GMR
The Original

AN EDGE-CENTRIC SECURITY RISK ASSESSMENT FRAMEWORK FOR INTERNET OF MEDICAL THINGS WITH QOS-AWARE SIMULATION

Ms. S. Mary Helan Felista[1], Dr. M. Ganaga durga[2]

[1]Research Scholar, Department of Computer Applications, Sri Meenakshi Govt. Arts College for Women(A), Madurai & Assistant Professor, Department of MCA, Fatima College, Mary Land, Madurai. E-mail: felistamichael2012@gmail.com
[2]Research Supervisor, Assistant Professor, Department of Computer Applications, Sri Meenakshi Govt. Arts College for Women(A), Madurai. E-mail: mgdurga@yahoo.com

ABSTRACT
Background
The rapid adoption of the Internet of Medical Things (IoMT) has enabled continuous monitoring and transmission of sensitive healthcare information through interconnected medical sensors, wearable devices, edge nodes, and cloud services. However, the heterogeneous and resource-constrained nature of IoMT environments introduces significant security risks, while attacks on edge-connected medical devices can adversely affect both security and quality of service (QoS). Existing studies have primarily focused on individual security mechanisms, intrusion detection, authentication, or blockchain-based protection, with comparatively less emphasis on integrating security-risk assessment with edge-resource and QoS evaluation. Recent literature also demonstrates the need for systematic approaches to IoMT risk assessment and management. This paper proposes an Edge-centric IoMT Security Risk Assessment (EISRA) framework for evaluating security risks in edge-enabled IoMT environments. The proposed framework models heterogeneous medical devices, edge nodes, an edge gateway, and a healthcare cloud while considering multiple security threats, including Distributed Denial-of-Service (DDoS), Man-in-the-Middle, replay, data injection, and device impersonation attacks. A composite risk score is formulated using likelihood, impact, device criticality, vulnerability, and edge exposure. A simulation environment is developed to evaluate the proposed framework under varying IoMT device densities and attack intensities. The performance is assessed using security and QoS parameters including risk score, latency, throughput, packet delivery ratio, CPU utilization, memory utilization, energy consumption, and network overhead. The simulation results are subsequently compared with representative existing approaches under common evaluation criteria. The framework provides an integrated basis for evaluating security risk and edge-level QoS performance in IoMT environments.

KEYWORDS: Internet of Medical Things, Edge Computing, Security Risk Assessment, IoMT Security, QoS, Edge Devices, Cybersecurity, Simulation.

INTRODUCTION
1.1 Background and Motivation
The Internet of Medical Things (IoMT) has emerged as an important component of smart healthcare by enabling medical devices, sensors, wearable systems, monitoring equipment, and healthcare servers to communicate and exchange medical information [1], [2]. IoMT-based systems support continuous monitoring of patients by collecting physiological parameters such as electrocardiogram (ECG), blood pressure, blood glucose, oxygen saturation (SpO_2), and other health-related measurements [1], [3]. The availability of continuous medical data can support remote patient monitoring, timely clinical decision-making, and improved healthcare services [1], [2]. However, the increasing connectivity and exchange of sensitive medical information also introduce significant security and privacy concerns [2], [4].

IoMT environments differ from conventional IoT systems because the information handled by these devices is highly sensitive and the operation of some medical applications can be time-critical [2], [4]. IoMT devices are also heterogeneous and may have limited computational capacity, memory, storage, and energy resources [2], [5]. These characteristics make them vulnerable to different security threats, including Distributed Denial-of-Service (DDoS), Man-in-the-Middle (MitM), replay, data injection, and device impersonation attacks [4], [5]. A successful attack may compromise the confidentiality or integrity of medical information and may also affect the availability and timely delivery of healthcare services [4], [5]. Therefore, security evaluation in IoMT should consider not only the existence of vulnerabilities but also the potential impact of attacks on medical devices and healthcare services [4], [6].

Edge computing provides an effective architectural layer for processing IoMT data closer to the data-generating devices [1], [7]. Instead of transferring all medical information to a remote cloud, edge nodes can perform data processing, aggregation, monitoring, and preliminary security analysis near the IoMT devices. This can reduce communication delay and improve the responsiveness of healthcare applications [1], [7]. However, edge-enabled IoMT environments introduce additional security considerations because multiple medical devices may communicate through shared edge gateways and edge nodes [5], [7]. An attack affecting an edge node can therefore influence several connected IoMT devices and increase resource utilization at the edge [5].

Consequently, IoMT security assessment should consider both security risk and system performance. A security mechanism that provides stronger protection but introduces excessive computational, communication, or energy overhead may not be suitable for resource-constrained medical environments [5]. Hence, parameters such as latency, throughput, packet delivery ratio, CPU utilization, memory utilization, energy consumption, and network overhead should be evaluated together with security risk [5], [7]. This motivates the development of an edge-centric security-risk assessment framework that can evaluate the security behaviour and QoS of IoMT systems under different device populations and attack conditions.

1.2 Problem Statement and Research Gap

Existing IoMT security research has investigated several individual security mechanisms, including authentication, intrusion detection, trust management, privacy protection, vulnerability assessment, and risk assessment [2], [4], [6]. Although these approaches have contributed significantly to improving IoMT security, many studies primarily focus on a particular security objective rather than jointly evaluating security risk, edge-device characteristics, and quality of service [4], [6]. In particular, the interaction between security threats and the resource utilization of edge nodes requires further investigation. Increasing numbers of IoMT devices and attack traffic may increase the workload of edge resources and consequently affect the performance of the healthcare network [5], [7].

Another limitation is that different medical devices may have different levels of criticality and vulnerability. Therefore, security risk cannot be adequately represented using a single factor. A comprehensive assessment should consider attack likelihood, potential impact, device criticality, vulnerability, and exposure at the edge layer [6]. Furthermore, the influence of different attack intensities on both security risk and QoS should be investigated under different IoMT network scales. A controlled simulation environment is therefore required to provide consistent experimental conditions and enable systematic comparison with existing approaches.

Based on these observations, this paper addresses the following problem: how to assess security risk in an edge-enabled IoMT environment while simultaneously considering heterogeneous medical devices, different attack conditions, edge-resource characteristics, scalability, and QoS performance? To address this problem, an Edge-centric IoMT Security Risk Assessment (EISRA) framework is proposed. The framework provides a simulation-based environment in which heterogeneous IoMT devices communicate through edge resources and are evaluated under different attack intensities. The proposed approach combines multiple security-risk factors and evaluates their relationship with important QoS and resource-utilization parameters.

1.3 Objectives and Contributions

The primary objective of this study is to develop and evaluate a simulation-based Edge-centric IoMT Security Risk Assessment (EISRA) framework that jointly considers security risk and QoS in an edge-enabled IoMT environment. The specific contributions of this work are:

Edge-enabled IoMT simulation environment: A simulation environment is developed consisting of heterogeneous medical devices, an edge gateway, multiple edge nodes, and a healthcare cloud.

Proposed EISRA risk model: A composite security-risk model is proposed by considering likelihood, impact, medical-device criticality, vulnerability, and edge exposure.

Multi-attack security evaluation: The framework considers DDoS, MitM, replay, data injection, and device impersonation attacks under different attack-intensity levels.

Security and QoS analysis: The proposed framework evaluates security risk together with latency, throughput, packet delivery ratio, CPU utilization, memory utilization, energy consumption, and network overhead.

Scalability and comparative evaluation: The framework is evaluated for different IoMT populations and edge-node configurations, with a feature-based comparison against representative existing approaches.

The remainder of this paper is organized as follows. Section 2 presents the related work on IoMT security, risk assessment, edge-based security, and QoS-aware healthcare systems. Section 3 describes the proposed EISRA framework, including the system architecture, threat model, risk factors, and risk calculation. Section 4 presents the simulation environment, experimental configuration, attack scenarios, and QoS parameters. Section 5 presents and discusses the simulation results with respect to security risk, attack intensity, scalability, QoS, and edge-resource utilization. Section 6 concludes the paper and presents directions for future enhancement.

2. RELATED WORK

2.1 IoMT Security and Risk Assessment

The increasing deployment of IoMT devices has resulted in considerable research on security, privacy, vulnerability assessment, and risk management. Existing studies have investigated different approaches to identify and mitigate security threats in medical IoT environments. A recent scoping review by Svandova and Smutny examined security risk assessment and management approaches for IoMT and highlighted the importance of systematically identifying vulnerabilities, threats, and associated risks in healthcare environments [8]. This work demonstrates the importance of risk-oriented security assessment but also indicates the diversity of approaches used for managing IoMT security risks.

Several studies have investigated specific security mechanisms for IoMT environments. Research on heterogeneous IoMT devices has explored risk evaluation and attack detection using analytical and fuzzy-logic-based approaches, demonstrating that different device characteristics and security conditions can influence the overall risk level [9]. Other studies have investigated dynamic cyber-risk assessment, where the security state of a medical IoT environment is evaluated under changing attack scenarios [10]. Such approaches demonstrate the importance of considering dynamic threat conditions rather than relying on static security assessment.

2.2 Edge-Based IoMT Security

The integration of edge computing with IoMT has received increasing attention because edge resources can process medical information closer to data-generating devices. Edge computing can reduce communication latency and decrease

the amount of data transmitted to remote cloud servers. However, the introduction of edge nodes also creates additional security concerns because edge nodes may serve multiple medical devices and can become potential targets for attackers. Recent research has investigated intrusion detection at the IoMT edge. For example, trust-centric intrusion detection approaches have been proposed to improve the identification of malicious activities in IoMT edge networks [11]. Such approaches demonstrate the importance of considering trust and network behaviour when detecting attacks at the edge. Other studies have combined blockchain and edge computing to improve IoMT authentication and trust management [12], [13]. Similarly, blockchain-enabled IoMT frameworks have evaluated performance parameters such as latency, throughput, packet delivery ratio, and energy consumption [12], [14]. These studies are particularly relevant because they demonstrate the importance of evaluating security mechanisms together with QoS.

2.3 Comparative Research Gap

The existing literature demonstrates that IoMT security has been investigated from several perspectives, including risk assessment, attack detection, authentication, trust management, blockchain, and edge computing. However, these research directions are generally evaluated independently or with different experimental configurations. This makes it difficult to directly assess the relationship between security risk and QoS in a scalable edge-enabled IoMT environment.

The proposed EISRA framework addresses this research gap by providing a common simulation environment in which heterogeneous IoMT devices communicate through edge resources and are evaluated under multiple attack conditions. Unlike approaches that primarily focus on a single security mechanism, EISRA combines risk assessment, attack analysis, edge-resource evaluation, QoS measurement, and scalability analysis.

Table 1. Comparison of Existing Research and Proposed EISRA

Research work	IoMT	Edge	Risk Assessment	Attack Analysis	QoS	Scalability
Švandová&Smutný (2024), Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review	✓	–	✓	✓	–	–
Czekster et al. (2025), Dynamic risk assessment approach for analysing cyber security events in medical IoT networks	✓	–	✓	✓	–	✓
Pritika, Shanmugam&Azam (2024), Risk Evaluation and Attack Detection in Heterogeneous IoMT Devices Using Hybrid Fuzzy Logic Analytical Approach	✓	–	✓	✓	–	✓
Nagarajan et al. (2024), A trust-centric approach to intrusion detection in edge networks for medical internet of thing Ecosystems	✓	✓	–	✓	✓/Performance	✓/Performance
Fiaz et al. (2024), A Two-Phase Blockchain-Enabled Framework for Securing Internet of Medical Things Systems	✓	Not central	Limited	✓	✓	✓
Khan et al. (2025), A lightweight scalable hybrid authentication framework for Internet of Medical Things (IoMT) using blockchainhyperledger consortium network with edge computing	✓	✓	–	Security evaluation	✓/Performance	✓
Ghadi et al. (2024), The role of blockchain to secure internet of medical things	✓	–/Not central	–	Security	Performance	Limited
Proposed EISRA	✓	✓	✓	✓	✓	✓

2.4 Research Gap Identified

Based on the reviewed studies, the following research gaps are identified. Existing research has addressed IoMT security, risk assessment, attack detection, edge-based security, and QoS from different perspectives. However, these aspects are generally evaluated separately or under different experimental conditions. Therefore, a unified framework that combines security-risk assessment with edge-device characteristics, multiple attack conditions, QoS, and scalability remains necessary.

Table 2. Research Gaps and Positioning of the Proposed EISRA Framework

Gap	Existing Research	Proposed EISRA
Heterogeneous IoMT devices	Considered in some studies	Explicitly modelled

Edge environment	Considered in selected studies	Integrated into the framework
Multiple attack types	Considered partially or for specific attack scenarios	Integrated
Device criticality	Limited consideration	Included as a risk factor
Vulnerability	Considered in some risk-assessment approaches	Included as a risk factor
Edge exposure	Limited consideration	Included as a risk factor
Security-risk score	Different risk-assessment approaches are used	Unified composite EISRA score
QoS evaluation	Evaluated in some security/performance studies	Integrated with security-risk analysis
Different IoMT scales	Evaluation conditions and scales vary across studies	10–200 IoMT devices
Attack intensity	Limited/varied evaluation	Low, Moderate, High and Very High levels
Edge resource utilization	Limited in risk-assessment studies	CPU, memory and energy evaluation
Common simulation environment	Different simulation platforms and experimental conditions	Common EISRA simulation environment
Comparative evaluation	Results are generally reported under study-specific conditions	Common evaluation framework for EISRA analysis

The identified gaps provide the motivation for the proposed EISRA framework. Unlike approaches that primarily focus on risk assessment, intrusion detection, blockchain security, or performance evaluation independently, EISRA considers security risk and edge-system performance within the same IoMT simulation environment. The framework represents heterogeneous IoMT devices, evaluates multiple attack conditions, incorporates device criticality, vulnerability and edge exposure into the risk calculation, and examines the corresponding effects on QoS and edge resources. The framework is further evaluated at different IoMT scales to investigate its scalability and consistency.

3. PROPOSED EISRA FRAMEWORK

This section presents the proposed Edge-centric IoMT Security Risk Assessment (EISRA) framework for evaluating security risks in an edge-enabled Internet of Medical Things environment. The framework is designed to represent heterogeneous medical devices, edge resources, communication threats, and healthcare cloud services within a common simulation environment. In addition to calculating a security-risk score, the framework enables the effect of security threats on QoS and edge-resource performance to be analysed.

3.1 System Architecture

The proposed architecture consists of four main layers: IoMT device layer, edge gateway layer, edge processing layer, and healthcare cloud layer. Such layered architectures are commonly used for IoMT systems to support device connectivity, localized processing, and cloud-based healthcare services [15], [16].

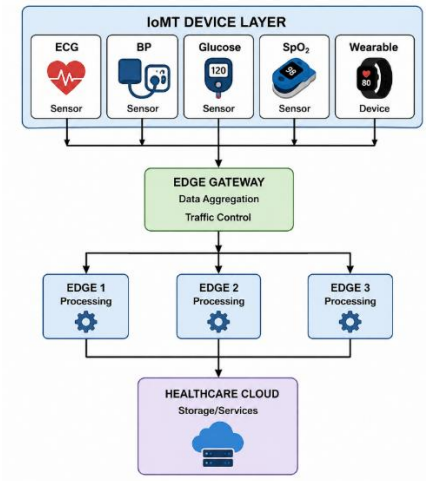

Figure 1 System Architecture

IoMT Device Layer

The IoMT layer represents heterogeneous medical devices that continuously generate healthcare information. Five representative device categories are considered in the simulation:

- ECG sensor – generates cardiac monitoring information.
- Blood Pressure (BP) sensor – generates blood pressure measurements.
- Glucose sensor – generates blood glucose measurements.
- SpO_2 sensor – generates blood oxygen saturation information.
- Wearable device – represents continuously connected wearable healthcare equipment.

These device types are representative of connected medical sensors and wearable healthcare devices commonly considered in IoMT environments [15], [16].
Each device is characterized by parameters such as device type, data-generation rate, computational requirement, criticality, vulnerability, and communication behaviour. This allows the proposed framework to distinguish between devices with different security requirements. The consideration of device characteristics and risk factors is consistent with existing IoMT risk-assessment research [17], [18]..

Edge Gateway
The edge gateway acts as an intermediate communication point between IoMT devices and edge nodes. It aggregates incoming medical data and forwards them to the appropriate edge node for processing. The gateway also represents an important security point because malicious traffic generated by compromised IoMT devices may pass through this layer. Edge and gateway-based processing are commonly considered in healthcare IoT architectures because processing data closer to the source can reduce communication latency and support time-sensitive healthcare applications [16], [19].

Edge Nodes
Multiple edge nodes are incorporated into the architecture to represent distributed edge computing resources. Edge nodes perform data processing closer to IoMT devices and reduce the need for direct communication with the healthcare cloud [16], [19]. The simulation can vary the number of edge nodes according to the IoMT population. For example:

IoMT devices	Edge nodes
10	1
25	1
50	2
100	4
150	5
200	8

The edge layer is particularly important in EISRA because the proposed framework evaluates not only security risk but also CPU utilization, memory utilization, energy consumption, latency, throughput, and network overhead.

Healthcare Cloud
The healthcare cloud represents the higher-level healthcare infrastructure responsible for long-term storage, centralized services, analytics, and access to processed medical information. Cloud, edge, and fog architectures have been investigated for healthcare applications to address processing, scalability, latency, and data-management requirements [16], [19].

The proposed framework therefore models the complete communication path:

IoMT Devices → Edge Gateway → Edge Nodes → Healthcare Cloud

3.2 Threat Model
The proposed framework considers five representative attacks that can affect different components of the IoMT-edge environment. IoMT security studies have identified a broad range of network, device, and communication threats affecting connected medical environments[17], [20].
Distributed Denial-of-Service Attack: A DDoS attack is modelled by generating excessive malicious traffic toward the gateway or edge resources. The increased traffic load can consume network and computational resources and consequently affect service availability and QoS.Denial-of-service attacks are recognized threats in IoMT environments [20].
Man-in-the-Middle Attack: A MitM attack represents unauthorized interception of communication between IoMT devices, gateways, and edge nodes. The attack is considered in the risk assessment because it may compromise the confidentiality and integrity of medical information [17], [20].
Replay Attack:A replay attack is represented by retransmitting previously captured legitimate messages. Such behaviour may result in incorrect or repeated medical information being processed by the healthcare system[20].
Data Injection Attack: In a data injection attack, malicious or modified information is introduced into the IoMT communication flow. Since healthcare decisions may depend on the integrity of sensor measurements, data injection is considered an important risk factor [17], [20].
Device Impersonation Attack: Device impersonation represents an unauthorized entity attempting to behave as a legitimate IoMT device. Successful impersonation may allow malicious traffic or fabricated medical information to enter the edge-enabled healthcare environment[17], [20]. The threat model therefore considers both network-level and device-level threats, allowing the proposed framework to evaluate their influence on security risk and system performance.
3.3 EISRA Risk Model
The central component of the proposed framework is the Edge-centric IoMT Security Risk Assessment (EISRA) model. Instead of representing security risk using a single parameter, the proposed model combines multiple factors associated with the likelihood and consequences of a security event. Existing IoMT risk-assessment research emphasizes the importance of considering multiple risk dimensions, including threats, vulnerabilities, impacts, and characteristics of medical devices [17], [18]. Building on this risk-oriented perspective, the proposed EISRA model additionally incorporates edge exposure to represent the security conditions associated with the edge-enabled architecture.
The proposed Edge-centric IoMT Security Risk Assessment (EISRA) is defined as:
$ERAS=\alpha L+\beta I+\gamma C+\delta V+\epsilon E$
where:

L = Attack Likelihood
I = Attack Impact
C = Medical Device Criticality
V = Device Vulnerability
E = Edge Exposure
α,β,γ,δ,ϵ = weighting coefficients.

For the initial simulation, the following normalized weights are considered:α=0.20, β=0.25. Thus,0.20+0.25+0.20+0.20+0.15=1, all five factors are normalized to the range 0–100 before calculating the final score.

3.3.1 Attack Likelihood (L)

Attack likelihood represents the probability or estimated possibility of a security attack affecting an IoMT device or edge resource. Higher attack likelihood values indicate a greater possibility of an attack occurring. In the simulation, attack likelihood is determined based on several factors, including attack intensity, attack frequency, abnormal traffic patterns, device exposure, and the type of attack. These factors collectively contribute to estimating the level of security threat faced by IoMT devices and edge resources.

3.3.2 Attack Impact (I)

Attack impact represents the potential consequence of a successful attack. Higher values indicate greater potential damage to the IoMT service. For example, an attack affecting the availability of an edge node serving multiple medical devices can have a greater impact than an attack affecting an individual low-criticality sensor.

3.3.3 Device Criticality (C)

Device criticality represents the importance of an IoMT device to healthcare services.
For example:

Table 3. Relative Criticality of IoMT Devices

Device	Relative criticality
ECG	High
SpO	High
Blood Pressure	Medium–High
Glucose	Medium–High
Wearable	Medium

These values should be defined explicitly in the simulation configuration rather than changed between experiments.

3.3.4 Vulnerability (V)

Vulnerability represents the susceptibility of an IoMT device or edge component to security threats. The vulnerability score can be determined by considering various characteristics, including resource constraints, software and security weaknesses, communication exposure, authentication strength, and susceptibility to attacks. For simulation purposes, the vulnerability value is normalized on a scale from 0 to 100, where higher values indicate a greater level of vulnerability.

3.3.5 Edge Exposure (E)

Edge exposure is an important factor introduced in the proposed framework, representing the extent to which an IoMT device or edge node is exposed to potentially malicious communication. A device connected to a heavily loaded or highly exposed edge node can receive a higher exposure score. The level of edge exposure can therefore be influenced by several factors, including the number of connected devices, edge-node workload, malicious traffic, communication intensity, and the number of exposed connections.

3.3.6 Normalized Risk Score

The calculated ERAS value is normalized to obtain a percentage-based risk score:

$$ERAS_N = \frac{ERAS - ERAS_{min}}{ERAS_{max} - ERAS_{min}} \times 100$$

Since the five input factors are normalized and the weights sum to one, the implementation can also directly constrain the composite score to the 0–100 range.
The resulting value is used for risk classification.

3.4 Risk Classification

The normalized EISRA score is classified into four security-risk levels.

Table 4. EISRA Risk Classification Levels

Risk Score	Risk Level	Interpretation
0–24.99	Low	Limited security risk
25–49.99	Moderate	Requires monitoring
50–74.99	High	Security intervention recommended
75–100	Critical	Immediate security attention required

The risk-level boundaries were defined as equal-width intervals on the normalized 0–100 EISRA scale to provide a transparent and reproducible four-level interpretation. These thresholds are intended as decision-support boundaries rather than universally established clinical or cybersecurity standards.

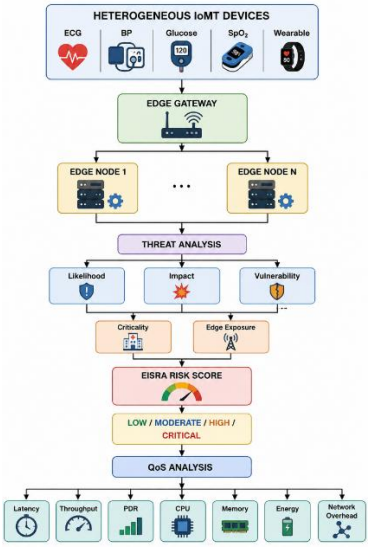

Figure 3Overall EISRA Workflow

4. SIMULATION METHODOLOGY

This section describes the simulation environment, configuration, QoS parameters, and execution procedure used to evaluate the proposedEdge-centric IoMT Security Risk Assessment (EISRA) framework. The simulation is designed to represent heterogeneous IoMT devices communicating through an edge gateway and distributed edge nodes before reaching the healthcare cloud. The same simulation conditions are used across different device populations and attack intensities to enable consistent performance and comparative analysis.

4.1 Simulation Environment

A standalone simulation environment is developed to model an edge-enabled IoMT healthcare network. The environment consists of heterogeneous IoMT devices, an edge gateway, multiple edge nodes, and a healthcare cloud. The IoMT devices generate medical monitoring data and transmit the generated traffic to the edge gateway. The gateway forwards the traffic to the available edge nodes for processing. Processed information is subsequently transmitted to the healthcare cloud.

The simulated IoMT devices include ECG sensors, blood-pressure sensors, glucose sensors, SpO sensors, and wearable devices. Each device is assigned characteristics such as device type, data-generation behaviour, criticality, vulnerability, and communication activity. The edge nodes provide computational resources for processing IoMT traffic and are monitored for CPU utilization, memory utilization, energy consumption, and network activity.

The simulation also introduces malicious traffic corresponding to DDoS, MitM, replay, data injection, and device impersonation attacks. For each simulation scenario, the EISRA model calculates the security-risk score using attack likelihood, impact, device criticality, vulnerability, and edge exposure. The resulting security risk is analysed together with QoS parameters.

The overall simulated communication path is:

IoMT Devices→Edge Gateway→Edge Nodes→Healthcare Cloud

The simulation is implemented as a standalone prototype simulation, where the device, attack, risk, edge-load, and QoS models are executed computationally. It is therefore intended to demonstrate and evaluate the proposed methodology rather than represent measurements obtained from physical medical devices.

4.2 Simulation Configuration

To evaluate scalability, the number of IoMT devices is varied from 10 to 200. The number of edge nodes is increased according to the device population. Four attack-intensity levels are considered: low, moderate, high, and very high. Each experimental scenario is repeated 30 times, and the mean value is used for the final analysis.

Table 5. Simulation Configuration

Parameter	Values
IoMT device types	ECG, BP, Glucose, SpO_2, Wearable
Number of IoMT devices	10, 25, 50, 100, 150, 200
Number of edge nodes	1, 2, 4, 5, 8
Edge gateway	1
Healthcare cloud	1
Attack types	DDoS, MitM, Replay, Injection, Impersonation
Attack intensity	Low, Moderate, High, Very High
Simulation runs/scenario	30
Risk factors	Likelihood, Impact, Criticality, Vulnerability, Edge Exposure
Risk range	0–100
Risk levels	Low, Moderate, High, Critical

The different device populations enable the scalability of the proposed framework to be investigated. For example, the 10-device scenario represents a relatively small IoMT deployment, whereas the 200-device scenario represents a substantially larger edge-enabled IoMT environment. The attack-intensity levels are used to investigate whether increasing malicious activity produces corresponding changes in the calculated risk and system performance.

4.3 QoS Parameters

Security assessment alone does not provide a complete evaluation of an edge-enabled IoMT system. Therefore, the proposed simulation measures both security andQuality of Service (QoS).

Table 6. QoS Evaluation Parameters

Parameter	Unit	Objective
Latency	ms	↓
Throughput	Mbps	↑
Packet Delivery Ratio (PDR)	%	↑
CPU Utilization	%	↓
Memory Utilization	%	↓
Energy Consumption	J	↓
Network Overhead	%	↓

Latency

Latency represents the time required for medical data to travel through the simulated IoMT-edge environment.

Latency=Tarrival−Tgeneration

Lower latency is desirable for time-sensitive healthcare applications.

Throughput

Throughput represents the amount of successfully transmitted data during the simulation period.

$$Throughput = \frac{Successfully\ Delivered\ Data}{Simulation\ Time}$$

Higher throughput indicates better data-transfer performance.

Packet Delivery Ratio

PDR represents the proportion of transmitted packets that are successfully received.

$$PDR = \frac{Packets\ Received}{Packets\ Sent} \times 100$$

A higher PDR indicates more reliable communication.

CPU Utilization

CPU utilization represents the processing workload imposed on the edge nodes.

$$CPU\ Utilization = \frac{CPU\ Used}{CPU\ Available} \times 100$$

Lower utilization is desirable when comparing otherwise equivalent scenarios.

Memory Utilization

Memory utilization represents the proportion of available edge memory consumed during simulation.

$$Memory\ Utilization = \frac{Memory\ Used}{Memory\ Available} \times 100$$

Energy Consumption

Energy consumption represents the simulated energy required by IoMT and edge resources during processing and communication.Lower energy consumption indicates better resource efficiency.

Network Overhead

Network overhead represents the additional communication generated by control, security, retransmission, and attack-related traffic relative to useful data transmission.Lower network overhead is desirable.

4.4 Simulation Procedure

The simulation follows a sequence of initialization, traffic generation, security-risk assessment, edge-resource evaluation, and QoS measurement.

Step 1: Initialize IoMT Devices

The selected number of IoMT devices is created and distributed among the available edge nodes. Each device is assigned its device type and corresponding characteristics.

Step 2: Generate Medical Traffic

Normal medical traffic is generated from ECG, BP, glucose, SpO_2, and wearable devices according to their configured traffic behaviour.

Step 3: Generate Attack Traffic

The selected attack scenario and attack intensity are introduced into the simulation. Malicious traffic is generated according to the corresponding attack model.

Step 4: Calculate Security Risk

For each scenario, the EISRA model evaluates:

L, I, C, V, E

and calculates:

ERAS=αL+βI+γC+δV+ϵE

The resulting score is converted into the corresponding Low, Moderate, High, or Critical risk category.

Step 5: Calculate Edge Load

The workload generated at each edge node is calculated based on the number of connected devices, normal traffic, malicious traffic, and processing requirements.

Step 6: Calculate QoS

The simulation calculates several key performance metrics to evaluate the effectiveness of the proposed framework, including latency, throughput, Packet Delivery Ratio (PDR), CPU utilization, memory utilization, energy consumption, and network overhead. These metrics provide a comprehensive assessment of network performance, resource utilization, communication efficiency, and energy requirements within the IoMT environment.

Step 7: Repeat the Simulation

Each configuration is executed for 30 independent runs to reduce the effect of random variation.

Step 8: Calculate Average Results

The mean value of each security and QoS parameter is calculated:

$$Mean(X) = \frac{1}{N}\sum_{i=1}^{N} X_i$$

where N=30.

Step 9: Comparative Analysis

The averaged results are compared across different IoMT device populations, different attack intensities, and different attack types. In addition, the performance of the proposed framework is compared with representative existing approaches wherever comparable implementations or published measurement results are available. This comparison helps evaluate the effectiveness and performance of the proposed framework under different IoMT and security conditions.

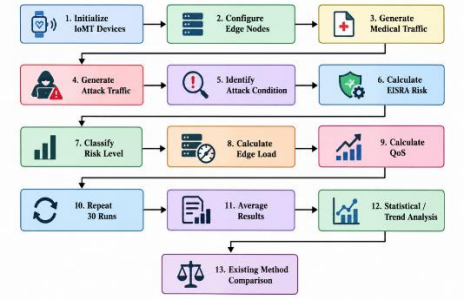

Figure 4 Overall EISRA Simulation Workflow

5. RESULTS AND DISCUSSION

This section presents the performance evaluation of the proposed Edge-centric IoMT Security Risk Assessment (EISRA) framework under different IoMT network sizes. The evaluation considers both security risk and network/system performance in the simulated edge-enabled IoMT environment. The number of IoMT devices is varied across 10, 25, 50, 100, 150, and 200 devices, while the corresponding number of edge nodes is increased from 1 to 8 to accommodate the growing device population. The evaluated performance parameters include EISRA risk score, latency, throughput, packet delivery ratio (PDR), CPU utilization, and energy consumption. Each configuration is executed for 30 simulation runs, and the average values are used for analysis.

5.1 Security Risk and Performance Analysis

The experiment evaluates the effect of increasing the IoMT device population on the security risk and overall performance of the proposed edge-enabled IoMT environment. The IoMT device population is increased from 10 to 200 devices, with the number of edge nodes adjusted from 1 to 8. The evaluation considers the EISRA risk score, latency, throughput, PDR, CPU utilization, and energy consumption to provide a consolidated assessment of security and system performance.

Table 7. Security Risk and Performance Metrics with Increasing IoMT Device Population

IoMT Devices	Edge Nodes	Risk	Latency (ms)	Throughput (Mbps)	PDR (%)	CPU (%)	Energy (J)
10	1	61.54	41.31	32.89	90.31	44.25	38.01
25	1	62.19	50.79	30.57	88.94	71.62	47.57
50	2	63.50	53.48	29.39	88.44	71.79	58.08
100	4	66.03	58.63	27.19	87.64	71.78	79.16
150	5	68.58	66.25	24.34	86.31	80.83	101.24
200	8	70.95	68.57	22.65	85.82	71.84	121.19

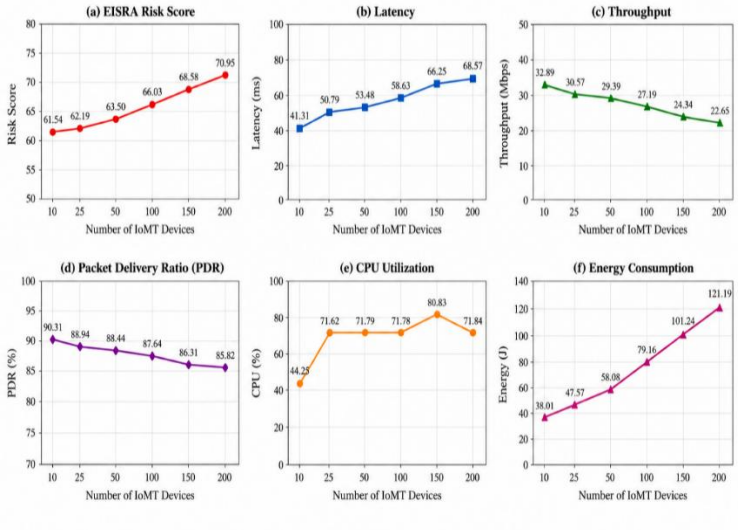

Figure 5. Performance Metrics versus Number of IoMT Devices under High Attack Intensity

The results presented in Table 4 and Figure 4 show the effect of increasing the IoMT device population on the security and performance characteristics of the proposed edge-enabled IoMT environment. As the number of IoMT devices increases from 10 to 200, the EISRA risk score increases from 61.54 to 70.95, while latency increases from 41.31 ms to 68.57 ms. In contrast, throughput decreases from 32.89 Mbps to 22.65 Mbps and PDR decreases from 90.31% to 85.82%.

Security Risk

The EISRA risk score increases progressively with the number of IoMT devices. The risk score increases from 61.54 for 10 devices to 70.95 for 200 devices. This represents an increase of approximately 15.3% across the evaluated network sizes. The increasing risk score indicates that a larger IoMT environment introduces greater overall security exposure. As the number of connected endpoints increases, the number of potential entry points and interactions within the edge environment also increases. Although additional edge nodes are introduced to support the growing device population, the increase in IoMT endpoints continues to contribute to the overall security exposure.The EISRA score incorporates factors such as attack likelihood, attack impact, device criticality, and vulnerability. Therefore, the observed increase represents the combined effect of these security-related factors rather than device count alone.Based on the risk thresholds defined in Section 3, the obtained scores fall within the High-risk categoryfor all evaluated configurations. Thus, the proposed framework is able to distinguish the gradual increase in security risk as the IoMT environment scales while maintaining an interpretable risk classification.

Latency

The latency increases with the growth of the IoMT device population. At 10 devices, the measured latency is 41.31 ms, whereas it increases to 68.57 msat 200 devices.The increase in latency can be attributed to the additional communication and processing demands introduced by the larger number of IoMT devices. As more devices generate and transmit data through the edge environment, the processing and communication workload increases. The additional edge nodes help accommodate the growing device population, but the overall latency still increases as the network becomes larger.The approximately 66.0% increase in latency from 10 to 200 devices indicates that network scalability has a measurable effect on communication responsiveness.

Throughput

The throughput exhibits a decreasing trend as the number of IoMT devices increases. The throughput decreases from 32.89 Mbps at 10 devices to 22.65 Mbps at 200 devices.This reduction indicates that the available network and edge-processing capacity is increasingly shared among a larger number of IoMT devices. Consequently, the effective data delivery rate decreases as the device population grows. The result highlights the importance of efficient edge resource management when supporting large-scale IoMT deployments.Overall, the throughput decreases by approximately 31.1% between the smallest and largest configurations.

Packet Delivery Ratio

The PDR also decreases gradually as the IoMT network size increases. The PDR decreases from 90.31% for 10 devices to 85.82% for 200 devices.The reduction indicates that larger network configurations experience comparatively lower successful packet delivery. The increased communication activity and network workload associated with additional IoMT devices can contribute to packet delivery degradation.Although the PDR decreases by approximately 4.9 percentage points, the value remains above 85% for all evaluated configurations. This indicates that the edge-enabled environment continues to provide a relatively high level of packet delivery even as the network scales.

CPU Utilization

CPU utilization shows variations across the evaluated configurations. The CPU utilization increases from 44.25% at 10 devices to 71.62% at 25 devices, followed by values of 71.79%, 71.78%, 80.83%, and 71.84% for 50, 100, 150, and 200 devices, respectively. The increase in CPU utilization from the smallest configuration indicates the additional computational demand created by increasing IoMT traffic and processing requirements. The results also show that CPU utilization does not increase monotonically across every configuration. This behaviour can be attributed to the corresponding changes in edge-node allocation as the device population increases.The relatively stable CPU utilization around the 71–72% range for several configurations suggests that the additional edge nodes provide computational support

as the IoMT population increases. The higher value observed at 150 devices indicates a comparatively greater processing demand for that configuration.

Energy Consumption

Energy consumption demonstrates a clear increasing trend with increasing IoMT device population. The energy consumption increases from 38.01 J for 10 devices to 121.19 J for 200 devices. This increase is associated with the larger number of devices and the corresponding increase in communication, data-processing, and edge-network activities. As the IoMT environment becomes larger, more computational and communication operations are required, resulting in greater overall energy consumption. The energy consumption increases by approximately 219.0% between 10 and 200 devices. This result highlights the importance of considering energy efficiency when deploying the proposed framework in large-scale IoMT environments. The consolidated results demonstrate that network scale has a direct influence on both security risk and system performance. As the number of IoMT devices increases from 10 to 200, the EISRA risk score and latency increase, while throughput and PDR decrease. Energy consumption also increases substantially with network size. CPU utilization remains comparatively stable for several configurations despite the increase in device population, indicating the contribution of additional edge nodes in distributing the computational workload.

The simultaneous increase in risk and latency, together with the reduction in throughput and PDR, demonstrates the increasing complexity of managing large-scale IoMT environments. The results therefore show that security assessment should not be considered independently from communication and resource-performance characteristics. Overall, the experiment demonstrates that the proposed EISRA framework provides a consolidated assessment of security risk and edge-enabled IoMT performance as the network scales from 10 to 200 devices. The results establish the baseline performance of the proposed framework and provide a basis for the subsequent comparison with existing methods and further analysis of attack conditions. The proposed EISRA framework is compared with existing IoMT security approaches based on the security and performance characteristics addressed by each method. Existing approaches generally focus on individual aspects such as risk assessment, intrusion detection, trust management, or QoS, whereas EISRA integrates security-risk assessment with edge exposure, device characteristics, QoS, resource utilization, and scalability within a common simulation framework.

6. CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

This paper proposed an Edge-centric IoMT Security Risk Assessment (EISRA) framework for evaluating security risks in an edge-enabled Internet of Medical Things environment. The proposed framework models heterogeneous IoMT devices, including ECG, blood-pressure, glucose, SpO, and wearable devices, communicating through an edge gateway and distributed edge nodes. A composite risk model was developed by considering attack likelihood, attack impact, device criticality, vulnerability, and edge exposure.

The proposed framework evaluates multiple security threats, including DDoS, Man-in-the-Middle, replay, data injection, and device impersonation attacks, under different attack-intensity levels. In addition to security-risk assessment, the simulation evaluates important QoS and resource parameters, including latency, throughput, packet delivery ratio, CPU utilization, memory utilization, energy consumption, and network overhead. The scalability of the framework is investigated by varying the number of IoMT devices from 10 to 200 and evaluating the corresponding edge-resource behaviour. A comparative analysis with representative existing approaches is also performed to assess the coverage and performance of the proposed framework. Overall, EISRA provides a common simulation-based approach for jointly analysing IoMT security risk, edge-resource behaviour, QoS, attack conditions, and scalability, thereby addressing the limitations of evaluating these aspects independently.

6.2 Future Work

The proposed framework provides a foundation for extending IoMT security assessment toward decentralized and trust-aware security management. As the next stage of this research, blockchain-based trust management will be incorporated into the edge layer to provide decentralized security records, tamper-resistant trust information, and improved management of interactions among IoMT devices and edge nodes. The extended framework will investigate the security benefits of blockchain while also analysing its additional latency, computational overhead, communication overhead, storage requirements, and energy consumption. This will enable a systematic comparison between the EISRA baseline and the proposed blockchain-enhanced security framework.

REFERENCES

[1] M. A. Ahad, S. Paiva, G. Tripathi, and N. F. Ahmed, “Enabling technologies and sustainable smart healthcare: A review,” IEEE Access, vol. 9, pp. 11468–11486, 2021.

[2] Y. Sun, F. P.-W. Lo, and B. Lo, “Security and privacy for the Internet of Medical Things enabled healthcare systems: A survey,” IEEE Access, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/ACCESS.2019.2960617.

[3] K. Svandova and Z. Smutny, “Internet of Medical Things security frameworks for risk assessment and management: A scoping review,” Journal of Multidisciplinary Healthcare, vol. 17, pp. 2281–2301, 2024, doi: 10.2147/JMDH.S459987.

[4] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, “Securing Internet of Medical Things systems: Limitations, issues and recommendations,” Future Generation Computer Systems, vol. 105, pp. 581–606, 2020, doi: 10.1016/j.future.2019.12.028.

[5] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, A. Lymberopoulos, and J. S. Rodríguez, “A survey on security threats and countermeasures in Internet of Medical Things (IoMT),” Transactions on Emerging Telecommunications Technologies, vol. 33, no. 6, Art. no. e4049, 2022, doi: 10.1002/ett.4049.

[6] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, and P. Kotzanikolaou, “Risk assessment methodologies for the Internet of Medical Things: A survey and comparative appraisal,” IEEE Access, vol. 9, pp. 40049–40075, 2021, doi: 10.1109/ACCESS.2021.3064682.
[7] L. Kong, J. Tan, J. Huang, G. Chen, S. Wang, X. Jin, P. Zeng, M. Khan, and S. K. Das, “Edge-computing-driven Internet of Things: A survey,” ACM Computing Surveys, vol. 55, no. 8, Art. no. 174, 2023, doi: 10.1145/3555308.
[8] Y. Sun, F. P.-W. Lo, and B. Lo, “Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey,” IEEE Access, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/ACCESS.2019.2960617.
[9] R. M. Czekster, T. Webber, L. BertolinFurstenau, and C. Marcon, “Dynamic risk assessment approach for analysing cyber security events in medical IoT networks,” Internet of Things, vol. 29, Art. no. 101437, 2025, doi: 10.1016/j.iot.2024.101437.
[10] Pritika, B. Shanmugam, and S. Azam, “Risk Evaluation and Attack Detection in Heterogeneous IoMT Devices Using Hybrid Fuzzy Logic Analytical Approach,” Sensors, vol. 24, no. 10, Art. no. 3223, 2024, doi: 10.3390/s24103223.
[11] G. Nagarajan, M. Margala, S. S. Shankar, P. Chakrabarti, and R. I. Minu, “A trust-centric approach to intrusion detection in edge networks for medical internet of thing Ecosystems,” Computers & Electrical Engineering, vol. 115, Art. no. 109129, 2024, doi: 10.1016/j.compeleceng.2024.109129.
[12] K. Fiaz, A. Zeb, S. Hussain, K. Khurshid, R. R. Irshad, M. Alharby, T. Rahman, I. M. Alwayle, and F. Pallonetto, “A Two-Phase Blockchain-Enabled Framework for Securing Internet of Medical Things Systems,” Internet of Things, vol. 28, Art. no. 101335, 2024, doi: 10.1016/j.iot.2024.101335.
[13] A. A. Khan, A. A. Laghari, R. Alroobaea, A. M. Baqasah, M. Alsafyani, H. Alsufyani, and S. Ullah, “A lightweight scalable hybrid authentication framework for Internet of Medical Things (IoMT) using blockchainhyperledger consortium network with edge computing,” Scientific Reports, vol. 15, no. 1, Art. no. 19856, 2025, doi: 10.1038/s41598-025-05130-w.
[14] K. Svandova and Z. Smutny, “Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review,” Journal of Multidisciplinary Healthcare, vol. 17, pp. 2281–2301, 2024, doi: 10.2147/JMDH.S459987.
[15] K. Svandova and Z. Smutny, “Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review,” Journal of Multidisciplinary Healthcare, vol. 17, pp. 2281–2301, 2024, doi: 10.2147/JMDH.S459987.
[16] M. Hartmann, G. Zilberman, and others, “Edge computing in smart health care systems: Review, challenges, and research directions,” Transactions on Emerging Telecommunications Technologies, vol. 33, no. 3, Art. no. e3710, 2022, doi: 10.1002/ett.3710.
[17] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou, and C. Douligeris, “Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal,” IEEE Access, vol. 9, pp. 40049–40075, 2021, doi: 10.1109/ACCESS.2021.3064682.
[18] F. Alsubaei, A. Abuhussein, and S. Shiva, “Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment,” in Proc. IEEE 42nd Conference on Local Computer Networks Workshops, 2017, pp. 112–120, doi: 10.1109/LCN.Workshops.2017.72.
[19] R. Dwivedi, D. Mehrotra, and S. Chandra, “Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review,” Journal of Oral Biology and Craniofacial Research, vol. 12, no. 2, pp. 302–318, 2022, doi: 10.1016/j.jobcr.2021.11.010.
[20] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. S. Rodríguez, and D. Lymberopoulos, “A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT),” Transactions on Emerging Telecommunications Technologies, vol. 33, no. 6, Art. no. e4049, 2022, doi: 10.1002/ett.4049.
[21] M. K. Hasan, T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, A. A. Eshmawi, S. Abdel-Khalek, and H. M. Alkhassawneh, “A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things,” IET Communications, vol. 16, no. 5, pp. 421–432, 2022, doi: 10.1049/cmu2.12301.