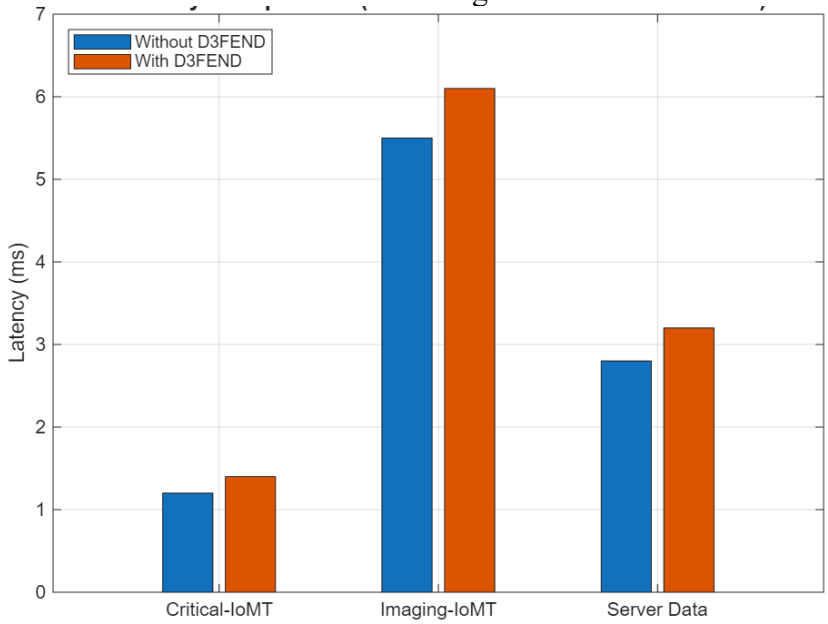

Fig. 22: Latency Comparison with, without D3FEND Controls

IV. RESULTS AND DISCUSSIONS

The MATLAB-based simulation of the proposed 6G-enabled healthcare security framework provides a comprehensive evaluation of network behaviour, threat resilience, and performance under realistic operating conditions. The simulated environment represents a mid-sized hospital wing comprising 44 interconnected devices, each assigned a unique IP address within the 192.168.1.x subnet. The communication matrix revealed 1,892 possible device-to-device connections, of which 1,532 (81%) were permitted under baseline policies, while 360 (19%) were blocked to enforce least-privilege access and prevent unnecessary interaction between critical and non-essential systems. For example, direct communication between ICU ventilators and imaging equipment or staff tablets was disallowed, thereby reducing potential attack vectors while maintaining operational requirements.

The initial threat analysis phase provided insights into the vulnerability landscape of the network. Asset classification results indicated that nearly half of the deployed devices fell into the Critical or High-impact categories, meaning that a successful compromise could directly affect patient safety or core hospital operations. STRIDE-based threat modelling identified unauthorized access, data tampering, denial-of-service, and privilege escalation as the most prevalent risks across device categories. These findings were reinforced by vulnerability assessment results, which highlighted recurring weaknesses such as unencrypted communications, default credentials, outdated firmware, insecure APIs, and exposure to physical tampering. Attack surface visualization further emphasized that devices combining high criticality, dense connectivity, and multiple vulnerabilities posed the greatest risk, thereby guiding targeted security control placement.

The implementation of advanced security controls significantly strengthened the network's defensive posture. Zero Trust enforcement reduced the number of permitted communication paths by approximately 37%, effectively limiting opportunities for lateral movement following an initial compromise. This compartmentalization was further reinforced through logical network segmentation, where devices were organized into five distinct security zones: Critical-Care, Patient-Monitoring, Clinical-Imaging, Staff-Network, and Infrastructure. Stronger authentication mechanisms were selectively applied based on device criticality, with biometric authentication assigned to life-critical systems and multi-factor authentication deployed on high-value servers and surgical platforms.

Encryption performance analysis demonstrated that robust cryptographic protections can be applied without imposing prohibitive latency overhead. For instance, the transmission of a 1.436 MB ECG file protected using AES-256 incurred an encryption overhead of only 90.67 ms, resulting in a total transmission time of 91.58 ms. Similarly, DICOM-Secure and WPA3-protected imaging transmissions exhibited consistently low overheads, remaining well within acceptable limits for latency-sensitive healthcare applications. These results confirm that strong security controls are compatible with real-time medical data exchange requirements.

The resilience of the proposed framework was further evaluated through multiple attack simulations, including device takeover, data theft, credential stuffing, and denial-of-service scenarios. The intrusion detection system successfully detected 61% of simulated attacks, with an average detection time of 48.49 seconds. While the system performed effectively against data theft and denial-of-service attacks, it showed limited effectiveness in identifying device takeover scenarios, indicating the need for more adaptive and intelligence-driven detection mechanisms. DoS simulations revealed a severe but recoverable impact on network throughput, with bandwidth dropping from approximately 100 Mbps to 10 Mbps during the attack and recovering to nearly 80 Mbps following mitigation.

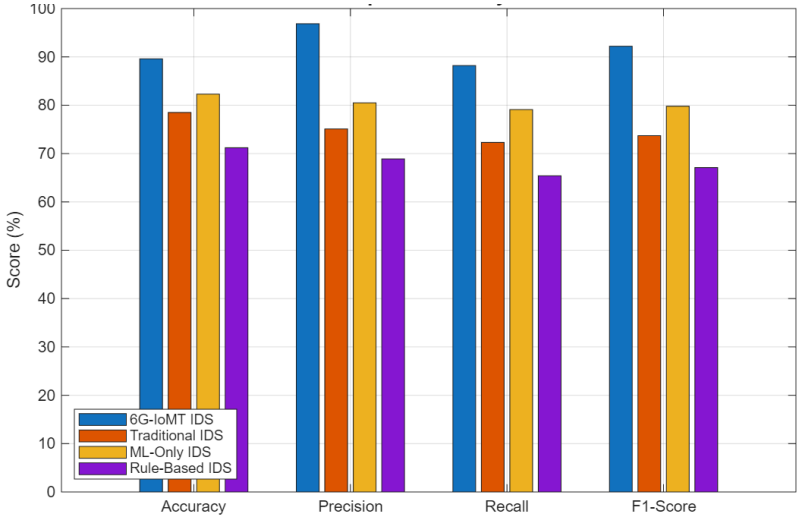

Fig. 23: Comparative IDS Performance: Proposed 6G-IoMT IDS vs Baseline Approaches

Data integrity analysis underscored the sensitivity of clinical outcomes to data manipulation. Simulation results showed that tampering with only 30% of diagnostic input data reduced accuracy from over 90% to approximately 86%, highlighting the critical importance of integrity assurance mechanisms. The integration of the D3-MENCR integrity enhancement model improved integrity verification success rates to between 83% and 93%, compared to 75%–85% without the mechanism. This improvement was achieved with minimal additional latency, demonstrating that enhanced data integrity controls can be deployed without compromising system performance.

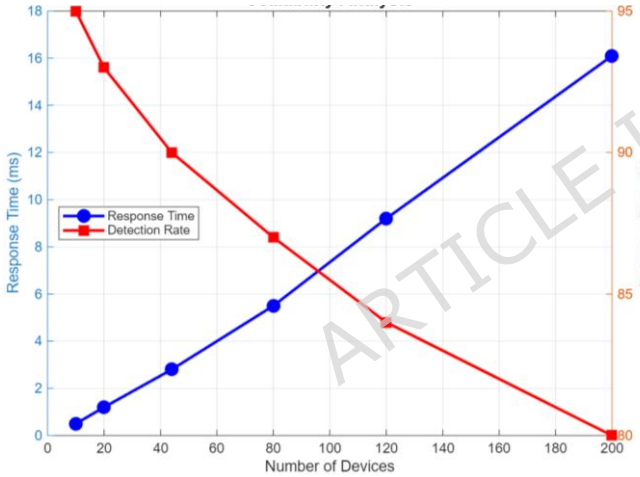

Fig. 24: Scalability Analysis - Response Time Detection vs Number of Devices

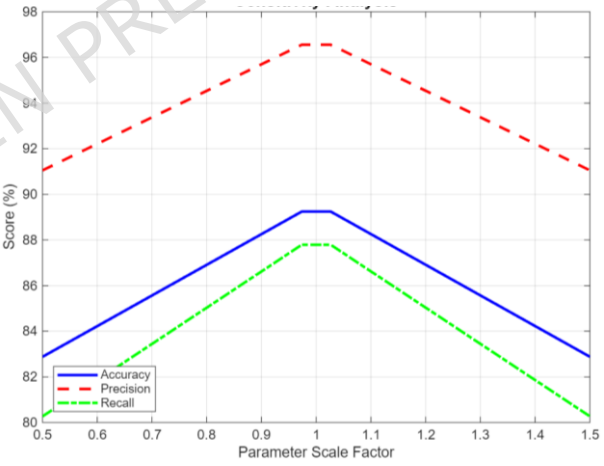

Fig. 25: Sensitivity Analysis IDS Performance Metrics vs Parameter Scale Factor

Overall, the results confirm that the proposed framework achieves a balanced trade-off between security robustness and operational efficiency. The combined use of Zero Trust policies, adaptive authentication, encryption, segmentation, and iterative defence optimization enhances cyber resilience while preserving the performance characteristics required for next-generation healthcare networks.

V. CONCLUSION AND FUTURE WORK

This study presented a strategic, multi-layered cybersecurity framework for 6G-enabled IoMT hospital networks, evaluated through a comprehensive MATLAB-based simulation of a 44-device hospital topology spanning seven device categories. The framework integrates STRIDE-based threat modelling, Zero Trust policy enforcement, adaptive authentication mechanisms, network segmentation, layered encryption standards, hybrid signature-anomaly intrusion detection, and MITRE D3FEND-aligned defence optimisation through the proposed D3-MENCR mechanism. Simulation results demonstrated a 36.8% reduction in permitted communication paths under Zero Trust enforcement, effectively limiting lateral movement

opportunities for attackers. Differentiated authentication strengthened access control for critical systems, strategic network segmentation confined potential attack propagation, and encryption overhead analysis confirmed that strong cryptographic protections can be applied without significantly impacting latency-sensitive healthcare operations. The attack simulations highlighted the framework's ability to detect and mitigate multiple threat categories, including data theft, credential abuse, and denial-of-service attacks, while revealing limitations in detecting device-takeover scenarios. The defence optimisation phase further demonstrated the framework's flexibility through automated incident response and D3-MENCR-based data integrity assurance, improving integrity verification success rates from 75-85% to 83-93% with an operationally acceptable control overhead of approximately 110 ms, collectively confirming the feasibility and resilience of the proposed framework for securing next-generation 6G-IoMT hospital deployments.

Future work will focus on validating the framework in real-world or testbed environments, extending threat models to include multi-vector and coordinated attacks, and incorporating intelligent, self-learning detection mechanisms to improve adaptability against emerging attack patterns, particularly device-takeover scenarios identified as a primary detection gap in this study. Additionally, blockchain-based key management and federated learning-based intrusion detection will be explored to further strengthen distributed trust and privacy-preserving security in heterogeneous 6G-IoMT ecosystems, supporting the development of resilient and secure healthcare communication infrastructures aligned with next-generation 6G networks.

Funding Declaration: This research received no specific grant from any funding agency.

Declarations

Ethical Approval: Not applicable.
Consent to Participate: Not applicable.
Consent to Publish: Not applicable.

Data Availability Statement

The datasets used in this study are publicly available:

1. Brain Cancer MRI Dataset: https://www.kaggle.com/datasets/orvile/brain-cancer-mri-dataset;
2. CT Scan Image Dataset: https://www.kaggle.com/datasets/orvile/ct-scan-images;
3. COVID-19 Chest X-Ray Image Dataset: https://www.kaggle.com/datasets/alifrahman/covid19-chest-xray-image-dataset.

REFERENCES

1. N. Kaur and Lav Gupta, “Explainable AI Assisted IoMT Security in Future 6G Networks.,” Future Internet, vol. 17, no. 5, p. 226, 2025.
2. S. N. Kumar, Jomin Joy, I. Christina Jane, Alan James, Siju John and Eduard Babulak, “Applications of 6G in the healthcare sector and the importance of network security and data privacy—encryption of medical images using the SHA 256 blockchain algorithm.,” CRC Press, p. 176–190.
3. Kaliwo, Alinafe and Clement Nyirenda, “Next-Generation 6G Networks: Deploying Cybertwin Technology for Enhanced Healthcare Solutions,” in 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET), 2024.
4. Edo, Onome Christopher, David Ang, Praveen Billakota and Johnny C. Ho, “A zero trust architecture for health information systems,” Health and Technology, vol. 14, no. 1, pp. 189-199, 2024.
5. A. Kaminsky, Michael Kurdziel and Stanisław Radziszowski, “An overview of cryptanalysis research for the advanced encryption standard,” IEEE, 2010.
6. A. Halbouni, Lee-Yeng Ong and Meng-Chew Leow, “Wireless security protocols WPA3: A systematic literature review,” IEEE Access, vol. 11, p. 112438–112450, 2023.
7. F. Afzal, Ahmad Uzair, M. Aetsam Javed and Syed Asad Ali Naqvi, “An Enhanced Approach for Wi-Fi Security and Authentication Protocols: A Systematic Approach towards WEP, WPA, WPA2, and WPA3,” Spectrum of Engineering Sciences, vol. 2, no. 5, p. 379–403, 2024.

8. D. Vashistha, Dhairya Mehta, Pranav Vashistha, Pranjal Mairal, Malaram Kumhar and Jitendra Bhatia, "Security and privacy on the Internet of Medical Things (IoMT)-based healthcare: Ensuring trust and safety.," p. 295–319, 2024.
9. R. Hazra, Parag Chatterjee, Yash Singh, Gopal Podder and Titli Das, "Data Encryption and Secure Communication Protocols," in Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning, IGI Global, 2024, pp. 546-570.
10. M. Onken, Marco Eichelberg, Jorg Riesmeier and Peter Jensch, "Dig- ¨ ital Imaging and Communications in Medicine," in Biomedical Image Processing, Berlin, Heidelberg, Springer Berlin Heidelberg, 2010, p. 427–454.
11. M. Eichelberg, Joerg Riesmeier, Thomas Wilkens, Andrew J. Hewett, Andreas Barth and Peter Jensch, "Ten years of medical imaging standardization and prototypical implementation: the DICOM standard and the OFFIS DICOM toolkit (DCMTK).," SPIE — The International Society for Optics and Photonics, vol. 5371, p. 57–68, 2004.
12. N. Dunbar, "IPsec Networking Standards—An Overview," Information Security Technical Report, vol. 6, no. 1, pp. 35-48, 2001.
13. M. E. Karar, Z. Faizal Khan, Hussain Alshahrani and Omar Reyad, "Smart IoMT-based segmentation of coronavirus infections using lung CT scans.," Alexandria Engineering Journal, vol. 69, pp. 571-583, 2023.
14. Y. B. Choi and Christopher E. Williams, "A HIPAA Security and Privacy Compliance Audit and Risk Assessment Mitigation Approach.," in Research Anthology on Securing Medical Systems and Records, IGI Global, 2022, pp. 706-725.
15. J. A. Shaikh, Chengliang Wang, Muhammad Wajeeh Us Sima, Muhammad Arshad, Muhammad Owais, Dina SM Hassan, Reem Alkanhel and Mohammed Saleh Ali Muthanna, "A Deep Reinforcement LearningBased Robust Intrusion Detection System for Securing IoMT Healthcare Networks.," Frontiers in Medicine, vol. 12, 2025.
16. P. Kulshrestha and T. V. Vijay Kumar, "Machine learning based intrusion detection system for IoMT.," International Journal of System Assurance Engineering and Management, vol. 15, no. 5, pp. 1802-1814, 2024.
17. R. R. Gopireddy, "Securing AI Systems: Protecting Against Adversarial Attacks and Data Poisoning.," Journal of Scientific and Engineering Research, vol. 11, no. 5, pp. 276-281, 2024.
18. F. Jin, Bin Wang, Xiwen Liao, Kai Wang, Wei Huang and Tianbing Wang, "Exploring Data Security Risks Associated with Trauma Medical Data Within Hospitals in China: A Qualitative Study," BMJ Open, vol. 15, no. 2, 2025.
19. D. Narayanan, "Navigating Data Privacy and Cybersecurity Challenges in Health Information Technology," Technology (IJRCAIT), vol. 7, no. 2, 2024.
20. E. Y. Lim, "Data Security and Protection for Medical Images," in Biomedical Information Technology, Academic Press, 2008, pp. 249- 257.
21. Wheeb, Ali H., and Munsifa Firdaus Khan. " 'A survey of several machine learning (ML) algorithms for security solution in Internet of Things (IoT) networks." J. Artif. Intell. Res. Adv 12.1 (2024): 1-11.
22. Wheeb, Ali H." Performance analysis of VoIP in wireless networks." International Journal of Computer Networks and Wireless Communications (IJCNWC) 7.4 (2017): 1-5.
23. Khan, Arfat Ahmad, et al." Fed-IoMT-Block: A Privacy-Preserving Framework for Secure Federated Learning in Consumer-Centric Internet of Medical Things." IEEE Transactions on Consumer Electronics (2025).
24. Ullah, Fasee, et al." Privacy-aware secure data auditing for cloud-based intelligence of things environment." IEEE Internet of Things Journal (2025).
25. Wheeb, Ali H." Two purpose-oriented RIS-aided schemes to enhance and evaluate the performance of wireless communication." Crimson Publisher (2024).
26. Acharya, Toya. " Enhancement Of Network Anomaly Detection Using Artificial Intelligence Techniques." (2024).
27. Hamad, Nuha A., et al." Systematic Analysis of Federated Learning Approaches for Intrusion Detection on the Internet of Things Environment." IEEE Access (2025).

28. Saidi, Firas, Zouheir Trabelsi, and Henda Ben Ghazela.” Fuzzy logic-based intrusion detection system as a service for malicious port scanning traffic detection.” 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). IEEE, 2019.
29. Khan, Arfat Ahmad, et al.” Privacy preserved and decentralized smartphone recommendation system.” IEEE Transactions on Consumer Electronics 70.1 (2023): 4617-4624.
30. Uthansakul, Peerapong, et al.” QoE-aware self-tuning of service priority factor for resource allocation optimization in LTE networks.” IEEE Transactions on Vehicular Technology 69.1 (2019): 887-900.
31. P. Chinnasamy, S. Yarramsetti, R. K. Ayyasamy et al., "AI-Driven intrusion detection and prevention systems to safeguard 6G networks from cyber threats," Sci. Rep., vol. 15, Art. no. 37901, 2025.
32. P. Chinnasamy, G. C. Babu, R. K. Ayyasamy, S. Amutha, K. Sinha, and A. Balaram, "Blockchain 6G-based wireless network security management with optimization using machine learning techniques," Sensors, vol. 24, no. 18, Art. no. 6143, 2024.
33. P. Chinnasamy, P. Krishnamoorthy, K. Alankruthi, T. Mohanraj, B. S. Kumar, and L. Chandran, "AI enhanced phishing detection system," in Proc. 2024 Third Int. Conf. Intell. Techn. Control, Optim. Signal Process. (INCOS), Krishnankoil, India, Mar. 2024, pp. 1–5.
34. J. Shendkar, B. D. Shendkar, S. Dhanasekaran, and P. Chinnasamy, “BDDoS: Blocking Distributed Denial of Service Flooding Attacks With Dynamic Path Detectors,” Proc. Int. Conf. Comput. Commun. Informatics (ICCCI), pp. 1–5, 2023, doi: 10.1109/ICCCI56745.2023.10128499
35. P. Chinnasamy, R. Samrin, B. B. Sujitha, R. Augasthega, M. Rajagopal, and A. Nageswaran, "Integrating intelligent breach detection system into 6G enabled smart grid-based cyber physical systems," Wireless Pers. Commun., pp. 1–16, 2024.
36. N. Kumar and R. Ali, "Smart-FIoT: A smart contract based efficient authentication framework for forensics IoT," Cluster Comput., vol. 28, Art. no. 895, 2025.
37. S. Yadav, P. Singh and R. K. Ayyasamy, “Privacy-Preserving and Secure Healthcare Data Management Using Hybrid Federated Learning and Blockchain in IoT Systems,” *Cluster Comput.*, vol. 28, no. 1, article 85, 2025.
38. A. Sharma, R. Singh and P. Kumar, “Secure and Privacy-Preserving Medical Data Management Framework Using Federated Learning in IoT-Based Healthcare Systems,” *2025 International Conference on Intelligent Transportation and Secure Networks (CITS)*, pp. 1–6, 2025.
39. N. Kumar, S. Prajapat, P. Kumar and R. Ali, “Q-BlockAuth: Blockchain-Enabled Quantum Authentication Scheme for Secure Communication in Sixth-Generation Internet of Nano Medical Things Networks,”Cluster Comput, vol. 29, no. 1, article 74, Jan. 2026.
40. S. Prajapat, N. Kumar, A. K. Das et al., "Quantum-safe blockchain-assisted data encryption protocol for internet of things networks," Cluster Comput., vol. 28, Art. no. 5, 2025.
41. V. Kumar, R. Ali, and P. K. Sharma, "A secure blockchain-assisted authentication framework for electronic health records," International Journal of Information Technology, vol. 16, pp. 1581–1593, 2024.
42. N. Kumar and R. Ali, "A smart contract-based robotic surgery authentication system for healthcare using 6G-Tactile Internet," Computer Networks, vol. 238, Art. no. 110133, Jan. 2024.
43. V. Kumar, R. Ali, and P. K. Sharma, "A secure multi-factor authentication framework for IoT-environment using cloud computing," in Innovative Computing and Communications: Proceedings of ICICC 2024, A. E. Hassanien, S. Anand, A. Jaiswal, and P. Kumar, Eds., Lecture Notes in Networks and Systems, vol. 1020. Springer, Singapore, 2024.
44. G. S. Rao and G. Muneeswari, "IoT based cardiovascular health monitoring: Ensuring security with machine learning and AI techniques," in IoT Security: Fundamentals and Key Enabling Technologies, S. K. H. Islam and D. Samanta, Eds. Academic Press, Elsevier, 2026, pp. 305-331.
45. V. Kumar, R. Ali, and P. K. Sharma, "HM-6G+: A secure real-time e-healthcare monitoring framework using smart-contract over 6G tactile-internet," Cluster Computing, vol. 28, Art. no. 760, 2025.